Monitoring Windows Using WMI

Purpose

This document describes how to monitor Windows machines with Nagios XI using Windows Management Instrumentation (WMI). WMI allows for agentless monitoring of Windows machines 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 there is 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 the NCPA website.
- Watch this video about NCPA.

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. Watch this video that addresses SNMP.

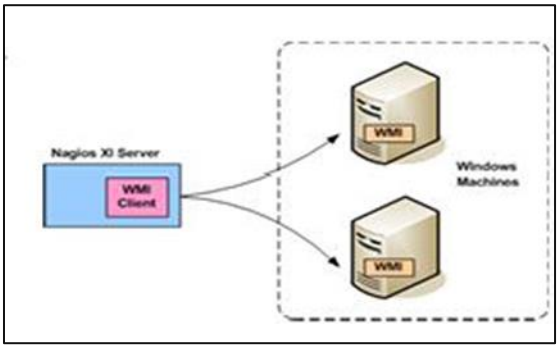
Another agentless option is using OpenSSH. Microsoft has embraced OpenSSH, but it is a bit more granular, as it is secure by default. Our SSH Proxy Wizard will allow you to retrieve metrics. However, there needs to be some prep work and testing, within your organization, and will require plugins from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

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.

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



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.

Windows Server Core (No Desktop)

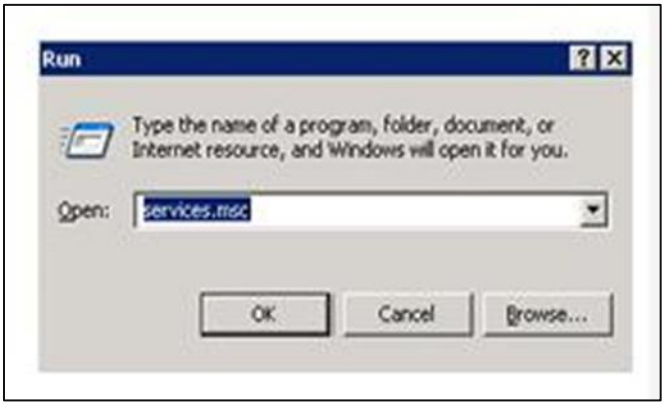
This guide does not provide instructions for configuring Windows Server Core, some of the required GUI utilities are not available in server core. It is technically possible to configure the permissions remotely by using the information in this document, you will need to research on how to perform the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

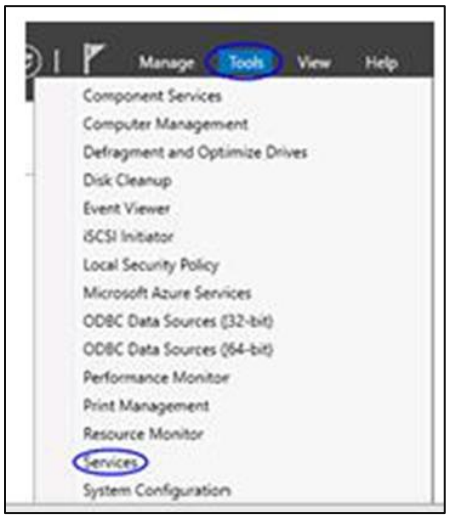
- Click **Start** and choose **Run**.
- The window to the right will appear and type `services.msc` in the Open field and then click **OK**.



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**



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

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.

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 fail the password policy requirements.

Setting WMI Permissions

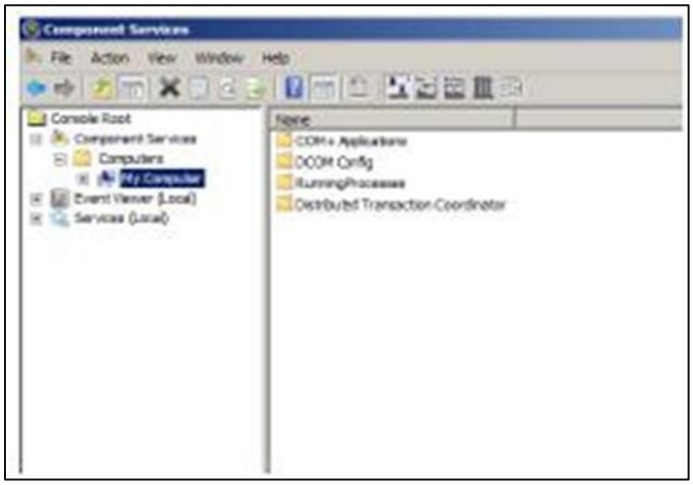
WMI requires a valid username and password on the target system. The following steps outline how to add only the permissions needed to the Windows user account. Some of these permissions do not need to be set if your user account is a member of the local administrators group HOWEVER from a security perspective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

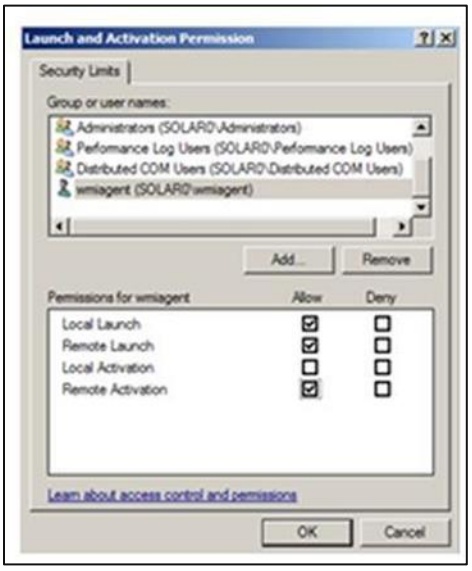
You need to give your newly created user access to DCOM on the localhost. To do this, open **Component Services**.

- 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**.



- 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**.



Note: 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.

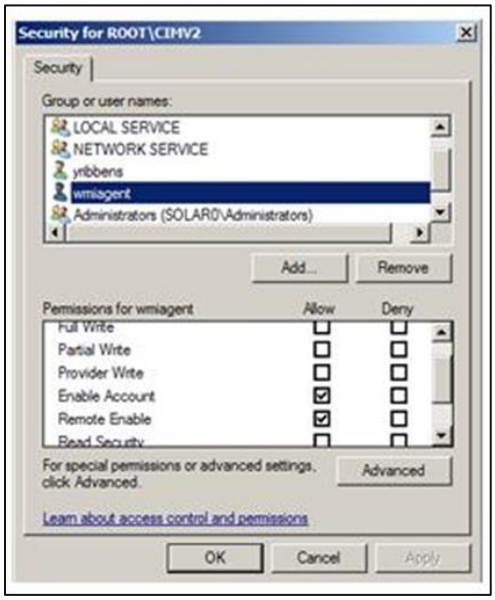
Adding Remote WMI Access

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**.



Note: 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.

Windows Firewall Settings

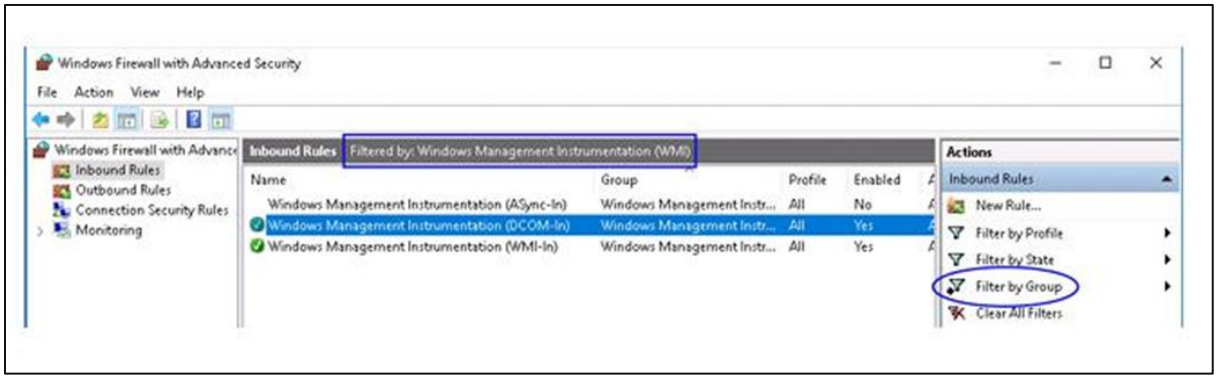
Next, configure the firewall rules specific to the version of windows being monitored.

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

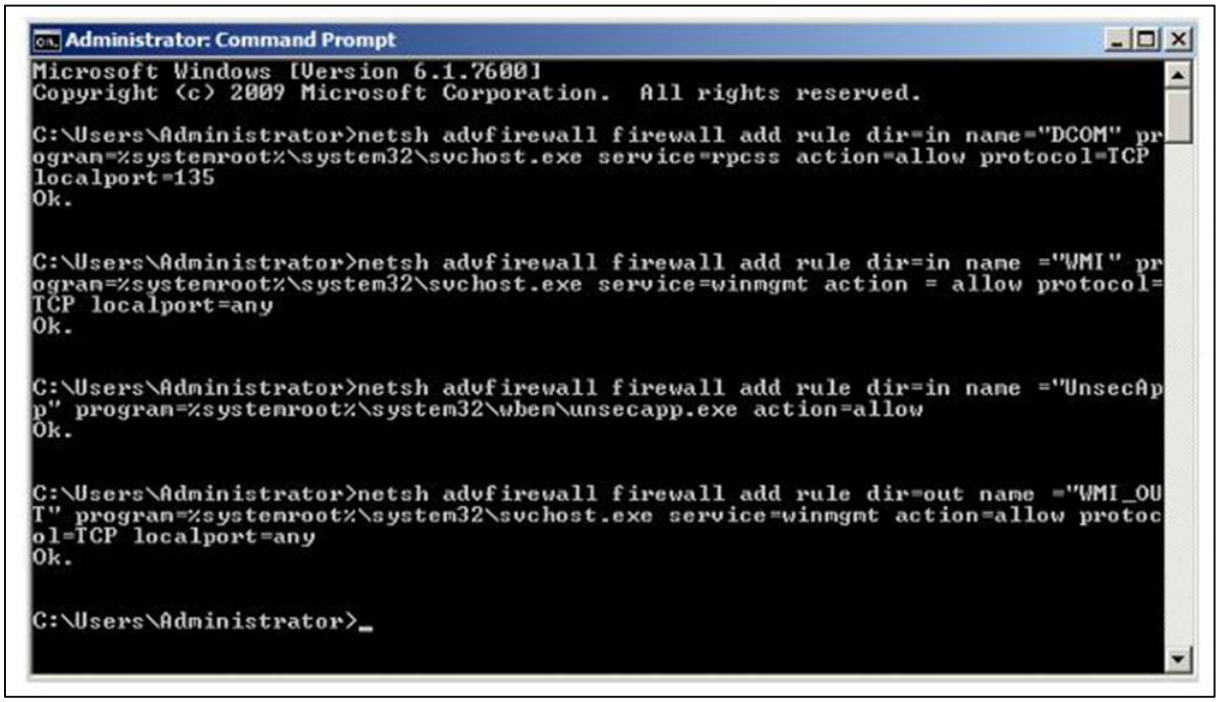
If the WMI rule group does not exist as pictured above, the recommended settings are listed here as outlined by Microsoft. From the command prompt enter (each command is one long command to type):

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

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
```

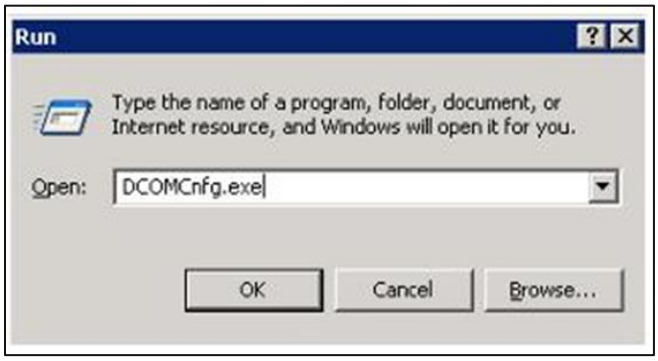


More details about 2008 Firewall settings can be found at this page.

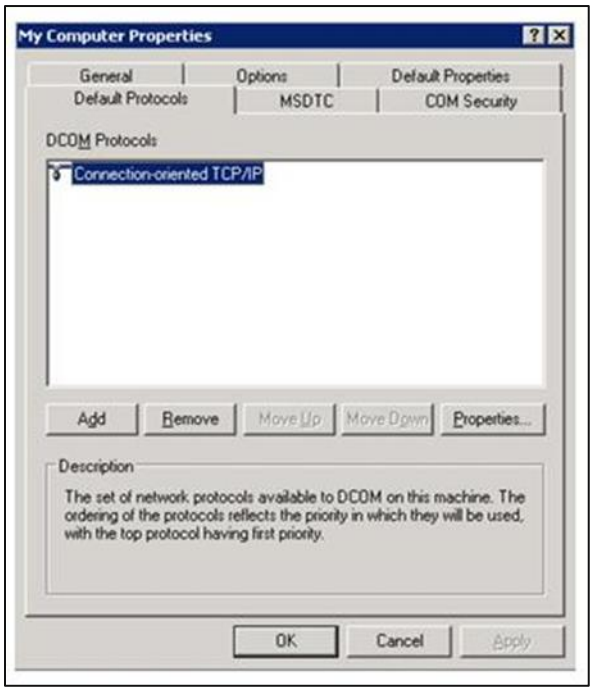
Windows Server 2003 Firewall Rules

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 to write firewall rules, specifying a port range is also described.

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



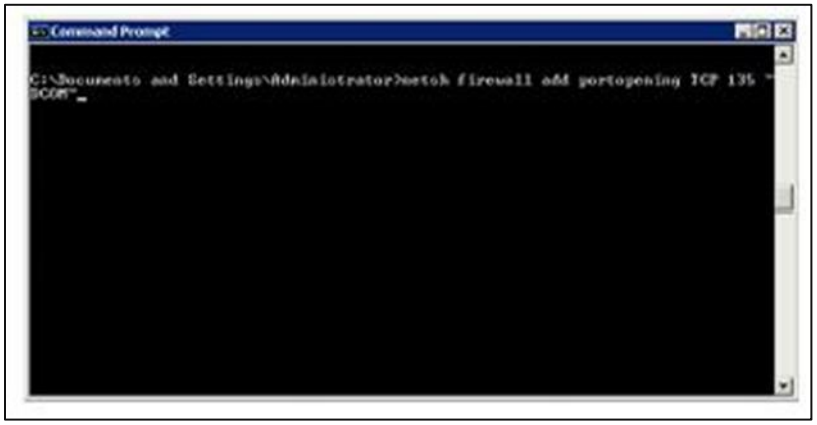
- Expand **Component Services**, expand **Computers**, right click **My Computer**, and select **Properties**.
- Click the **Default Protocols** tab
- Click the **Properties** button.



- 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.

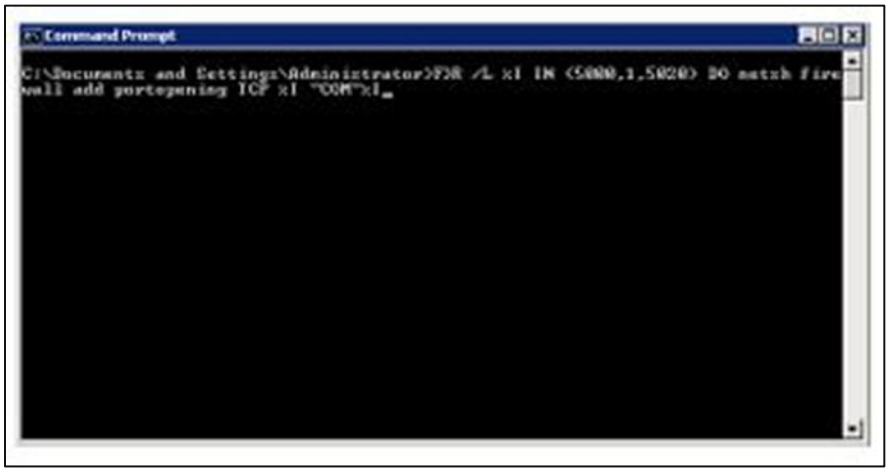
- Allow the port range through the windows firewall.
- This command will open ports from 5000-5020 to match the COM Internet Services Range.
- From the command prompt enter:

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



- Lastly, open DCOM port 135. From the command prompt type:

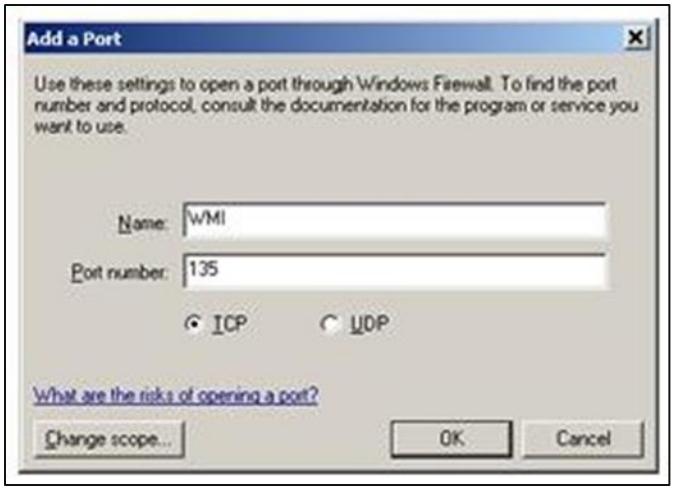
```
netsh firewall add portopening TCP 135 "DCOM"
```



Windows XP Firewall Rules

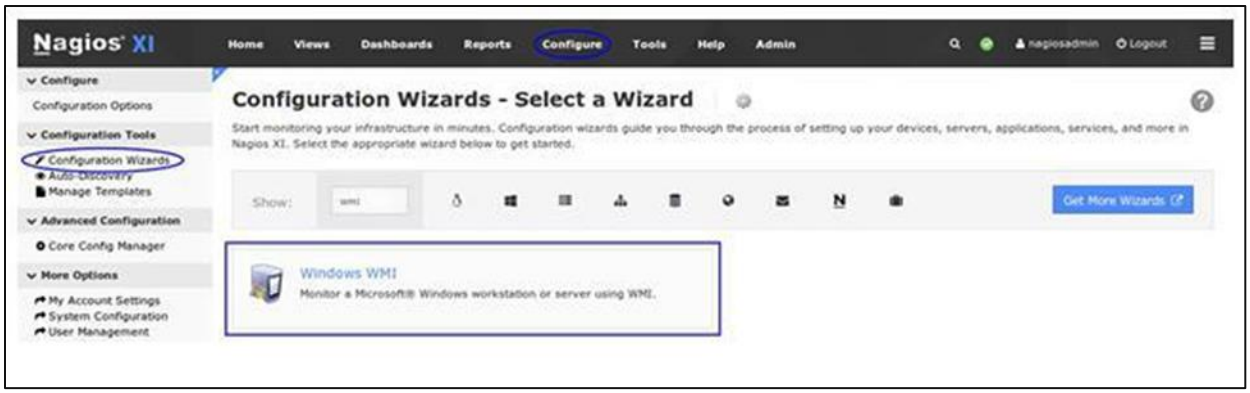
If you are running a firewall on the Windows machine, you must ensure that the Nagios server can contact the WMI service.

- 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

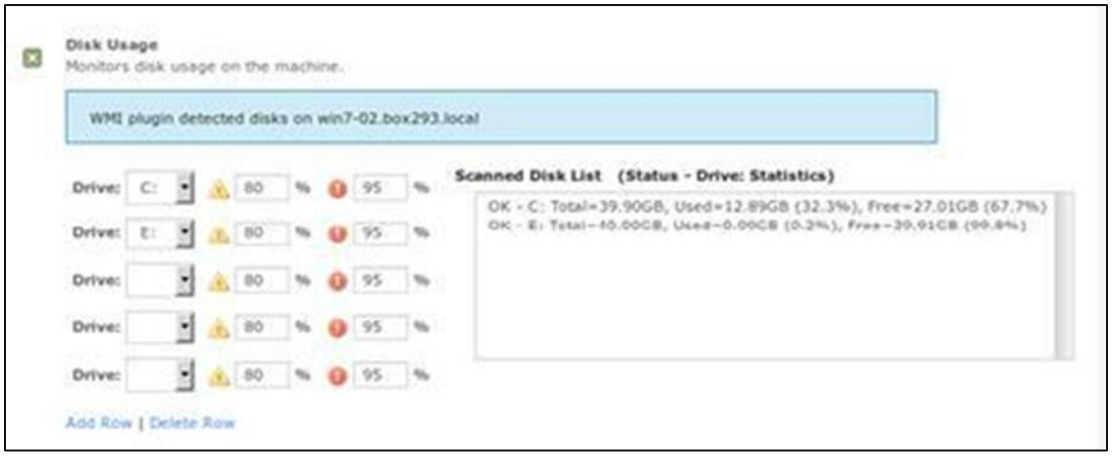
Now that WMI has been configured on your windows machine you can now run the Windows WMI wizard from your Nagios XI server. To begin using the Windows WMI wizard navigate via the top menu bar **to Configure > Run a configuring wizard** and select the **Windows WMI** wizard. In the following screenshot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



- 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 Authentication File section in this document for more information.
- Click **Next** to proceed to Step 2.

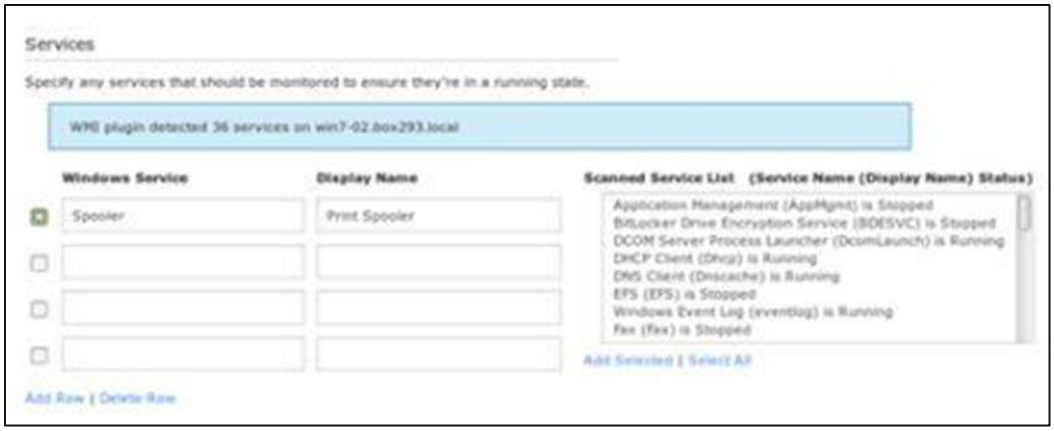
- When you proceed to **Step 2**, the wizard will perform a WMI query against the Windows machine to get a list of the available disks, services, and processes.
- If Nagios XI is not able to communicate via WMI, an error will be displayed (see the Troubleshooting section on resolving these errors).
- Make sure the **Host Name** field is correctly populated.
- Select the server metrics you wish to monitor and 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.

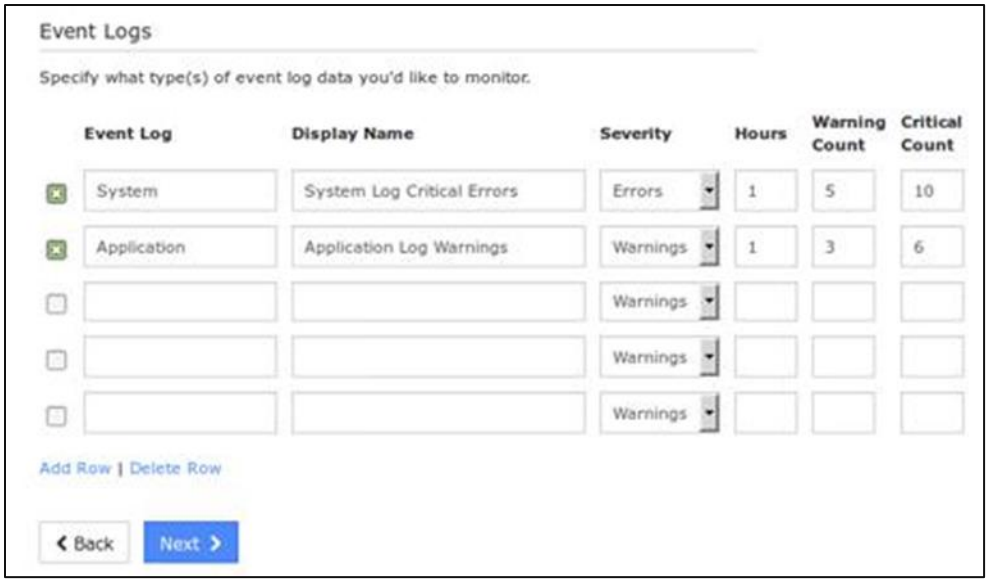


For Services, the automatically detected services will be populated in the **Scanned Service List.**

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



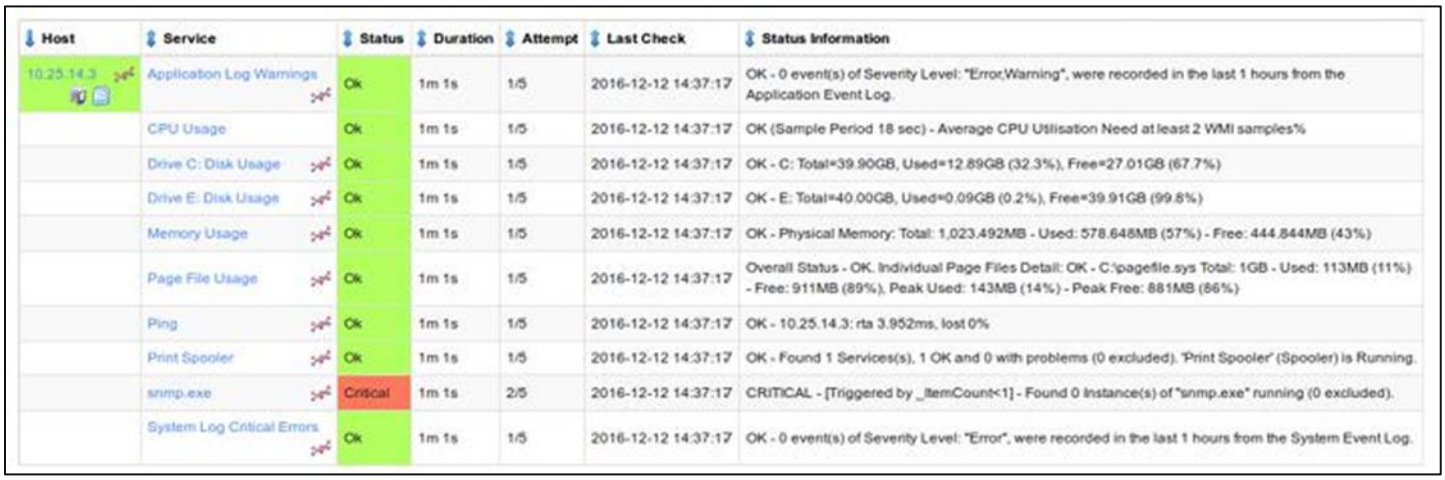
For Event Logs you can select the specific log on the windows machine and define warning and critical thresholds based on the amount of Warning or Error logs found in the past x hours.



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, click on **Finish** in the last step of the wizard. This will create new hosts and services and begin monitoring.

Once the wizard applies the configuration, click the **View status details for xxxxx** link to see the new host and services that were created.



Host	Service	Status	Duration	Attempt	Last Check	Status Information
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

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 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
```

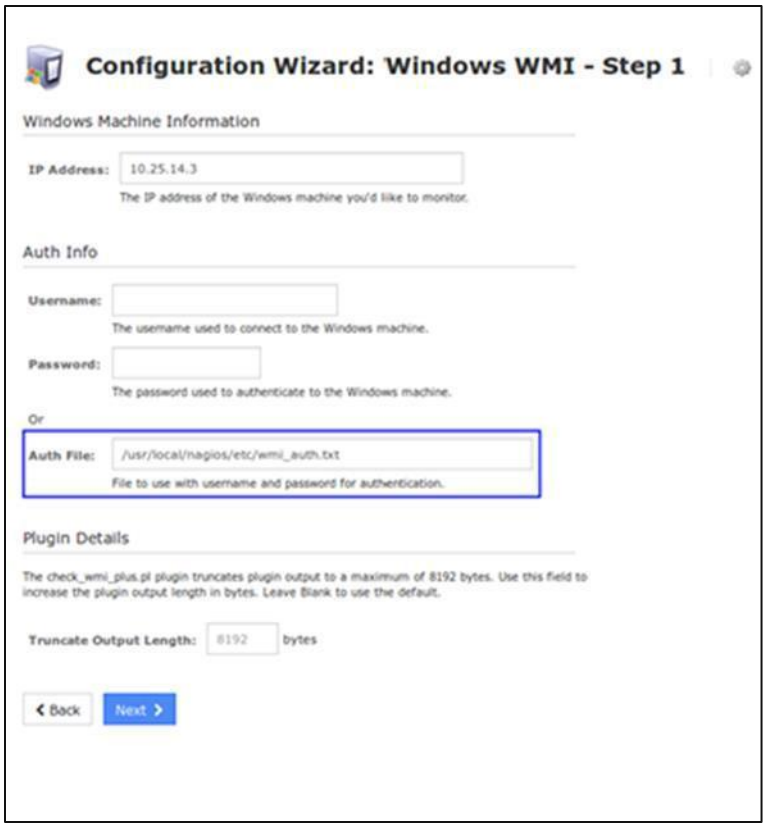
and press **Enter**.

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.

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 works correctly.

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



Troubleshooting

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

Finishing Up

This completes the documentation on how to monitor Windows machines with Nagios XI using Windows Management Instrumentation (WMI). If you have additional questions or other support-related questions, please visit us at our Nagios Support Forum, Nagios Knowledge Base, or Nagios Library:

Visit Nagios Support Forum Visit Nagios Knowledge Base Visit Nagios Library