Windows Management Instrumentation (WMI) firewall rule

Question

Your network contains two servers named ServerA and ServerB that run Windows Server 2012 R2. ServerA and ServerB are part of a workgroup.
On Servera and ServerB, you create a local user account named Helpdesk1. You add the account to the local Administrators group. On both servers, Helpdesk1 has the same password.
You log on to Server1 as Helpdesk1.You open Computer Management and connect to ServerB. When you attempt to create a scheduled task, view the event logs, and manage the shared folders, you receive Access Denied messages.

You need to ensure that you can administer ServerB remotely from ServerA by using Computer Management.

Wwhat should you configure on ServerB.

Enable WMI (Windows Management Instrumentation)

WMI comes installed on all of Microsoft's modern operating systems (Windows 2000, Windows XP, Windows 2003, Windows Vista and Windows 2008[1]). What this page will describe is how to enable ***remote access*** to WMI. The following steps should only take a minute or two of your time.

1. Enable remote WMI requests

This setting is usually all that needs to be changed to get WMI working. (Steps 2 and 3 are typically not needed, but they might be in some circumstances)

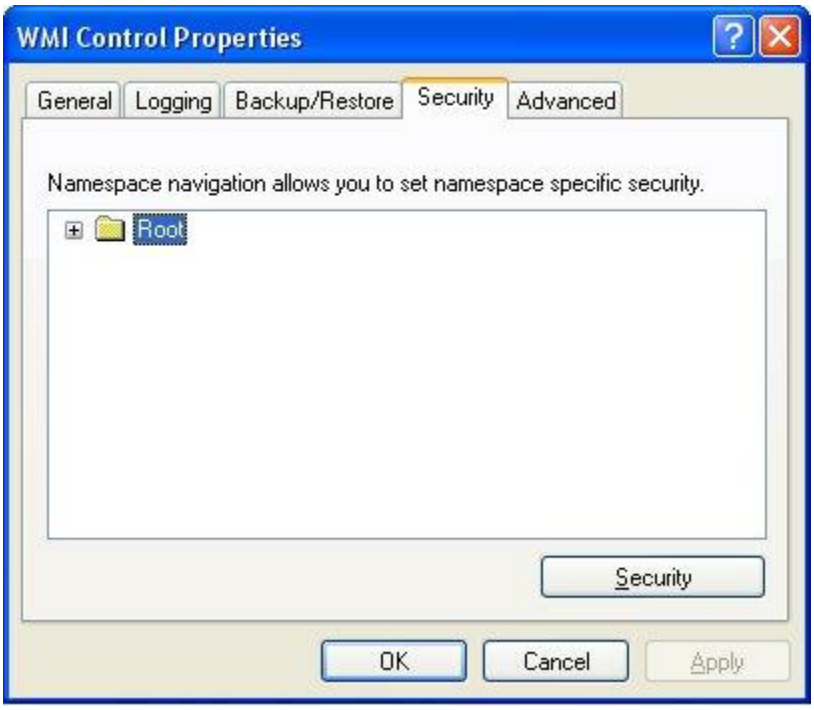
1. On the target server, go to Administrative Tools -> Computer Management.

2. Expand 'Services and Applications'

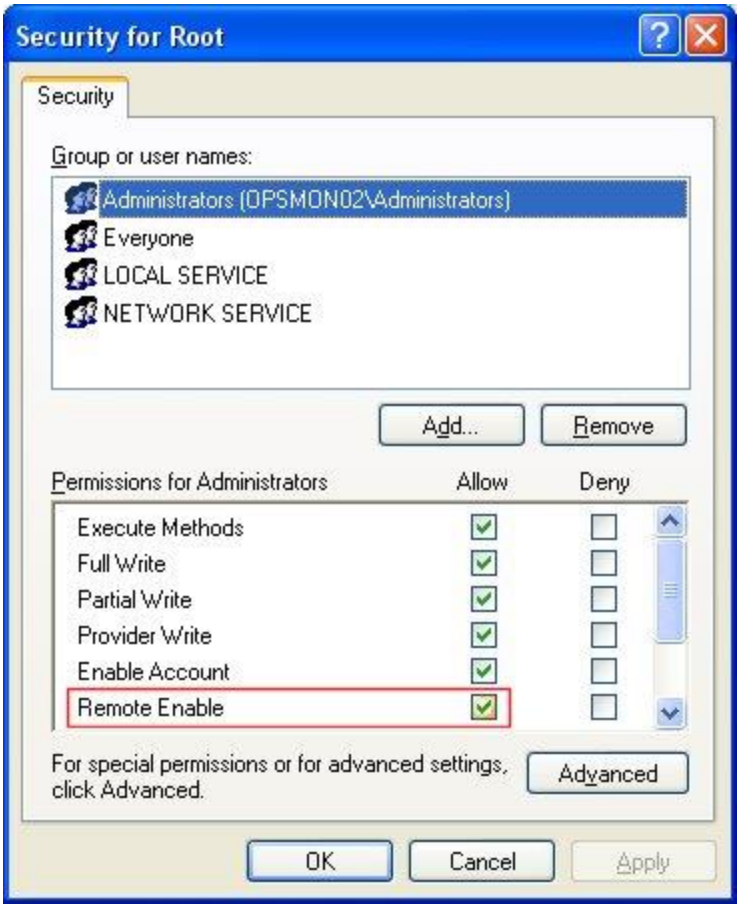
3. Right click for Properties on 'WMI Control'.

4. Select the Security tab

5. Press the Security button



6. Add the monitoring user (if needed), and then be sure to check Remote Enable for the user/group that will be requesting WMI data.



At this point go back and see if this fixes the problem. It might take a couple of minutes for the reports to re-generate.

2. Allow WMI through Windows firewall

All users (including non-administrators) are able to query/read WMI data on the local computer.

For reading WMI data on a remote server, a connection needs to be made from your management computer (where our monitoring software is installed) to the server that you're monitoring (the target server). If the target server is running Windows Firewall (aka Internet Connection Firewall) like what is shipped with Windows XP and Windows 2003, then you need to tell it to let remote WMI requests through[2]. This can only be done at the command prompt. Run the following on the target computer if it is running a Windows firewall:

```
netsh firewall set service RemoteAdmin enable
```

3. Enable DCOM calls on the remote machine

If the account you are using to monitor the target server is NOT an administrator on the target server, you need to enable the non-administrator to interact with DCOM by following the simple steps listed here. Follow the steps for:

- To grant DCOM remote launch and activation permissions for a user or group
- To grant DCOM remote access permissions

Further Investigation

If the above steps didn't help, we recommend installing the WMI Administrative Tools from Microsoft. This includes a WMI browser that will let you connect to a remote machine and browse through the WMI information. That will help to isolate any connectivity/rights issues in a more direct and simple environment. Once the WMI browser can access a remote machine, our products should be able to as well.

WMI Administrative Tools:
http://www.microsoft.com/downloads/details.aspx?FamilyId=6430F853-1120-48DB-8CC5-F2ABDC3ED314&displaylang=en

Finally, UAC

From reports we're receiving from the field, it appears UAC needs to be disabled for remote WMI queries to work. With UAC running, an administrator account actually has two security tokens, a normal user token, and an administrator token (which is only activated when you pass the UAC prompt). Unfortunately, remote requests that come in over the network get the normal user token for the administrator, and since there is no way to handle a UAC prompt remotely, the token can't be elevated to the true-administrator security token.

Server Manager console uses Windows Management Instrumentation (WMI) for remote administration. Connecting to WMI remotely requires that you configure the Windows Firewall to allow network connections to WMI on the remote computer. This article describes how to configure the Windows Firewall to enable Remote Administration in various environments.

Incorrect Windows Firewall settings are usually identified by receiving the **"RPC Server Unavailable"** error message when trying to remotely connect to the Server using the management console:

Windows Firewall configuration should be done locally on the server by the user with administrator rights. While Windows Firewall can be configured using the Control Panel, you may find it easier to use the **netsh** command lines. Appropriate command lines for the most widely used Windows versions are listed below.

Windows XP/Windows Server 2003

For Windows XP/Windows Server 2003 use following command at the system prompt:
netsh firewall set service RemoteAdmin enable

If you would rather use the Group Policy editor than the **netsh** commands above, use the following steps in the Group Policy editor (Gpedit.msc) to enable "Allow Remote Administration" on the server:

1. Under the **Local Computer Policy** heading, double-click **Computer Configuration**.
2. Double-click **Administrative Templates** > **Network** > **Network Connections** > **Windows Firewall**.
3. If the computer is in the domain, then double-click **Domain Profile**; otherwise, double-click **Standard Profile**.
4. Click **Windows Firewall: Allow remote administration exception**.
5. On the **Action** menu, select **Properties**.
6. Click **Enable**, and then click **OK**.

Windows Vista/Windows Server 2008

For Windows Vista/Windows Server 2008 use following command at the system prompt:
netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes

⚠
Note On Windows Vista and Windows Server 2008 operating systems the mentioned command line should be executed in the *elevated command prompt*.

If you would rather use the Firewall UI than the **netsh** commands above, use the following steps on the server:

1. In the **Control Panel**, click **Security** and then click **Windows Firewall**.
2. Click **Change Settings**, and then click the **Exceptions** tab.
3. In the Exceptions window, select the check box for **Windows Management Instrumentation (WMI)** to enable WMI traffic through the firewall. To disable WMI traffic, clear the check box.

Enabling remote management – windows powershell

http://blogs.technet.com/b/bruce_adamczak/archive/2013/02/10/windows-2012-core-survival-guide-powershell-remote-management.aspx