Troubleshoot WMI connectivity issues

In order to use WMI, the user account under which the Collection Service runs must have administrator permissions on the remote server. The most frequently encountered problems with WMI relate to RPC traffic failing to get through to the remote computer. Another issue involves DCOM/WMI permissions.

The following links provide additional information about how to troubleshoot WMI connectivity issues:

- Securing a remote WMI connection
- Help with Scripts

Using WbemTest (Windows Management Instrumentation Tester)

You can use the WbemTest tool to connect to a server and issue WMI queries. Download this tool from Microsoft TechNet to help you test and troubleshoot WMI issues.

To use WbemTest:

1. Run `wbemtest.exe`.
2. Click **Connect**.
3. In the **NameSpace text** box, enter **\\server\root\cimv2** where server is the name of the server to which you want to connect.
4. Click **Connect**.
5. Click **Query**.
6. Enter **select** * from win32_process.
7. Click **Apply**.

If WbemTest connects to the remote server and issues the query using WMI, you should see a query result with output. In this case, WMI to the required server is working and no further action is needed. For more information on the Windows Management Instrumentation Tester, refer to the Microsoft document,Windows Management Instrumentation Tester overview.

If you receive an error message, use the following processes to help identify and resolve the issue.

Error: The RPC Server Is Unavailable

This error usually indicates that the RPC traffic is not getting to the remote server, or there is no RPC listener on the remote server.

To troubleshoot this RPC error:

1. Make sure that the Remote Procedure Call (RPC) service is running on the remote server.
2. Verify that there is a TCP listener on the remote server by running the netstat -nao command and verifying that there is the following entry: `TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 1304`
3. In the Tools subdirectory, run `rpcping /s <servername> /t ncacn_ip_tcp` where `<servername>` is the name of the remote server. This command verifies that RPC can communicate with the remote server and output similar to:
   ```
   Completed 1 calls in 15 ms
   66 T/S or 15.000 ms/T
   ```
4. Make sure that local or internal network firewalls do not block traffic by either disabling the firewall or configuring the Windows firewall to allow incoming RPC traffic.
5. Try to use the remote server IP address instead of the server name. If the IP address works, you may have a DNS issue.
6. If the remote server resides in a different domain, the two domains may not trust each other, or the user account does not have administrator permissions on the remote server/domain.
7. If both computers are in the same domain, and the user account has administrator permissions, try rejoining both computers to the domain.

Error: Access Denied

This error can indicate permission issues.

To troubleshoot this access error:

1. If the remote computer is running Windows XP, make sure it is not set to Force Guest. This setting forces impersonation of any connection as Guest.
   a. Open the Local Security Policy console from Administrative Tools.
   b. Browse to **Security Settings > Local Policies > Security Options** .
   c. Double-click Network Access: Sharing And Security Model For LocalAccounts.
   d. Change the settings from `Guest Only` to Classic.
2. Make sure DCOM is enabled on the remote server:
   a. Run `DcomCnfg` on the remote server.
   b. Click **Component Services**.
   c. Expand **Computers**.
   d. Right click **My Computer** and select **Properties**.
   e. Click the **Default Properties** tab.
   f. Make sure **Enable Distributed COM** on this computer is checked.
3. Verify the configuration of the correct DCOM remote launch and activation permissions:
   a. Run `DcomCnfg` on the remote server.
   b. Click **Component Services**.

c. Expand **Computers**.
d. Right click **My Computer** and select **Properties**.
e. Make sure **Enable Distributed COM** on this computer is checked.
f. Click the **Com Security** tab.
g. Under **Launch and Activation Permissions**, click **Edit Limits**.
h. In the Launch Permissions dialog box, make sure your user account or group is listed in the Groups or user names list. If your user account or group is not listed, click **Add** and add it to the list.
i. In the Launch Permission dialog box, select your user account or group in the Group or user names list. In the Allow column under Permissions for User, select **Remote Launch** and **Remote Activation**, and then click **OK**.

4. Make sure the correct DCOM remote access permissions are configured:
   a. Run `DcomCnfg` on the remote server.
   b. Click **Component Services**.
   c. Expand **Computers**.
   d. Right click **My Computer** and select **Properties**.
   e. Make sure **Enable Distributed COM** on this computer is checked.
   f. Click the **Com Security** tab.
   g. Under **Access Permissions** , click **Edit Limits**.
   h. In the Access Permission dialog box, select `ANONYMOUS LOGON` name in the Group or user names list. In the Allow column under Permissions for User, select **Remote Access**, and then click **OK**.
5. Make sure the correct WMI namespace permissions are configured.
   a. On the target machine, run `wmimgmt.msc`.
   b. Right-click **WMI Control**, and then select **Properties**.
   c. In the Security tab, select the CIMV2 namespace, and then click **Security**.
   d. Locate the appropriate account, and then check **Remote Enable** in the Permissions list.

SQL Diagnostic Manager identifies and resolves SQL Server performance problems before they happen. Learn more > >

IDERA Website	Products	Purchase	Support	Community	About Us	Resources	Legal