

Creating a new role for the SQL Safe Backup services

Creating a new role for the SQL Safe Backup services ensures the high availability of the services during a failover.

The following instructions help you to configure the SQL Safe Backup services in its own cluster. Make sure you have an available disk in the cluster to store the temporary files used by the SQL Safe Backup services.

Create a Role

1. Log onto the active cluster node using an Administrator Account.
2. Launch the **Microsoft Failover Cluster Manager**.
3. Right-click on **Roles** and select **Create Empty Role**.
4. Right-click on the newly created role and select **Properties**.
5. **Rename the role** to a unique name (e.g. *SQLSafeServices*), then click **OK**.
6. Right-click on the role and select **Add Resource > Client Access Point**.
On the **Client Access Point** screen, enter a unique **Network Name** (e.g. *SQLSafeCluster*) and an available IP Address that has been reserved for the clustered resource, then click **Next**.
On the **Confirmation** screen, click **Next**.
On the **Summary** screen, click **Finish**.
7. Right-click on the role and select **Add Storage**.
8. Select an available disk, then click **OK**.

Add a Shared Path

1. **Open** File Explorer and navigate to the drive that was added as the **storage resource**.
2. **Create a folder** for the SQL Safe Backup services (e.g. *H:\Idera\SQLsafe*).
3. Launch **Registry Editor** and navigate to *HKLM\SOFTWARE\Idera\SQLsafe*.
4. **Create** a new **string value** named *Shared Path* and supply the path to the folder (e.g. *H:\Idera\SQLsafe*).

Create a Generic Service Resource

1. **Create a Generic Service resource** for each of the SQL Safe Backup services (SQL Safe Backup Service, SQL Safe Collection Service, SQL Safe Filter Service, SQL Safe Management Service, SQL Safe OLR Service, and SQL Safe Rest Service).
 - a. Right-click on the role and select **Add Resource > Generic Service**.
On the **Select Service** screen, locate and select the **SQL Safe Backup Service**. Click **Next** to proceed.
On the **Confirmation** screen, click **Next**.
On the **Summary** screen, click **Finish**.
 - b. Right-click on the role and select **Add Resource > Generic Service**.
On the **Select Service** screen, locate and select the **SQL Safe Collection Service**. Click **Next** to proceed.
On the **Confirmation** screen, click **Next**.
On the **Summary** screen, click **Finish**.

- c. Right-click on the role and select **Add Resource > Generic Service**.
On the **Select Service** screen, locate and select the **SQL Safe Filter Service**. Click **Next** to proceed.
On the **Confirmation** screen, click **Next**.
On the **Summary** screen, click **Finish**.
 - d. Right-click on the role and select **Add Resource > Generic Service**.
On the **Select Service** screen, locate and select the **SQL Safe Management Service**. Click **Next** to proceed.
On the **Confirmation** screen, click **Next**.
On the **Summary** screen, click **Finish**.
 - e. Right-click on the role and select **Add Resource > Generic Service**.
On the **Select Service** screen, locate and select the **SQL Safe OLR Service**. Click **Next** to proceed.
On the **Confirmation** screen, click **Next**.
On the **Summary** screen, click **Finish**.
 - f. Right-click on the role and select **Add Resource > Generic Service**.
On the **Select Service** screen, locate and select the **SQL Safe Rest Service**. Click **Next** to proceed.
On the **Confirmation** screen, click **Next**.
On the **Summary** screen, click **Finish**.
2. **Configure** the properties for each of the newly created generic service resources.
- a. Right-click on the newly generic service resource and select **Properties**.
On the **Properties** window, go to the **Dependencies** tab.
Add the following dependencies:
 - i. Name of the clustered role.
 - ii. Storage resource.
 - b. Click **Apply**.
 - c. Go to the **General** tab.
 - d. Enable the **Use Network Name for computer name** checkbox, then click **Apply**.
 - e. Go to the **Registry Replication** tab. Click the **Add** button and enter SOFTWARE\Idera\SQLsafe\ into the Root Registry Key field, then click **OK**.



There is a bug in Windows 2012 where the Registry Replication tab is not available. If the tab is unavailable, use the [Add-ClusterCheckpoint](#) PowerShell cmdlet to add the necessary setting.

EXAMPLE: Add-ClusterCheckpoint -ResourceName "SQLsafe Management Service" -RegistryCheckpoint "SOFTWARE\Idera\SQLSafe\Management Service" -Cluster "[ClusterName]"

- f. Repeat the steps above for each generic service resource.
3. Right-click on the Role and select **Start Role**.

Reconfigure the SQL Safe Management Console

1. Launch the **SQL Safe Management Console** (Start > All Programs > IDERA > SQL Safe Management Console).
2. Go to **Tools > Repository and Management Service Settings**.

3. Next to the **Computer** field, click the **Change** button.
4. On the window that appears, enter the **cluster name** that SQL Safe Management Service is associated to, then click **OK**.
5. **Update** the SQL Server and Database field if necessary.
6. Click **OK** on the **Repository and Management Service Settings** window.

[IDERA](#) | [Products](#) | [Purchase](#) | [Support](#) | [Community](#) | [Resources](#) | [About Us](#) | [Legal](#)