Why do my APM WMI Monitors Show Status Unknown? ...................................................... 1
WMI Troubleshooting Flowchart for Orion APM 2
Testing Local WMI Services................................. 3
  Test WMI on the Target Server .................. 3
  Reset the WMI Counters ....................... 6
Testing Remote WMI Connectivity ............... 6
  Remotely Test WMI on the Target Server .... 6
  Verify Administrator Credentials .......... 9
  Enable Remote Procedure Call (RPC) ....... 9
  Configure Distributed Component Object
    Model (DCOM) and User Account Control
    (UAC) ................................................. 9
  Add a Windows Firewall Exception for
    Remote WMI Connections .................. 11
Verify APM Component Configuration .......... 12
WMI is Still Not Working, Now What? .......... 12

The following document troubleshoots environmental and connectivity issues that may be preventing Orion APM from retrieving WMI Performance Counter data for monitored nodes, applications, and services.
Why do my APM WMI Monitors Show Status Unknown?

To monitor APM applications containing WMI component monitors, the following conditions must be true:

- WMI on the remote server is enabled and functioning properly.
- The remote server is accessible through a RPC connection in order to run the WMI queries.

If these conditions cannot be met, the WMI component monitors in APM show an Unknown status. Examples of some issues that can prevent these conditions from being met include, but are not limited to:

- Trying to connect to a remote computer where you do not have local Administrator rights.
- A firewall blocking the WMI traffic.
- An operating system that is not configured for WMI.
- Mistyping the credential password in the APM component monitor.

To help diagnose and fix these issues and others, we can test the WMI services, the remote WMI connections, and the Orion APM component configuration to discover and correct the issues that can prevent your WMI component monitors from functioning correctly.

The topics in this guide are as follows:

- **WMI Troubleshooting Flowchart for Orion APM.** Provides a flowchart of the troubleshooting decisions described in this guide.
- **Testing Local WMI Services.** Ensures WMI is running correctly on the target computer.
- **Testing Remote WMI Connections.** Ensures the WMI connection to the target computer is not being blocked, ignored, or rejected.
- **Testing Orion APM Component Configuration.** Ensures you are properly configuring the WMI component credentials in Orion APM.
WMI Troubleshooting Flowchart for Orion APM

TESTING LOCAL WMI SERVICES

Test local WMI

Do you see WMI classes?

Yes

No

Reset WMI counters and retest local WMI

Do you see WMI classes?

Yes

No

Refer to Microsoft Articles

TESTING REMOTE WMI CONNECTIONS

Test remote WMI

Do you see WMI classes?

Yes

No

Are you specifying valid administrator credentials?

Yes

No

Obtain valid administrator credentials

Are DCOM and UAC configured properly?

Yes

No

Configure DCOM and UAC

Is the Windows Firewall disabled, or does it have a WMI exception?

Yes

No

Enable RPC

Is Remote Procedure Call Enabled?

Yes

No

Are DCOM and UAC configured properly?

Yes

No

Configure DCOM and UAC

Disable Windows Firewall or configure firewall exception

TESTING ORION APM COMPONENT CONFIGURATION

Are APM component credentials valid?

Yes

No

Refers to Thwack

Fix APM component credentials.

Did that fix your problem?

No

Refer to Thwack

Yes

Success
Testing Local WMI Services

Testing the local WMI services helps us isolate any faults on the target server we are trying to monitor. The testing program is a Microsoft program named WBEMTest that comes already installed on Microsoft Windows operating systems.

**Test WMI on the Target Server**

Complete the following procedure to check whether WMI on the target server is functioning correctly:

1. Log on to the target server with an administrator account.
2. Click **Start > Run**, enter `wbemtest.exe` and then click **OK**.
3. Click **Connect** on the Windows Management Instrumentation Tester window.
4. Enter `root\cimv2` in the field at the top of the dialog box next to the **Connect** button.

5. Click **Connect**.

6. Click **Enum Classes**.
8. Select the **Recursive** radio button without entering a superclass name, and then click **OK**.

9. **If the WMI class you are querying appears in this list**, local WMI services are functioning correctly. Skip to the next topic and test remote WMI.

10. **If the list does not appear or does not contain the desired WMI class**, WMI is not functioning correctly. Continue reading this section for guidance on repairing WMI services on the target server.

11. Click the **Close** button, and then click **Exit**.
**Reset the WMI Counters**

At times, the WMI performance counters may not get transferred to WMI because services were delayed or started out of order ([http://support.microsoft.com/kb/820847](http://support.microsoft.com/kb/820847)).

To manually reset the WMI counters:

1. Stop the Windows Management Instrumentation service.
2. Click Start, click Run, type cmd, and then click OK.
3. At the command prompt, type `winmgmt /resyncperf`, and then press ENTER.
4. At the command prompt, type `wmiadap.exe /f`, and then press ENTER.
5. Type `exit`, and then press ENTER to close the command prompt.

After resetting the WMI counters, retest WMI. If resetting the WMI counters did not solve your problem, see “WMI is Still Not Working, Now What?” on page 12.

**Testing Remote WMI Connectivity**

Testing the remote WMI connectivity of the target server helps us isolate faults that could prevent the target server from receiving or responding to our remote WMI requests. The testing program is a Microsoft program named WBEMTest that comes already installed on Microsoft Windows operating systems.

**Remotely Test WMI on the Target Server**

Complete the following procedure to check whether the target server is responding appropriately to remote WMI requests that originate from the Orion APM server:

1. Log on to the Orion APM server with an administrator account.
2. Click Start > Run, enter `wbemtest.exe` and then click OK.
3. Click Connect on the Windows Management Instrumentation Tester window.
4. Enter `\Target_Primary_IP_Address\root\cimv2` in the field at the top of the dialog box. Replace `Target_Primary_IP_Address` in the above example with the actual Hostname or Primary IP Address of the target server.

5. Enter the user name in the **User** field, the password in the **Password** field, and `NTLMDOMAIN:NameOfDomain` in the **Authority** field. Replace `NameOfDomain` with the domain of the user account specified in the User field.

6. Click **Connect**.

7. Click **Enum Classes**.
8. Select the Recursive radio button without entering a superclass name, and then click OK.

9. If the WMI class list appears, remote WMI is functioning correctly. Skip to the next topic and test your APM credentials.
10. **If the list does not appear**, remote WMI is not functioning correctly. Continue reading this topic for guidance on restoring remote WMI connections on the target server, and retest remote WMI after completing each troubleshooting step.

11. Click the **Close** button, and then click **Exit**.

**Verify Administrator Credentials**

Only a credential that has administrator rights on the target server has the necessary permissions to access the target server's WMI services. Make sure that the username and password you are using belongs to an administrator on the target server.

If the administrator credential is a domain member, be sure to specify both the user name and the domain in the standard Microsoft syntax. For example: `DOMAIN\Administrator`.

**Enable Remote Procedure Call (RPC)**

Remote WMI connections use RPC as a communications interface. If the RPC service is disabled on the target server, remote WMI connections cannot be established.

**To enable the RPC service:**

1. Log on to the target server with an administrator account.
2. Click **Start**, click **Run**, type `services.msc`, and then press **ENTER**.
3. Scroll the list to **Remote Procedure Call (RPC)**.
4. Right-click **Remote Procedure Call (RPC)**, and then click **Start** on the shortcut menu.

**Configure Distributed Component Object Model (DCOM) and User Account Control (UAC)**


<table>
<thead>
<tr>
<th>Item</th>
<th>Need</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DCOM</strong></td>
<td>Default and Limits permissions edited to allow the following actions:</td>
</tr>
<tr>
<td></td>
<td>• Local launch (default permission)</td>
</tr>
<tr>
<td></td>
<td>• Remote launch (default permission)</td>
</tr>
<tr>
<td></td>
<td>• Local activation (limits permission)</td>
</tr>
<tr>
<td></td>
<td>• Remote activation (limits permission)</td>
</tr>
<tr>
<td></td>
<td>For more information, see “Enabling DCOM” on page 10.</td>
</tr>
<tr>
<td><strong>WMI Namespaces</strong></td>
<td>Modify the CIMV2 security to enable and remote enable the account used to access the server or workstation through WMI. You must ensure the security change applies to the current namespace and subnamespaces. For more information, see “Enabling Account Privileges in WMI” on page 10.</td>
</tr>
<tr>
<td><strong>User Account Control</strong></td>
<td>Remote UAC access token filtering must be disabled when monitoring within a workgroup environment. For more information, see “Disabling Remote User Account Control for Workgroups” on page 11.</td>
</tr>
</tbody>
</table>
Enabling DCOM

WMI uses DCOM to communicate with monitored target computers. Therefore, for Application Performance Monitor to use WMI, DCOM must be enabled and properly configured.

To enable DCOM permissions for your Application Performance Monitor credentials:

1. Log on to the target server with an administrator account.
2. Navigate to Start > Control Panel > Administrative Tools > Component Services. You need to switch to the Classic View of the Control Panel to use this navigation path. You can also launch this console by double-clicking comexp.msc in the /windows/system32 directory.
4. Right-click My Computer, and then select Properties.
5. Select the COM Security tab, and then click Edit Limits in the Access Permissions grouping.
6. Ensure the user account you want to use to collect WMI statistics has Local Access and Remote Access, and then click OK.
7. Click Edit Default, and then ensure the user account you want to use to collect WMI statistics has Local Access and Remote Access.
8. Click OK.
9. Click Edit Limits in the Launch and Activation Permissions grouping.
10. Ensure the user account you want to use to collect WMI statistics has Local Launch, Remote Launch, Local Activation, and Remote Activation, and then click OK.
11. Click Edit Default, and then ensure the user account you want to use to collect WMI statistics has Local Launch, Remote Launch, Local Activation, and Remote Activation.
12. Click OK.

Enabling Account Privileges in WMI

The account you specify in the Credentials Library must possess security access to the namespace and subnamespaces of the monitored target computer. To enable these privileges, complete the following procedure.

To enable namespace and subnamespaces privileges:

1. Log on to the computer you want to monitor with an administrator account.
2. Navigate to Start > Control Panel > Administrative Tools > Computer Management > Services and Applications. You need to switch to the Classic View of the Control Panel to use this navigation path.
3. Click WMI Control, and then right-click and select Properties.
4. Select the Security tab, and then expand Root and click CIMV2.
5. Click Security and then select the user account used to access this computer and ensure you grant the following permissions:
   a. Enable Account
   b. Remote Enable
6. Click Advanced, and then select the user account used to access this computer.
7. Click Edit, select This namespace and subnamespaces in the Apply to field, and then click OK.
8. Click OK on the Advanced Security Settings for CIMV2 window.

9. Click OK on the Security for Root\CIMV2 window.

10. Click Services in the left navigation pane of Computer Management.

11. Select Windows Management Instrumentation in the Services result pane, and then click Restart.

Disabling Remote User Account Control for Workgroups

If you are monitoring a target in a workgroup, you need to disable remote User Account Control (UAC). This is not recommended, but it is necessary when monitoring a workgroup computer. Disabling remote user account control does not disable local user account control functionality.

Warning: The following procedure requires the modification or creation of a registry key. Changing the registry can have adverse effects on your computer and may result in an unbootable system. Consider backing up your registry before making these changes.

To disable remote UAC for a workgroup computer:

1. Log on to the computer you want to monitor with an administrator account.

2. Click Start > Accessories > Command Prompt.

3. Enter regedit.

4. Expand HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System.

5. Locate or create a DWORD entry named LocalAccountTokenFilterPolicy and provide a DWORD value of 1.

   Note: To re-enable remote UAC, change this value to 0.

Add a Windows Firewall Exception for Remote WMI Connections

If the target computer has Windows Firewall enabled, it must have a Remote WMI exception to allow remote WMI traffic through (http://msdn.microsoft.com/en-us/library/aa389286(VS.85).aspx). To add this exception:

1. Click Start, click Run, type cmd and then press ENTER.

2. At the command prompt, type netsh firewall set service RemoteAdmin enable, and then press ENTER.

3. At the command prompt, type exit, and then press ENTER.

If adding the firewall exception did not solve your problem, see “WMI is Still Not Working, Now What?” on page 12.
Verify APM Component Configuration

Make sure that the credential you are using for remote WMI is the same credential that you are using in the APM component.

After you click Set Component Credentials to set the component credentials, you must also click Submit at the bottom of the page.

WMI is Still Not Working, Now What?

This guide depicts only the most common scenarios that can cause WMI services to fail. If you are unable to get WMI services to work by this point, it is time to consult the Microsoft articles on this topic.

