Cannot access resource when browsing SQL Servers with Windows authentication

If you are using Windows authentication to connect to a SQL Server through the SQL Backup Pro graphical user interface and try to access a network share through the Folder Browser or File Browser, you may encounter the following error:

> Cannot access resource. Check that you have the correct permissions to view this resource.

This is caused by Windows security restrictions that prevent a "double hop" of credentials from one server to another, using an intermediate server. There are two possible solutions to this problem:

- Browsing network shares using the SQL Backup Agent service startup account
- Chaning the Windows authentication method to Kerberos

Browsing network shares using the SQL Backup Agent service startup account

This solution is only available if the SQL Backup Agent service startup account (the account the service logs on as) is a domain account with access to the network resources.

The SQL Backup Agent service is created for each SQL Server instance when you install the SQL Backup Pro server components. The name of the service is in the format: *SQL Backup Agent-<instance name>* You can change the account the service uses to log on from the Windows Services panel.

To allow a user to browse a network share using the SQL Backup Agent service startup account:

1. Open Registry Editor (regedit.exe).
2. Navigate to the following registry key:
   HKEY_LOCAL_MACHINE\SOFTWARE\Red Gate\SQL Backup\BackupSettingsGlobal\<instance>
   where *<instance>* is the SQL Server you are connecting to through the SQL Backup Pro GUI.
3. Create a Multi-String Value entry called *BrowsingUserList*.
4. In the Value data, list each of the Windows users that you want to allow to browse the network shares using the SQL Backup Agent service startup account. Each user should be listed on a new line in the format *DOMAIN\USER*.

Changing the Windows authentication method to Kerberos

This solution is only available if you have domain administrator privileges and access to the **Active Directory Users and Computers** applet on the Windows Active Directory server containing the computer account.

To change the Windows authentication method from NTLM to Kerberos you need to register a Service Principal Name for the SQL Server Service, then use Active Directory to trust the computer and any accounts for delegation.

Registering a Service Principal Name

To register a Service Principal name for the SQL Server service:

1. Ensure the server has a fully-qualified DNS entry, by pinging the IP address of the machine. (You can use *ipconfig* to get the IP address.)

   ```
   ping -a <IP address>
   ```

   The ping should return a full-qualified domain name for the server. If it does not, contact your network administrator to get the server added to your network's Domain Name Server.
2. For Windows Server 2003, install the SetSPN utility on the SQL Server.

   > ⚠ Microsoft has issued an update to SetSPN for Windows 2003. For more information, see Microsoft Technet, and to download, see Microsoft Support.

   For Windows 2008, SetSPN is a built-in command line tool, available if you have the Active Directory Domain Services server role installed. For more information, see Microsoft Technet.
3. Open an elevated command prompt and change directory to the folder where the utility is installed, then run this command:

   ```
   SetSPN -S MSSQLSvc/server.domain.local:1433 SERVER
   ```

   where: *server.domain.local* is the fully-qualified domain name of the server, and *SERVER* is the NETBIOS name of the server.

Trusting the computer and accounts for delegation

To trust the computer and any accounts for delegation you must have domain administrator privileges and access to the **Active Directory Users and Computers** applet on the Windows Active Directory server containing the computer account.

- If the SQL Server service runs as the *Local System* account, follow the steps below to trust the computer for delegation.
- If the SQL Server service runs as a domain account, follow the steps below to trust both the computer and domain account for delegation.

To trust the computer for delegation:

1. Open **Active Directory Users and Computers** and locate the computer account of the SQL Server. Right-click and select **Properties**.
2. Open the **Delegation** tab and select **Trust this computer for delegation to specified services only**. (On Windows 2000, this option is on the **G eneral** tab.)
3. Click **Add**, then **Users or Computers** and select the computer running the SQL Server.
4. Select the **MSSQLSvc** service type and click **OK**, then **OK** again.

On SQL Server clusters, this procedure must be done on the computer accounts of all nodes in the cluster.

To trust the domain account for delegation:

1. Open **Active Directory Users and Computers** and locate the domain account used by the SQL Server service. Right-click and select **Properties**.
2. Open the **Account** tab and:
    a. Ensure that **Account is sensitive and cannot be delegated** is not selected.
    b. Select **Account is trusted for delegation**.