Troubleshooting Remote Registry Read Problems During Environment Discoveries And Refreshes (KBA1552)

KBA
KBA#1552

Applicable Delphix Engine Versions
Click here to view the versions of the Delphix engine to which this article applies

Issue

During MSSQL Server environment discovery and refresh operations it can be necessary for the Delphix Connector host to run a Powershell command to remotely read the intended environment's registry to discover information about nodes and MSSQL Server instances.

You might encounter an error like this:

```
OpenRemoteBaseKey : Exception calling "OpenRemoteBaseKey" with "2" argument(s):
  "The network path was not found."
At D:\Delphix\DelphixConnector\discovery\420151e5-83e3-3bd5-6c70-ec480410062f-WINDOWS_CLUSTER-15\InstanceDiscovery.ps1:64 char:64
  $rootkey = [Microsoft.Win32.RegistryKey]::OpenRemoteBaseKey("LocalMachine", $sourceAddress)
+ CategoryInfo : NotSpecified: (:) [], MethodInvocationException
+ FullyQualifiedErrorId : DotNetMethodException
```

die : Error: ERROR_OPEN_ROOT_KEY
At D:\Delphix\DelphixConnector\discovery\420151e5-83e3-3bd5-6c70-ec480410062f-WINDOWS_CLUSTER-15\InstanceDiscovery.ps1:68 char:8
  die "ERROR_OPEN_ROOT_KEY"
+ CategoryInfo : NotSpecified: ([Write-Error], WriteErrorException)
+ FullyQualifiedErrorId : Microsoft.PowerShell.Commands.WriteErrorException,die

This can manifest as error or warning depending on what context, what is being queried.

Troubleshooting

There are a few things to check:
Remote Registry service

On the remote host, there is a Remote Registry service to check. You can start the Windows Services list GUI with the command `Services.msc`, or you can click the Services icon from the Administrative Tools group icon from Control Panel:

- The third column is startup type - make sure it is set to automatic. It's a "Trigger Start" so don't worry if not running, it'll start again when a query is made remotely to the registry. However, you can start it for the purposes of testing. If Disabled or set to Manual and not in started state, please start to test.

Registry permissions

If the windows service isn't the issue make sure the permissions on the windows host registry itself are adequate for reading by the Delphix OS (operating system) user designated for the Source environment discovery. You can check this by opening the `regedit.exe` utility on the remote windows host (source host), and under the Edit menu open Permissions. The Delphix OS user must have at least Read permissions for them to query (read) the registry.

- You can easily test remote read access from the DelphixConnector host, as the Delphix OS user for the source host, by opening regedit.exe, select from the menu File and select Connect Network Registry... and enter the name of the source host for the connection.

- If read access is available you'll be able to successfully navigate the registry keys. If not, you'll need administrative assistance to grant the necessary Read permissions to the user for this access.

Network connectivity

If the service and permissions aren't the issue, then you need to start troubleshooting the port 445, which provides inbound access to the remote registry service on the remote host. You'll want to run some generic Powershell commands in order to test remote registry access from the DelphixConnector host.

I recommend running these Powershell commands from powershell console or ISE:

- To test the ability to check port 445 is open on the target side from Windows host running DelphixConnector use this powershell command. Please note, if the remote host is a cluster, use the cluster address to test (the hostname/ip address used in the environment discovery):
In this case, port 445 is unreachable from this Windows host

- For general host access (yes, sometimes this can be the issue, especially in cluster setups), use this command to check that the host itself is reachable if you haven’t already tested using nslookup or other commands. This PowerShell command is typically used by our current Delphix installations:

```powershell
PS C:\windows\system32> [system.net.dns]::GetHostEntry("RemoteHost.com")
```

### HostName Aliases AddressList
-------- ------- -----------
RemoteHost.com {} (10.100.30.100)

You can run this and previous command from connector host to the remote host and in the case clusters are involved against the individual cluster nodes and also cluster address to pinpoint and isolate where problem occurs.

- You can also run this command to test remote registry access as it is called from our powershell scripts:

```powershell
[Microsoft.Win32.RegistryKey]::OpenRemoteBaseKey("LocalMachine", "RemoteHost.com")
```

<table>
<thead>
<tr>
<th>SubKeyCount</th>
<th>View</th>
<th>Handle</th>
<th>ValueCount</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Default</td>
<td>Microsoft.Win32.SafeHandles.SafeRegistryHandle</td>
<td>0</td>
<td>HKEY_LOCAL_MACHINE</td>
</tr>
</tbody>
</table>

An error presents itself similar to how we see it from the cluster discovery.

Keep in mind testing using OpenRemoteBaseKey is more for user access to the registry, whereas the TcpClient class is testing access to the remote system’s listener port 445, which among other things provides access to remote registry reading. But, OpenRemoteBaseKey can fail for network reasons - when calling it in powershell, if the issue is network related (hostname has no access to the registry), the error will throw after about one minute. If it is a permission issue local on the machine, the error is throw almost immediately.

**Membership of Backup Operators group**

Some failures will present a “requested registry access is not allowed” error, instead of the “network path was not found”
error described above:

```
Exception calling "OpenSubKey" with "1" argument(s): "Requested registry access is not allowed."
At C:\Program Files\Delphix\DelphixConnector\564de705-c619-fbf4-6c5c-c1f815f5e816-staging-1352\SCRIPT\GetInstancePort.ps1:97 char:1
+ $sqlServerKey = $rootkey.OpenSubKey("SOFTWARE\Microsoft\Microsoft SQL Server")
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
+ CategoryInfo     : NotSpecified: (:) [], MethodInvocationException
+ FullyQualifiedErrorId : SecurityException
```

This suggests that the configured Environment User for this Environment is not a member of the Windows "Backup Operators" group. On Windows Clusters, this group membership should be configured on every Cluster node.

---

**Resolution**

There are various resolutions based on the nature of the problem which are mostly environment related:

**Access Denied type issue**

- Provide the user with the necessary rights

**Host Access**

- Based on analysis, if there are issues accessing the host due to DNS or similar issues, then this is handled by the customer admins. Use the `nslookup` and `GetHostEntry` commands to determine this.

**Port 445 listener**

- This can be blocked by firewall and we discover, one weird obscure way. Naturally, have customer check the firewalls to make sure the port isn't blocked. Since it is used for SMB (Server Message Block protocol) the port handles access to sharing of files, printers and other communications across the network, basically remote access. Remote read registry access is part of this family. If not blocked by firewall or other network apparatus, please check the Network Adapter's properties on the remote host and check that "File and Printer Sharing for Microsoft Networks" is enabled. Port 445 can be open on the firewall but disabling this network adapter property can cause this sort of grief.

To get to this property, from the Windows Control Panel, open the Network (and Internet) section/icon, and under the list of Network Connections open the adapter that is used for the network between remote host and DelphixConnector host. Right click the adapter and select Properties and the mentioned property should appear on the list and needs to be enabled for the 445 port to be listening. The property "Client for Microsoft Networks" might also need to be enabled.

You can also shortcut to the Network Connections running this command from command line: `control ncpa.cpl`

This is an example of a Network adapter properties list:
Obscure Issues

- One obscure issue was related to this URL (from windows 2000 to windows XP upgrade, though not the same, the resolution was the same):

  **Remote Registry Access error**: HKEY_LOCAL_MACHINE cannot be opened. An error is preventing the key from being opened.

  The "LOCAL SERVICE" account was added to the specified key on the remote machine (Source environment) and READ permissions applied and access issue was resolved. The key of interest: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg**

  On that key right click and select permissions and Add "LOCAL SERVICE". Check the READ permission as seen here:
Permissions for winreg

Security

Group or user names:
- LOCAL SERVICE
- Administrators (10-43-13-221\Administrators)
- Backup Operators (10-43-13-221\Backup Operators)

Add...  Remove

Permissions for LOCAL SERVICE  Allow  Deny
- Full Control
- Read  
- Special permissions

For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

OK  Cancel  Apply