Deploy the SQL Compliance Manager Agent to cluster nodes

Now that the IDERA Cluster Configuration Console is installed, you need to add the SQL Compliance Manager Agent to the clustered instance that is to be audited.

Use the following checklist to help you deploy and configure SQL Compliance Manager in a clustered environment.

☑	**Follow these steps ...**
☐	Install SQL Compliance Manager.
☐	Identify which virtual SQL Server instances you want to audit.
☐	Identify which cluster nodes host each virtual SQL Server instance. Make sure that you identify the currently active node as well as any passive nodes in the same cluster.
☐	On each cluster node, open port 5200 for SQL Compliance Manager Agent communication.
☐	For each cluster node, identify the folder you want to use for the SQL Compliance Manager Agent trace directory. ***If a cluster node hosts more than one virtual SQL Server instance***, identify a trace directory for each additional instance you want to audit.
☐	For each cluster node, identify the account you want to use for the SQL Compliance Manager Agent Service. Verify that this account can access the computer where you installed the Collection Server. Also make sure that this account belongs to the Administrators group on each node. Review the SQL Compliance Manager Agent Service permission requirements.
☐	Deploy the SQL Compliance Manager Agent to each cluster node using the Cluster Configuration setup program.
☐	Add the SQL Compliance Manager Agent service on each cluster node using the Cluster Configuration Console.
☐	Register the SQL Compliance Manager Agent as a generic service using the Microsoft Cluster Administrator tool.
☐	Register each virtual SQL Server instance with SQL Compliance Manager using the Management Console. Note that you must choose manual deployment for the SQL Compliance Manager Agent.
☐	Specify the SQL Server events you want to audit on each registered virtual SQL Server instance using the Management Console.
☐	Run SQL Compliance Manager. Use report cards and the Audit Events tab to ensure you are auditing the correct SQL Server events.

1. Add the SQL Compliance Manager Agent

ⓘ You must perform these steps on **all nodes** of the cluster.

1. Once the ***Cluster Configuration Console*** launches, click **Add Service.**
2. On the ***General*** dialog window, specify the name of the clustered instance to be audited by IDERA SQL Compliance Manager and click **Next.**
3. On the ***Collection Server*** dialog window, specify the name of the server hosting the SQLcompliance Collection Service and click **Next.**
4. On the ***SQLcompliance Agent Trace Directory*** dialog window, specify the path on which trace files will temporarily reside before being transferred to the SQLcompliance Collection Service.
   The path specified should be on a drive that is a part of the same resource group as the SQL Server instance to be audited.
5. On the ***CLR Trigger Location*** dialog window, specify the path on which trigger assembly files will reside. The path specified should be on a drive that is a part of the same resource group as the SQL Server instance to be audited.
   Click **Next**.

   ⚠ Ensure the Agent Trace directory and the CLR Trigger location specified exist by creating the folder structure manually through Windows Explorer.

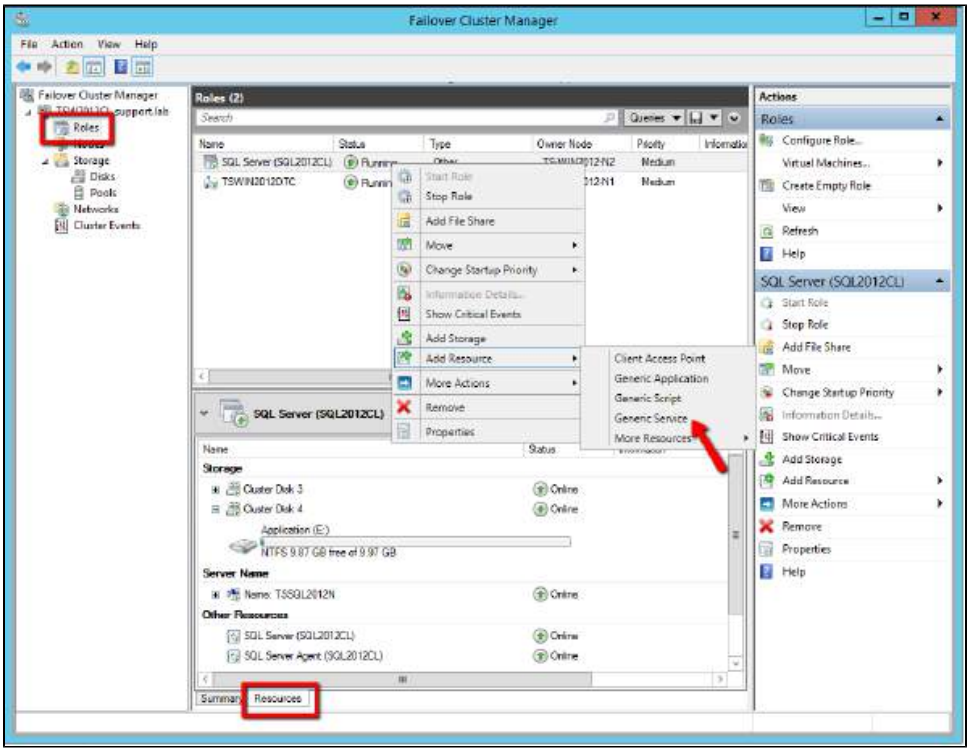
6. Review the configuration and click **Finish.**
7. The IDERA Cluster Configuration Console displays a confirmation message stating that you have successfully added the SQL Compliance Manager Agent.
   Click **OK**.

2. Register the SQL Compliance Manager Agent as a clustered service

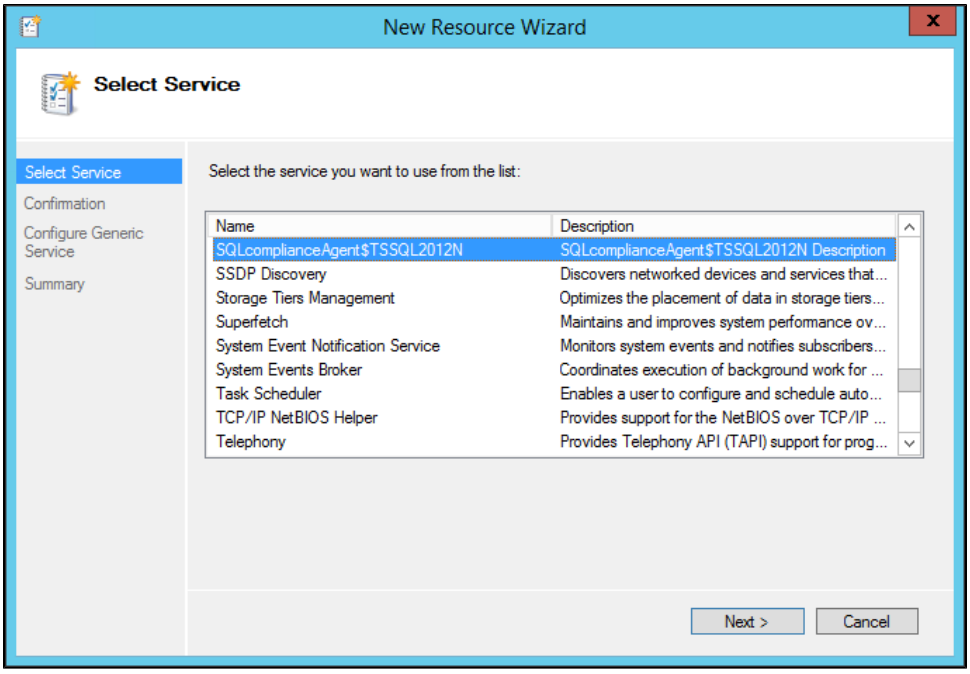
Registering the SQL Compliance Manager Agent service with Microsoft Failover Cluster Manager allows the Microsoft Cluster Service to manage the SQL Compliance Manager Agent service in failover situations. This configuration ensures that auditing will continue during a failover and no audit data is lost.

> You must perform these steps only **once**, in the **active node**.

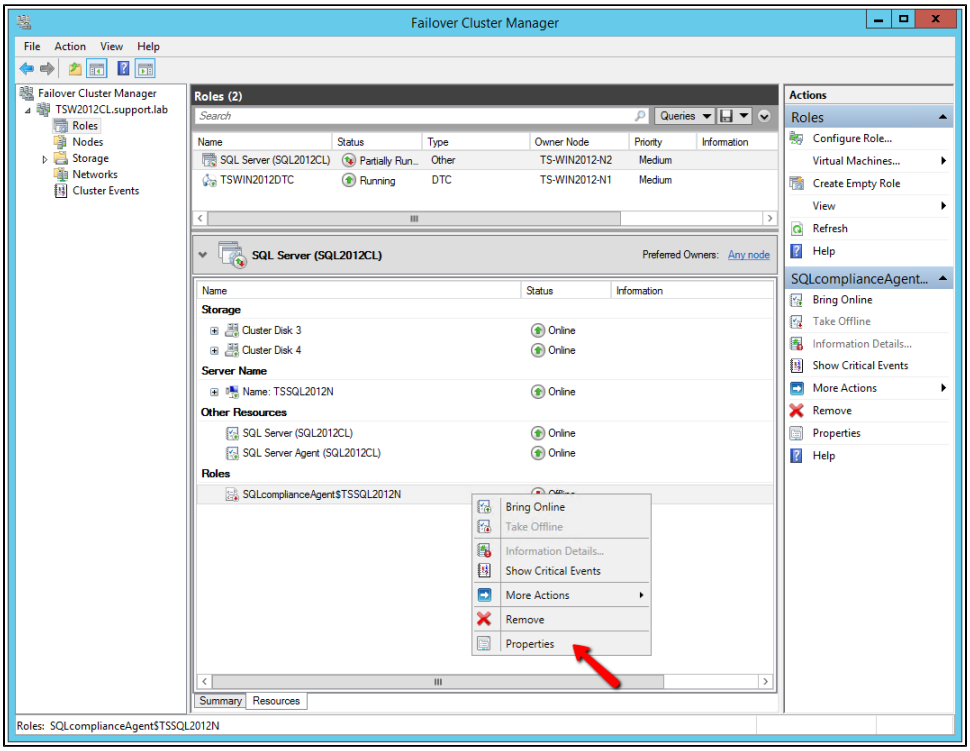
1. Log onto the active cluster node using an administrator account and launch the Microsoft Failover Cluster Manager.
2. Right-click the role created for the clustered instance, point to **Add a Resource,** and select **Generic Service**.



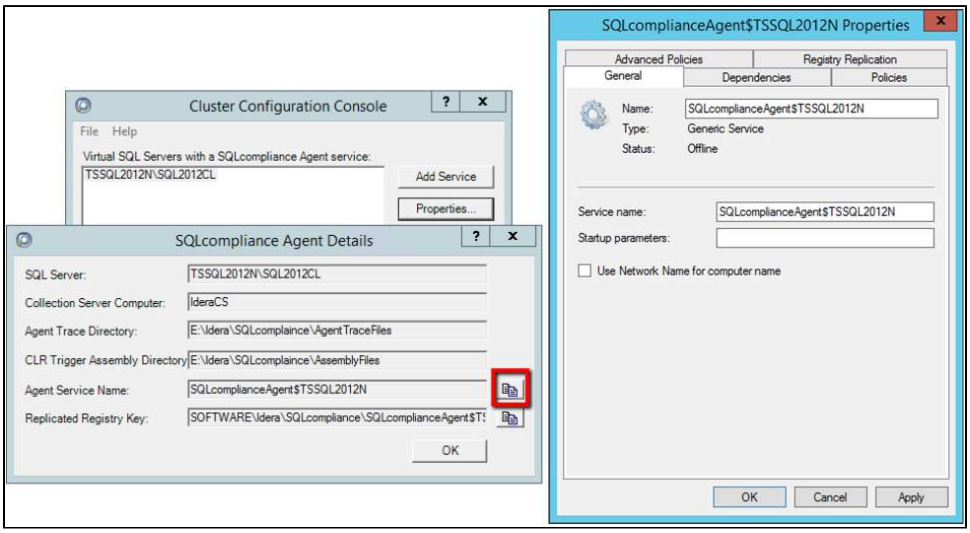
3. On the ***Select Service*** dialog window, **select** the SQL Compliance Manager Agent service created previously, continue following the wizard, and click **Finish**.



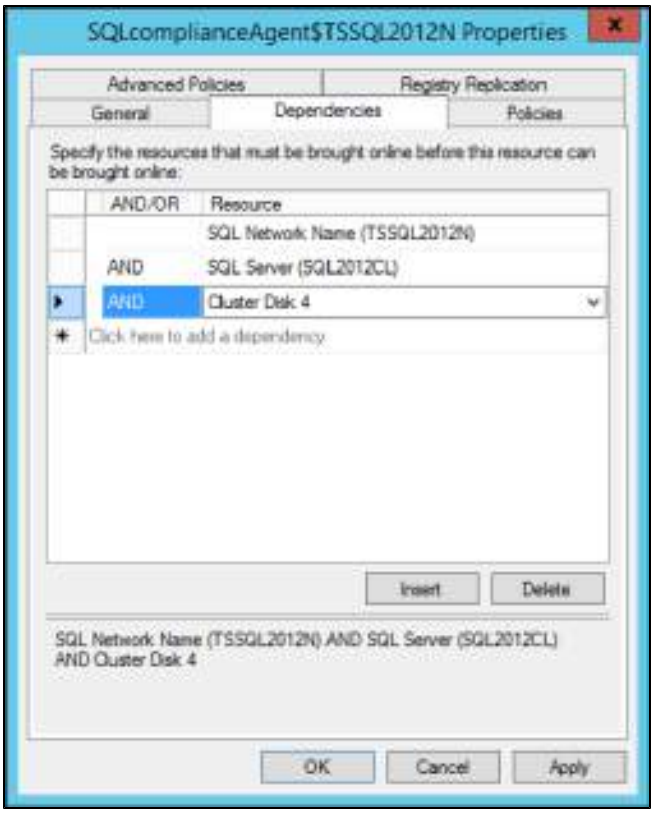
4. The Failover Cluster Manager displays the new resource in the resources tab. Right-click the new resource and select **Properties**.



5. In the ***General*** tab, specify the ***Service name*** as the Agent Service name found in the ***SQLcompliance Agent details*****.**



6. Clear the ***Startup parameters.***
7. Go to the ***Dependencies*** tab and add the following dependencies:
    a. *SQL Network Name:* name of the cluster hosting the SQL instance to be audited.
    b. *Cluster Disk(s):* the disk(s) on which the agent trace directory and the CLR trigger assemblies reside.
    c. *SQL Server:* the SQL Server instance to be audited by SQL Compliance Manager.

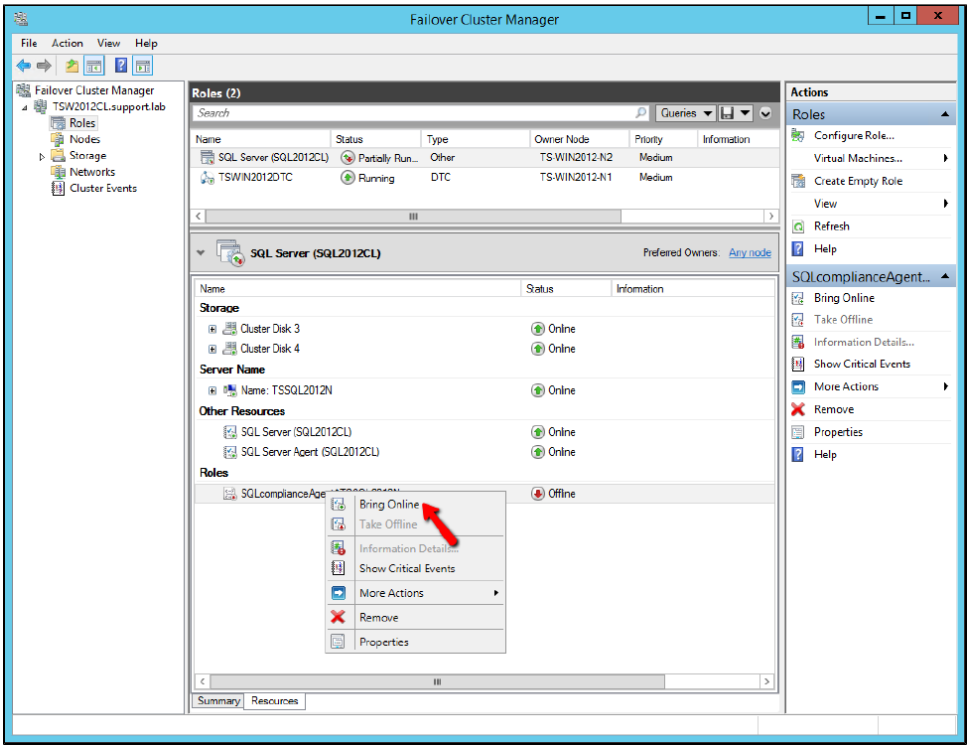


8. Once the dependencies are configured, click **Apply.**
9. Return to the ***General*** tab, check the **Use Network Name for computer name** box and click **Apply.**
10. Go to the ***Registry Replication*** tab.

> ⚠ The Registry Replication tab is not available in Windows Server 2012.
>
> If you are using Windows Server 2012, you must use the *"Add-ClusterCheckpoint"* PowerShell cmdlet to add the necessary setting.
>
> For more information, see Add ClusterCheckPoint.

Add a specific registry path. To obtain the correct path, go to the IDERA Cluster Configuration Console and copy the ***Replicated Registry Key*** from the ***SQLcompliance Agent details*****.**
Click **OK.**

11. On the **Properties** window, click **Apply** to save the changes, and click **OK** to return to the ***Resources*** *tab.*
12. Right-click the *SQLcompliance Agent* resource and click **Bring Online.**



After successfully deploy the SQL Compliance Manager Agent, you can start auditing your virtual SQL Server instances**.**