Troubleshooting WMI connectivity issues

The user account used by IDERA SQL Secure to gather Operation System and Active Directory objects must have administrator permissions on the remote server to be able to use WMI.

The most frequently encountered problems with WMI connectivity are:

- RPC traffic not getting through to the remote computer
- Invalid DCOM or WMI permissions
- Ports are not open or firewall is preventing access

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

- Securing a remote WMI Connection
- Help with Scripts

Resolve WMI Issues using WbemTest

You can use the WbemTest (Windows Management Instrumentation Tester) tool to connect to a server and issue WMI queries. Download this tool from Microsoft TechNet. This tool can help you test and troubleshoot WMI issues.

To use WbemTest:

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

If WbemTest was able to connect to the remote server and issue 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 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. Ensure 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 sub-directory, run `rpcping /s <servername> /t ncacn_tp_tcp` where `<servername>` is the name of the remote server. This command verifies that RPC can communicate with the remote server. The output should be similar to:
    - `Completed 1 calls in 15 ms`
    - `66 T/S or 15.000 ms/T`
4. Ensure that the traffic is not being blocked by local or internal network firewalls. Either disable the firewall or configure 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 being used 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 Force Guest is disabled. This setting forces any connection to be impersonated 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. Ensure that 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. Ensure **Enable Distributed COM** on this computer is checked.
3. Ensure the correct DCOM remote launch and activation 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. Ensure **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. Ensure 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. Ensure **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. Ensure the correct WMI namespace permissions are configured.
   a. Run `wmimgmt.msc`.
   b. Right-click **WMI Control**, and then select **Connect to another computer**.
   c. Enter the remote server name, and then click **OK**.
   d. Right-click **WMI Control**, and then select **Properties**.
   e. In the Security tab, select the namespace, and then click **Security**.
   f. Locate the appropriate account, and then check **Remote Enable** in the Permissions list.

Warning: The Network Path Was Not Found

This warning typically indicates that SQL Secure cannot access the target computer due to closed ports or firewall access settings. Ensure the appropriate port is open on the target computer and check your firewall configuration.

SQL Secure uses the default ports opened by the Windows operating system for local and remote communications. To learn about Windows port assignments, see Article 832017 on the Microsoft Support site. To better understand how port assignments work when Windows Firewall has been configured, see "Connecting Through Windows Firewall" on the MSDN site.