SOLARWINDS

NETWORK MANAGEMENT SOLUTIONS

Configuring WMI on Windows Vista and Windows Server 2008 for Application Performance Monitor

Revised 1/22/2008

By default, WMI is not enabled on Windows Vista and Windows Server 2008. The following document provides the required steps to ensure WMI is enabled on these operating systems.

Legal

Requirements

The following items must be secured before attempting to monitor a target application server with Application Performance Monitor WMI monitors.

Item	Need
User Account	Depending on your implementation, supply one of the following as credentials for the APM credentials database: • For domain-based authentication, a domain account with membership in the Administrators group on the monitored application server • For workgroup authentication, a local user account with membership in the Administrators group on the monitored application server For more information, see “Checking Application Performance Monitor Credentials Group Memberships” on page 1.
DCOM	Default and Limits permissions edited to allow the following actions: • Local launch (default permission) • Remote launch (default permission) • Local activation (limits permission) • Remote activation (limits permission) For more information, see “Enabling DCOM” on page 2.
WMI Namespaces	Modify the SIMV2 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 subnamepaces. For more information, see “Enabling Account Privileges in WMI” on page 3.
Windows Firewall	Ensure Windows Management Instrumentation (WMI) traffic can traverse the firewall. For more information, see “Allowing WMI through the Windows Firewall” on page 4.
User Account Control	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 4.

Checking Application Performance Monitor Credentials Group Memberships

Whether you are monitoring a Microsoft Vista Workstation or a server running Windows Server 2008, complete the following procedure to ensure the account specified in the Credentials Library has the appropriate permissions.

To add your monitor account to the local administrator group of a Vista or Server 2008 computer:

1. Log on to the computer you want to monitor with an administrator account.
2. Navigate to **Start > Control Panel > Administrative Tools > Computer Management > Local Users and Groups > Groups**. You need to switch to the Classic View of the Control Panel to use this navigation path.

3. Right-click **Administrators**, and then click **Add to group**.
4. ***If the account you want to use is not currently a member of this group,*** complete the following procedure:
   a. Click **Add** on the Administrators Properties window.
   b. Type the name of the account you want to use to gather WMI statistics, and then click **OK**. This is the account you specify in the Credentials Library of Application Performance Monitor.

      Note: If you are adding an account to a workgroup computer, you cannot add a domain account. You must use a local account.
5. Click **OK** on the Administrators Properties window, and then close the Computer Management window.

Ensuring the Correct Application Performance Monitor Credentials Syntax

When you specify an account for Application Performance Monitor to use for a WMI monitor, you add that account to the Application Performance Monitor Credentials Library. If the target to monitor is a member of a domain, specify the username of the credentials set as `domainName\userName`. If the target to monitor is a member of a workgroup, specify the username of the credentials set as `userName`.

To add an account to the Credentials Library:

1. Log on to the Orion Server with an administrator account.
2. Launch the Web Console.
3. Specify an Admin account and log on to the Orion Web Console.
4. Click **Application Performance Monitor** in the Modules toolbar.
5. Click **APM Settings**.
6. Click **Credentials Library**.
7. Click **Add New Credential**.
8. Provide a friendly name for the credential set. Application Performance Monitor displays this name in the **Credential for Monitoring** field of monitors that accept credentials.
9. Provide the user name and password, and then confirm the password and click **Submit**.

   Note: If you are providing windows credentials for accessing and harvesting information through WMI, ensure you provide the credentials in the following syntax: `domainName\userName` for domain credentials or `userName` for workgroup credentials.

Enabling DCOM

Windows Management Instrumentation (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 computer you want to monitor 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.

3. Expand **Component Services > Computers**.
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 `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:
   - `Enable Account`
   - `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**.

Allowing WMI through the Windows Firewall

You must allow WMI traffic through the firewall of the monitored application server. The following procedure walks you through allowing WMI through the Windows Firewall.

To allow WMI traffic through the Windows Firewall:

1. Log on to the computer you want to monitor with an administrator account.
2. Navigate to **Start > Control Panel > Security Center**. You need to switch to the Classic View of the Control Panel to use this navigation path.
3. Click **Windows Firewall** in the left navigation pane.
4. Click **Allow a program through Windows Firewall** in the left navigation pane.
5. Check **Windows Management Instumentation (WMI)**, and then click **OK**.

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`.