Enable automatic failover using AlwaysOn Availability Groups

The AlwaysOn Availability Groups feature uses the availability of a set of databases within your enterprise to improve your failover options and general availability. This feature makes the database highly available using the Windows Failover Cluster Service for Windows Server 2008 and above. As a result, this feature requires Windows Failover Cluster as well as SQL Server on all cluster nodes.

When an availability group is configured using multiple SQL Servers, one of the servers is designated as the PRIMARY node and others are considered SECONDARY nodes. If the primary node SQL Server stops or shuts down, the failover automatically switches to the synchronized secondary node with no data loss. You also can manually perform a failover on the SQL Server.

SQL Compliance Manager provides auditing of the AlwaysOn-configured database and audits the events on the AlwaysOn database along with the failovers.

> The AlwaysOn Availability Groups feature is available for SQL Server 2012 and above only.

How AlwaysOn integrates with SQL Compliance Manager

There are two scenarios of how SQL Compliance Manager can work with AlwaysOn availability group databases:

- **Listener** . Use this scenario when you want to audit a listener (virtual SQL server instance) that works only with a node in the PRIMARY role.
- **Nodes** . Use this scenario when you want to audit every node that can be in PRIMARY or SECONDARY roles. Note that the secondary role is read-only.

You can use only one scenario at a time and it is not possible to use them at the same time on cluster.

> Each node of the SQL Server instance used in the AlwaysOn Availability Group must have a license.

Configuring the Listener scenario

The Listener scenario is recommended for users who want to audit only AlwaysOn databases on the Primary node using LISTENER. ***If you want to audit read-only Secondary nodes*** , use the Nodes scenario.

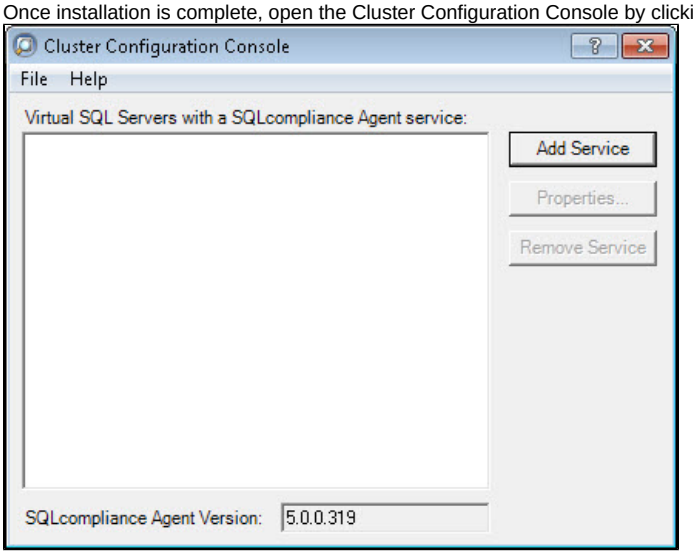
1. Install cluster agent services on all Listener nodes using the SQL Compliance Manager Cluster Configuration Console

Use the following steps on each node involved in the AlwaysOn group before adding the listener to SQL Compliance Manager for auditing.

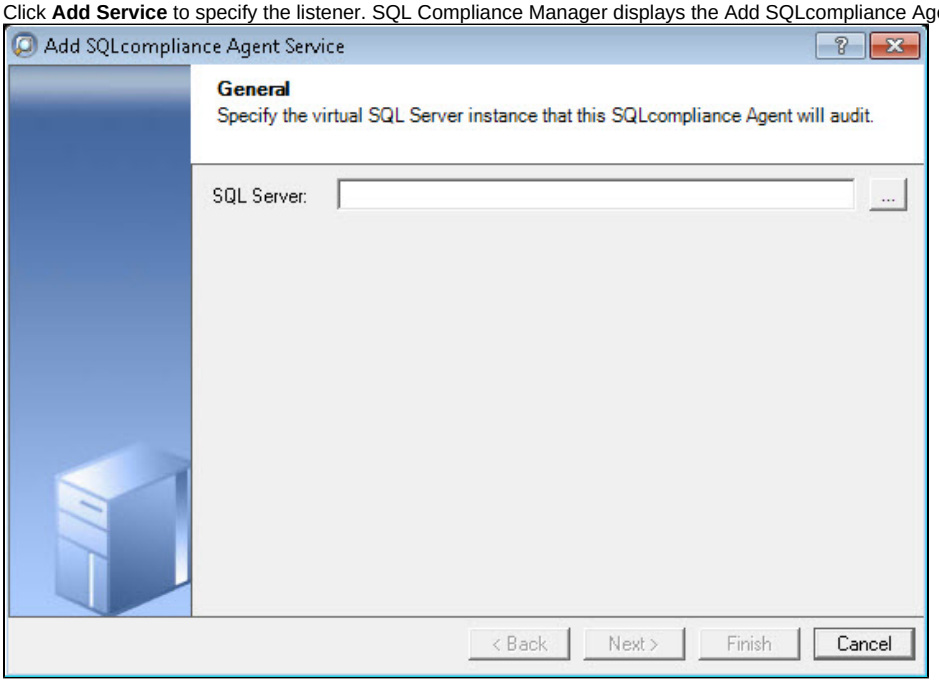
> Repeat these steps on each node in your AlwaysOn Availability Group. When you are finished configuring all the nodes, register the cluster service agent as a shared resource.

1. Run the **IderaSQLcmInstallationKit*.exe** setup file.
2. Extract the SQL Compliance Manager installation kit to the specified directory, and then launch it. SQL Compliance Manager displays the product Quick Start window.
3. In the Quick Start window, click **Cluster Configuration Console**. SQL Compliance Manager displays the Cluster Configuration Setup Wizard.
4. Follow the steps in the Setup Wizard to install and configure the SQLcompliance Agent Service on this cluster node.

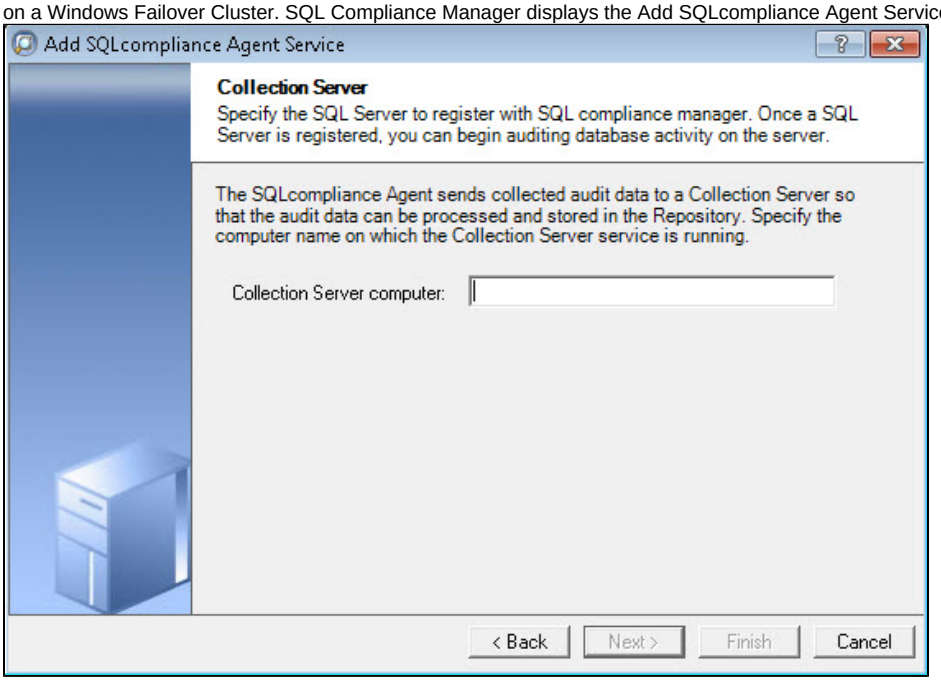
5. Once installation is complete, open the Cluster Configuration Console by clicking **Start > IDERA > Cluster Configuration Console**.



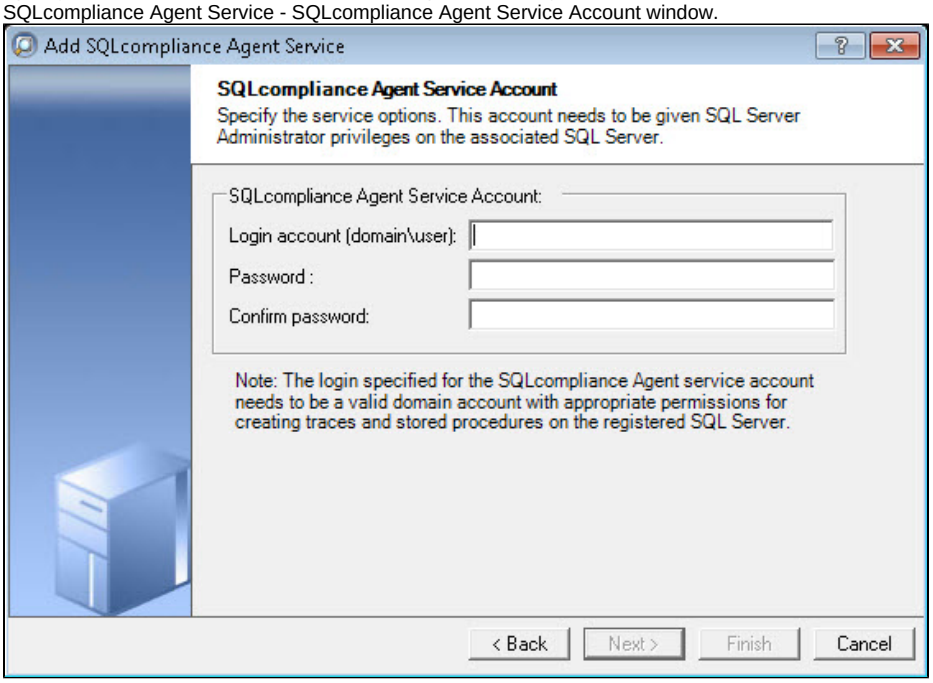
6. Click **Add Service** to specify the listener. SQL Compliance Manager displays the Add SQLcompliance Agent Service - General window.



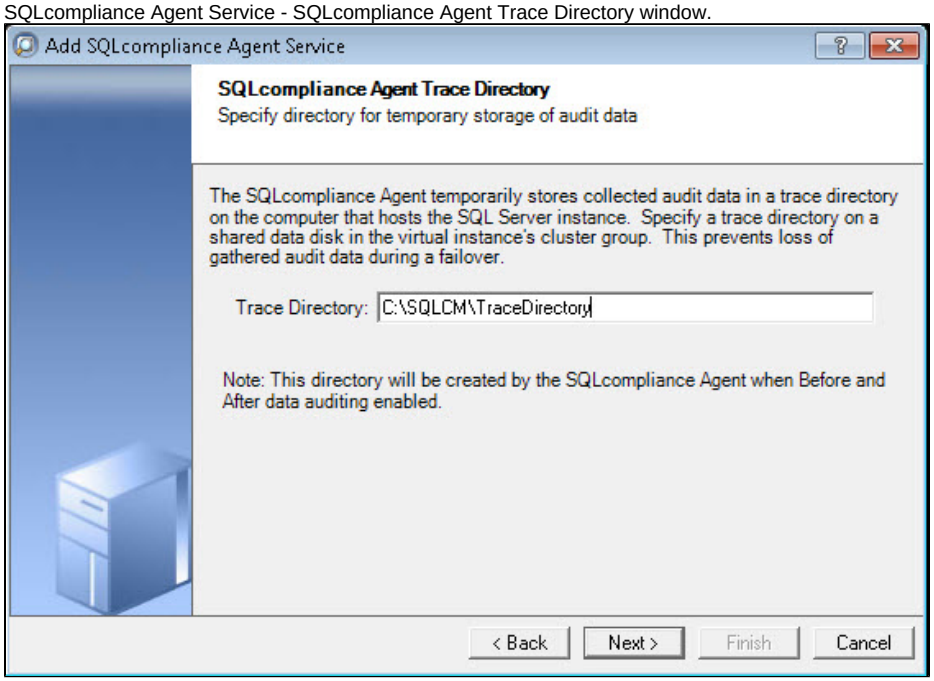
7. Type the SQL Server instance name, and then click **Next**. ***If you receive a message stating that the selected SQL Server instance is not clustered*** , click **Yes**. This is correct behavior when configuring a Listener scenario and confirms that the selected SQL Server instance is hosted on a Windows Failover Cluster. SQL Compliance Manager displays the Add SQLcompliance Agent Service - Collection Server window.



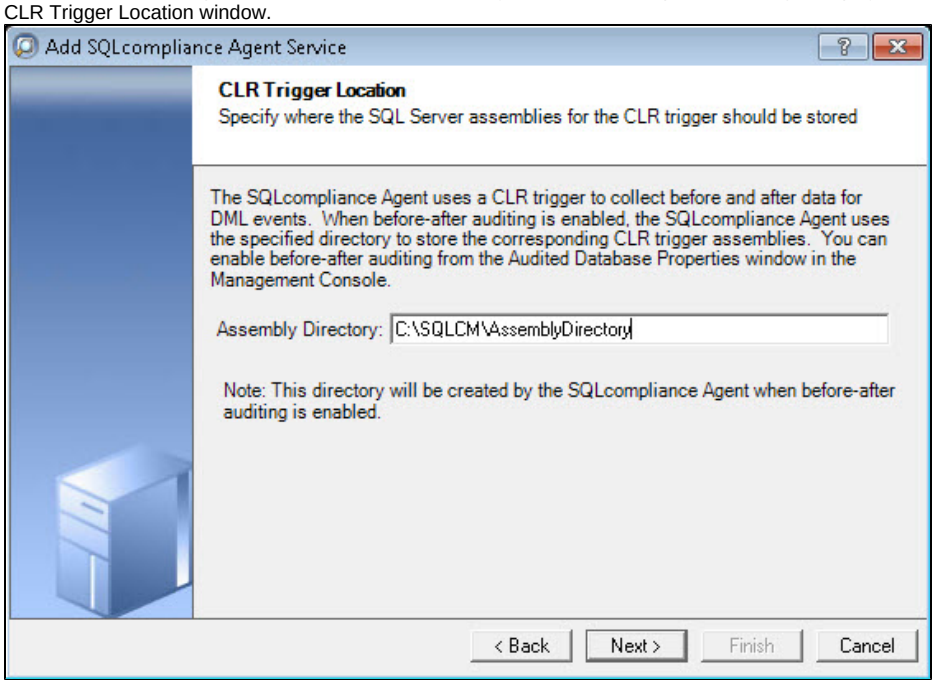
8. Specify the name of the server where SQL Compliance Manager is installed, and then click **Next**. SQL Compliance Manager displays the Add SQLcompliance Agent Service - SQLcompliance Agent Service Account window.



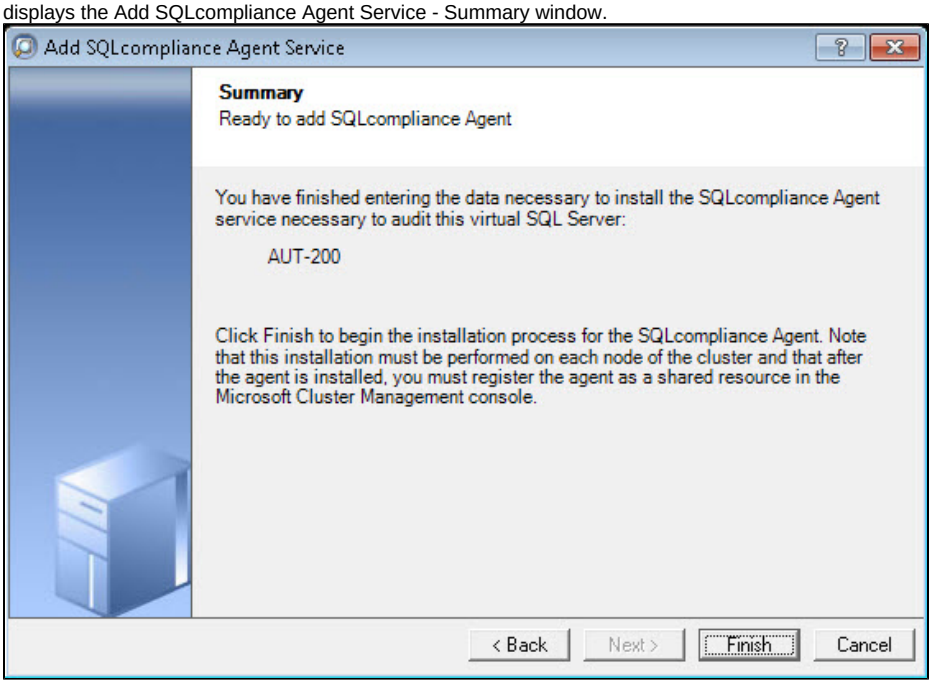
9. Specify the login credentials for the Agent service account, and then click **Next**. This account must have administrator privileges. Idera recommends that you use the same account as used for the Collection Server. After clicking Next, SQL Compliance Manager displays the SQLcompliance Agent Service - SQLcompliance Agent Trace Directory window.



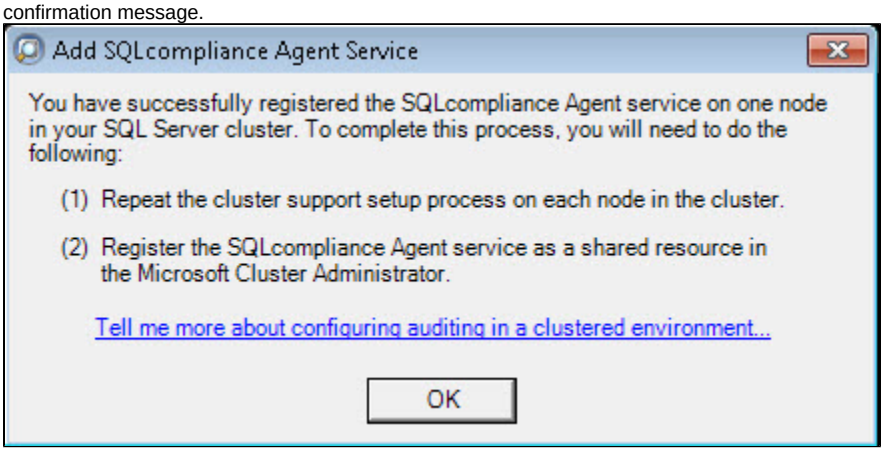
10. Specify the trace directory for the cluster agent service, and then click **Next**. Note that the administrator account specified for the cluster agent service has read/write permissions for this trace directory folder. SQL Compliance Manager displays the Add SQLcompliance Agent Service - CLR Trigger Location window.



11. Specify the location where you want the SQLcompliance Agent to store the corresponding CLR trigger assemblies, and then click **Next**. Note that the administrator account specified for the cluster agent service has read/write permissions for this assembly folder. SQL Compliance Manager displays the Add SQLcompliance Agent Service - Summary window.



12. Verify that the Summary window displays the correct SQL Server instance that you want to audit, and then click **Finish**. ***If you receive a message stating that the selected SQL Server instance is not clustered*** , click **Yes**. This is correct behavior when configuring a Listener scenario and confirms that the selected SQL Server instance is hosted on a Windows Failover Cluster. SQL Compliance Manager displays a confirmation message.



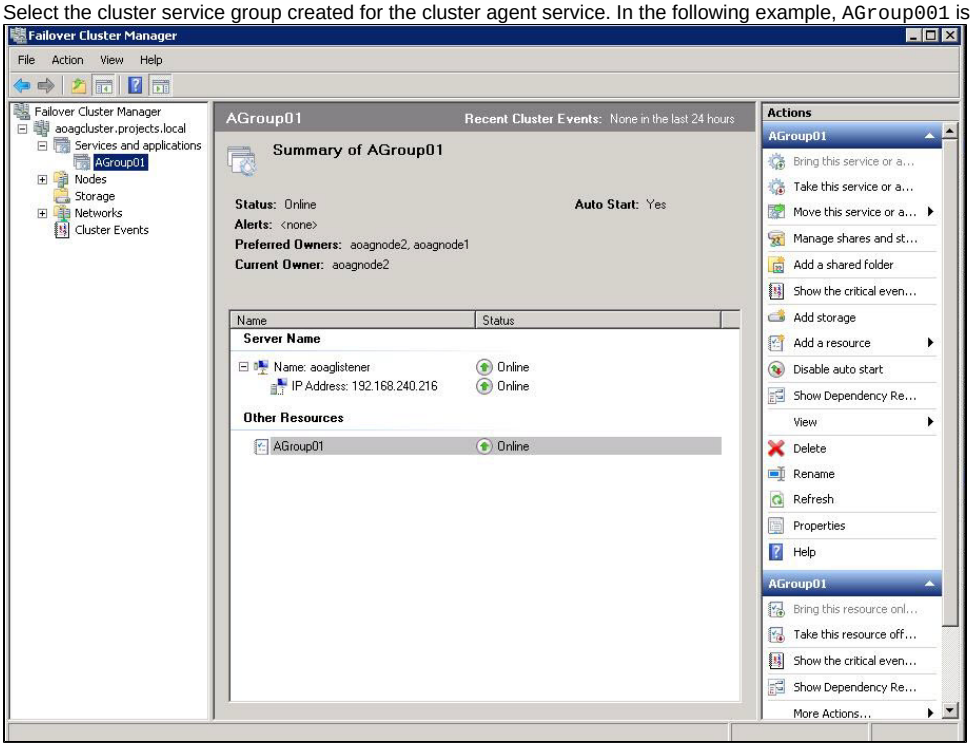
> Repeat these steps on each node in your AlwaysOn Availability Group. When you are finished configuring all the nodes, register the cluster service agent as a shared resource.

2. Install cluster agent services on all Listener nodes using the Failover Cluster Manager

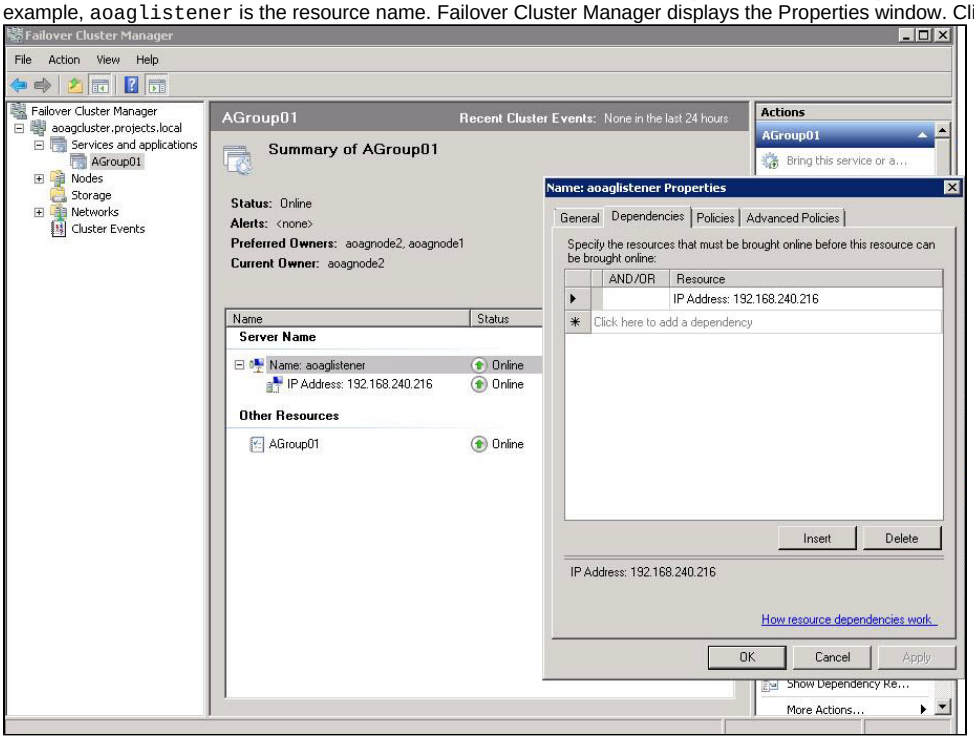
Use the following steps on each node involved in the AlwaysOn group before adding the listener to SQL Compliance Manager for auditing.

1. After installing the cluster agent service on all Listener nodes, open Server Manager.
2. In the Server Manager tree, click **Server Manager > Features > Failover Cluster Manager**. The system displays Failover Cluster Manager.

3. Select the cluster service group created for the cluster agent service. In the following example, `AGroup001` is the cluster service group.

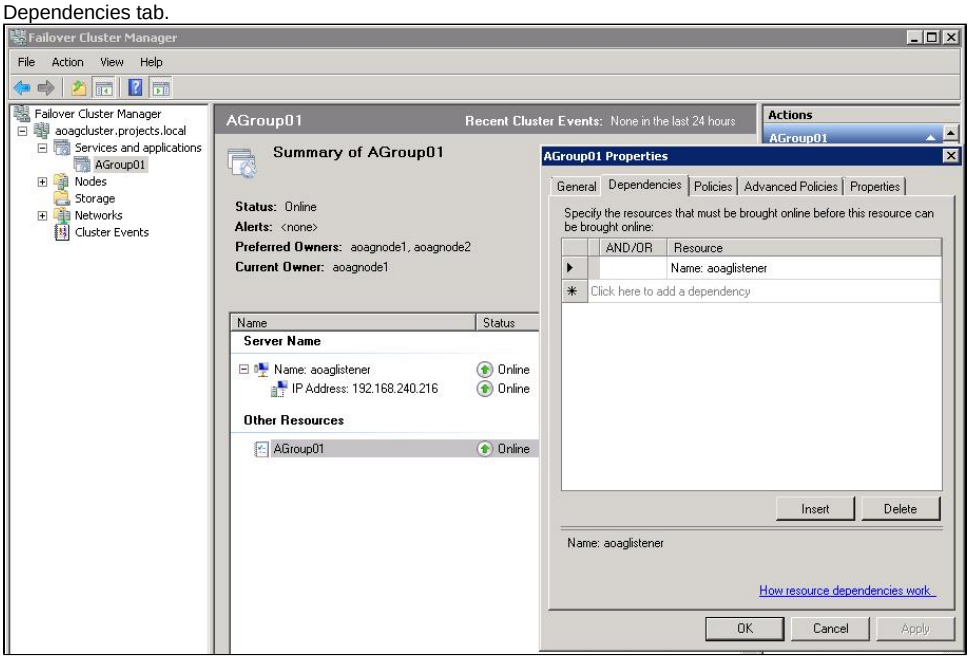


4. In the Server Name area, select the resource name of the cluster service group, and then click **Properties** in the Actions panel. In the following example, `aoaglistener` is the resource name. Failover Cluster Manager displays the Properties window. Click the Dependencies tab.

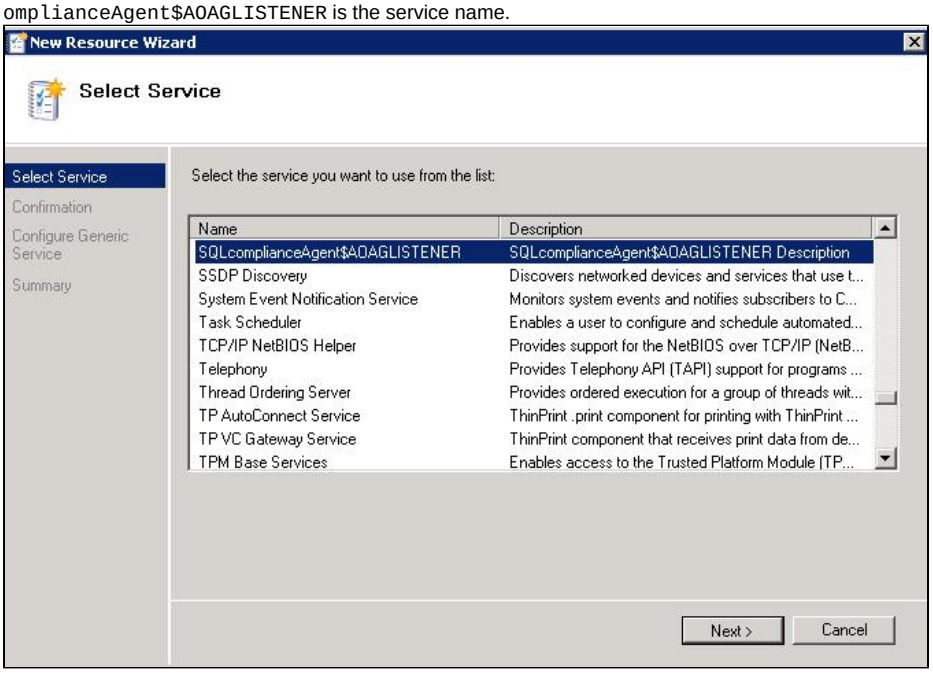


5. Verify that the **Resource** field displays the listener IP address.

6. In the Other Resources area of the Failover Cluster Manager window, select the resource within the cluster service group, and then select **Properties**. In the following example, `AGroup01` is the other resource name. Failover Cluster Manager displays the Properties window. Click the Dependencies tab.

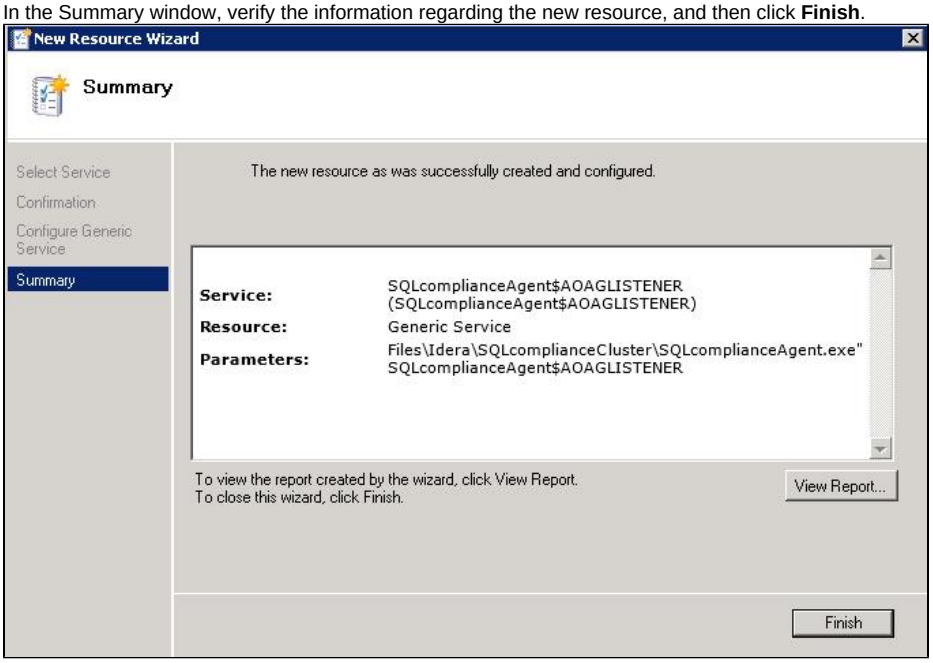


7. Verify that the **Resource** field displays the listener name. Click **Cancel** to close this window.
8. After adding the resource information, right-click the cluster service group in the tree, and then select **Add a resource > 4 - Generic Service**. Failover Cluster Manager displays the New Resource Wizard to allow you to create the new resource.
9. In the Select Service page of the New Resource Wizard, select the cluster service agent from the available list. The cluster service names are displayed in the format *SQLcomplianceAgent$[listener name]* where [*listener name*] is a virtual SQL Server name. In the following example, `SQLcomplianceAgent$AOAGLISTENER` is the service name.

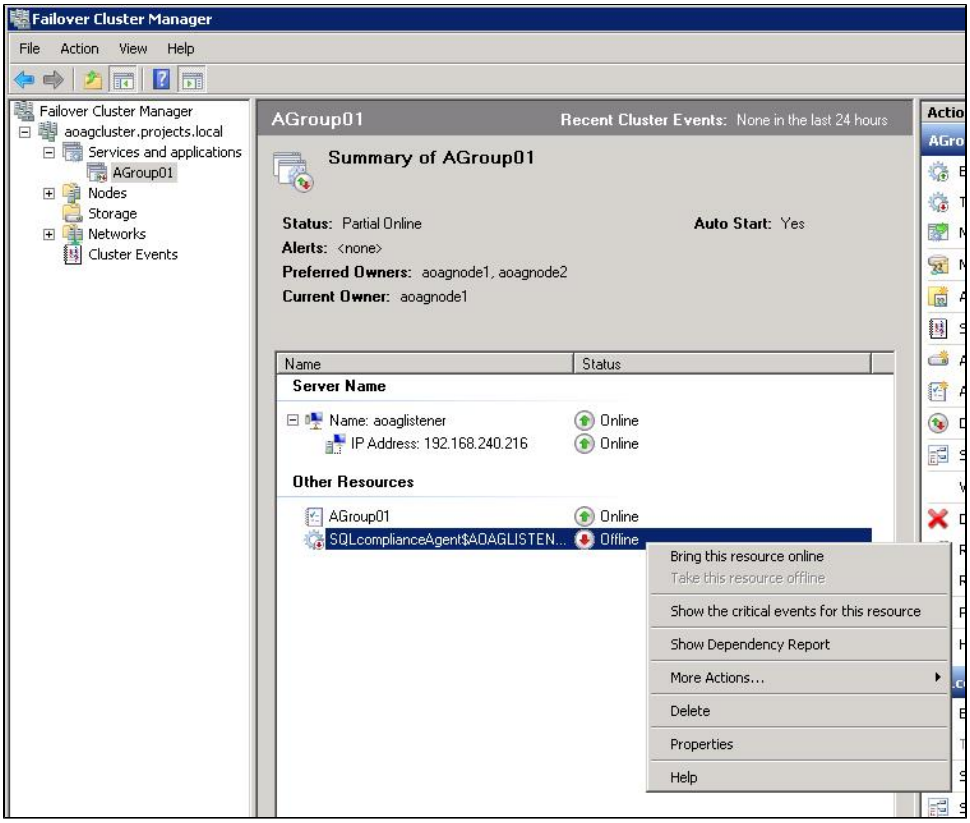


10. Click **Next**, the New Resource Wizard displays the Confirmation window.
11. Verify that the displayed information is correct, and then click **Next**.
12. In the Configure Generic Service window, Failover Cluster Manager creates the new resource. Click **Next**.

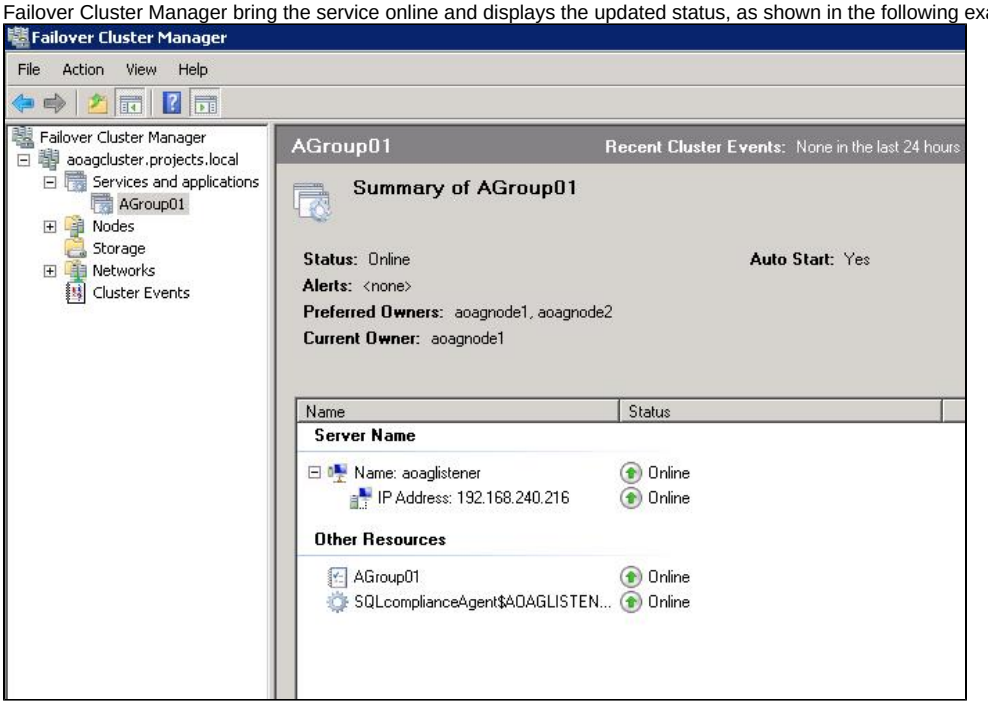
13. In the Summary window, verify the information regarding the new resource, and then click **Finish**.



14. In the Other Resources area of the Failover Cluster Manager window, select the *SQLcomplianceAgent$[listener name]* cluster service group, and then click **Bring this resource online** from the context menu. In the following example, `SQLcomplianceAgent$AOAGLISTENER` is the cluster service and is currently offline as noted in the **Status** column.

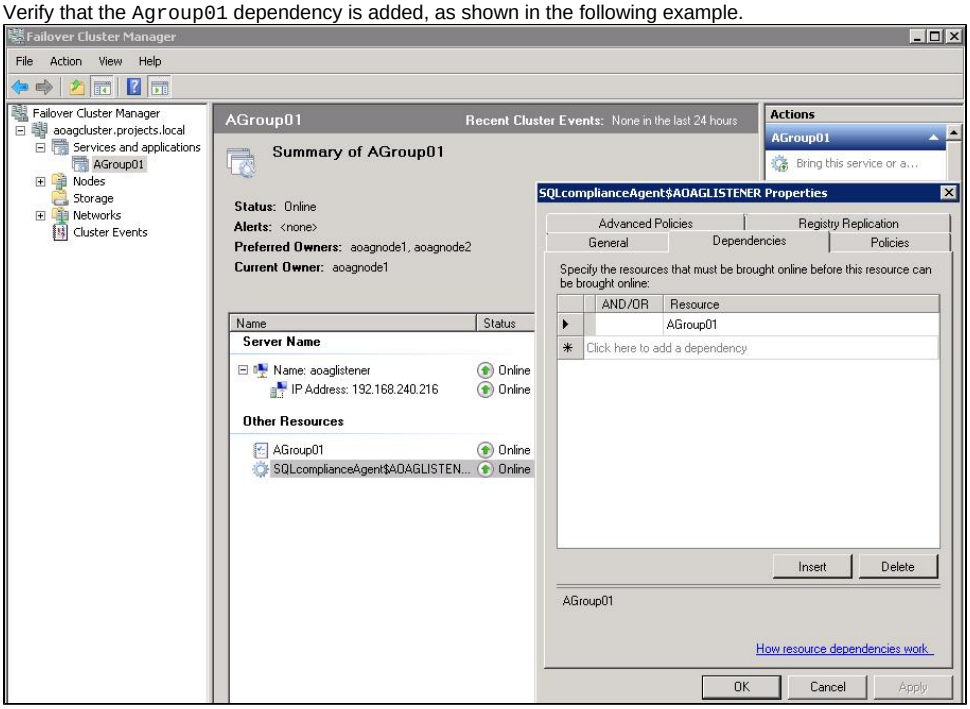


Failover Cluster Manager bring the service online and displays the updated status, as shown in the following example.

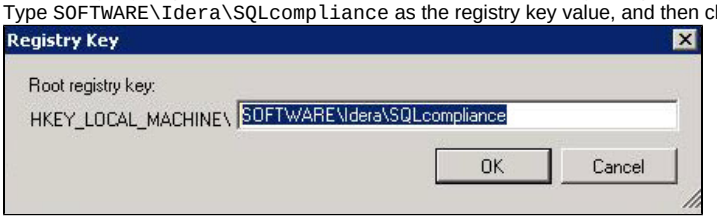


15. While the cluster service is online, select the *SQLcomplianceAgent$[listener name]* cluster service, and then select **Properties** from the context menu. In the following example, `SQLcomplianceAgent$AOAGLISTENER` is the cluster service name. Failover Cluster Manager displays the Properties window.

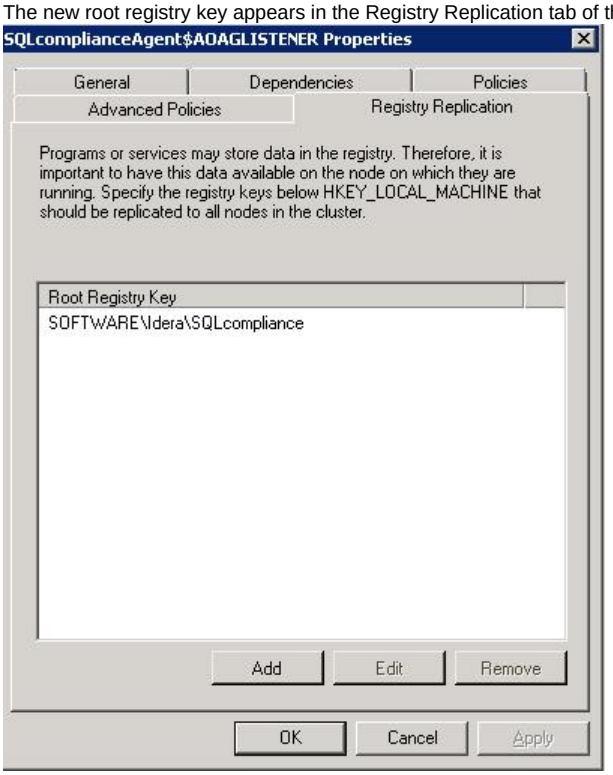
16. Verify that the `Agroup01` dependency is added, as shown in the following example.



17. On the Registry Replication tab, click **Add**. Failover Cluster Manager displays the Registry Key window.
18. Type `SOFTWARE\Idera\SQLcompliance` as the registry key value, and then click **OK**.



The new root registry key appears in the Registry Replication tab of the Properties window, as shown in the following example.

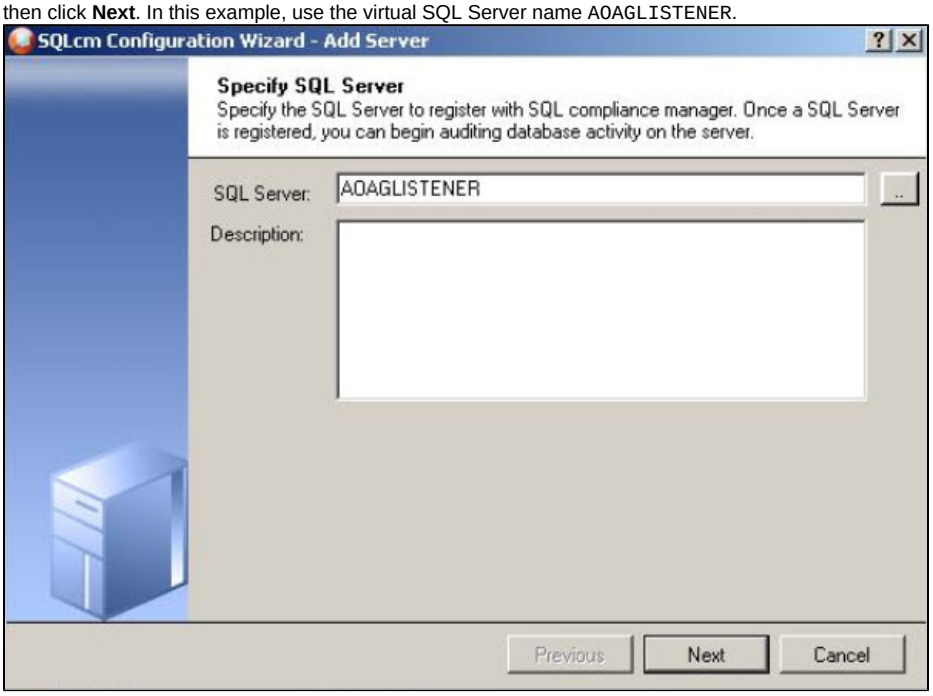


19. Close the Properties window by clicking **OK**.

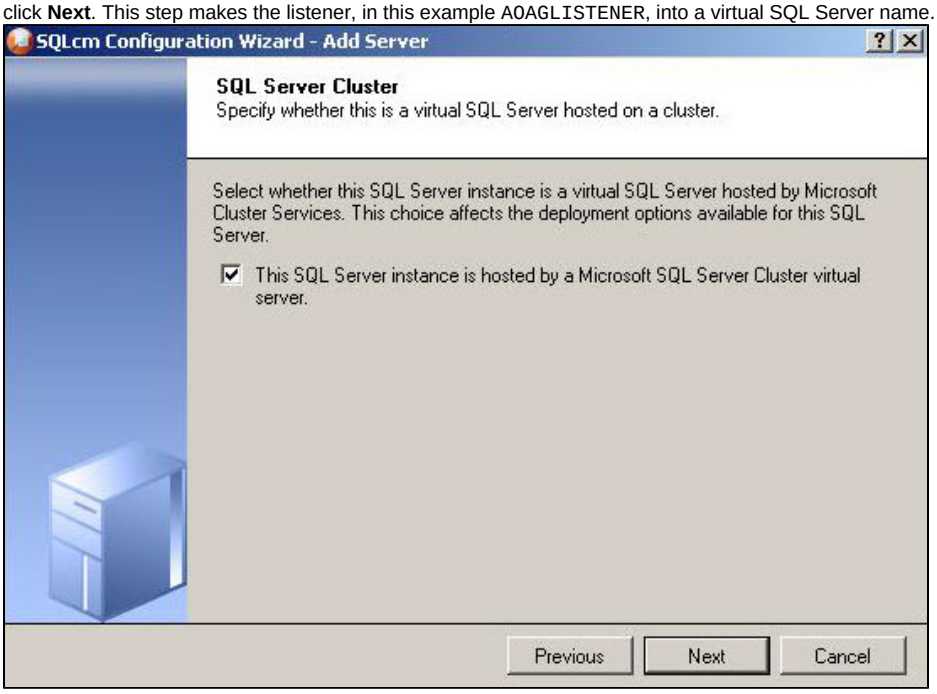
3. Add the Listener to SQL Compliance Manager

Use the following steps to add the listener to SQL Compliance Manager for auditing.

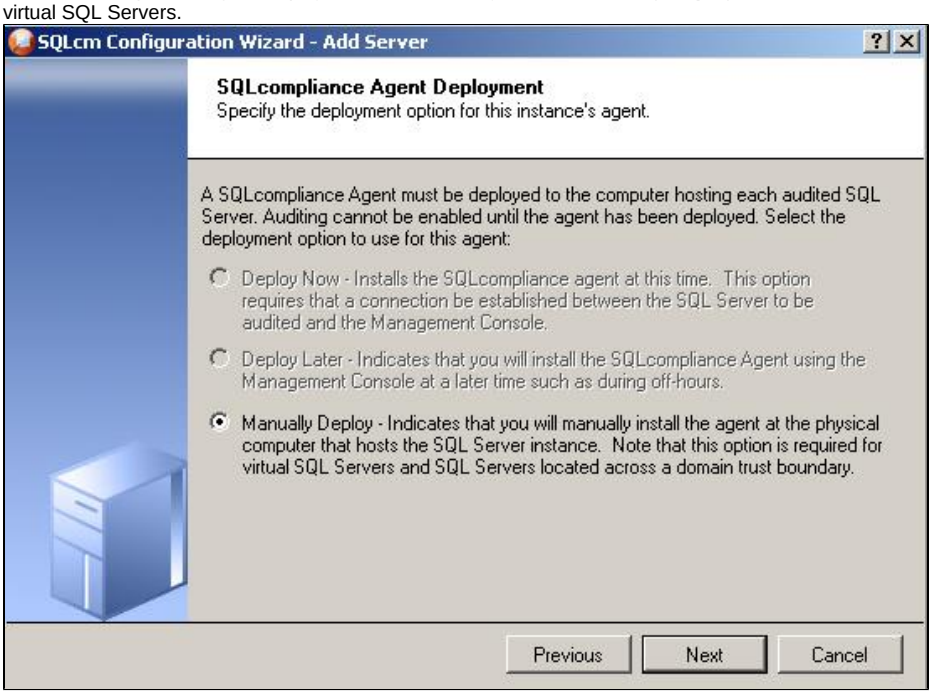
1. Start the SQL Compliance Manager Management Console, and then click **New > Registered SQL Server**.
2. In the SQL Compliance Manager Configuration Wizard, specify or browse to the listener you want to register with SQL Compliance Manager, and then click **Next**. In this example, use the virtual SQL Server name `AOAGLISTENER`.



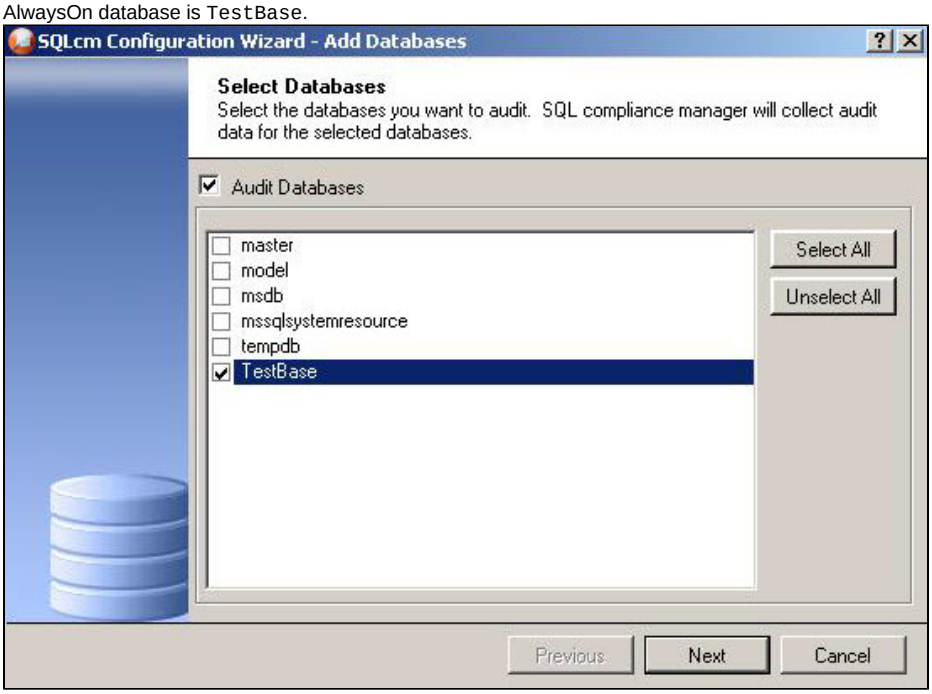
3. In the SQL Server Cluster window, check **This SQL Server instance is hosted by a Microsoft SQL Server Cluster virtual server**, and then click **Next**. This step makes the listener, in this example `AOAGLISTENER`, into a virtual SQL Server name.



4. In the SQLcompliance Agent Deployment window, verify that the **Manually Deploy** is selected, and then click **Next**. This option is required for all virtual SQL Servers.

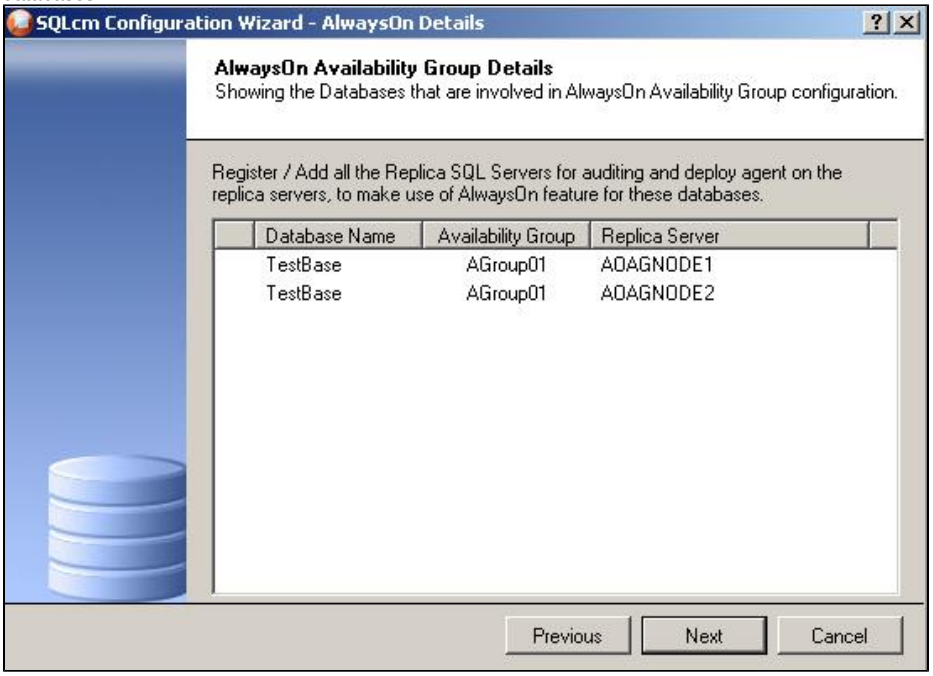


5. In the Select Databases window, check the AlwaysOn database that you want to audit, and then click **Next**. In the following example, the AlwaysOn database is `TestBase`.

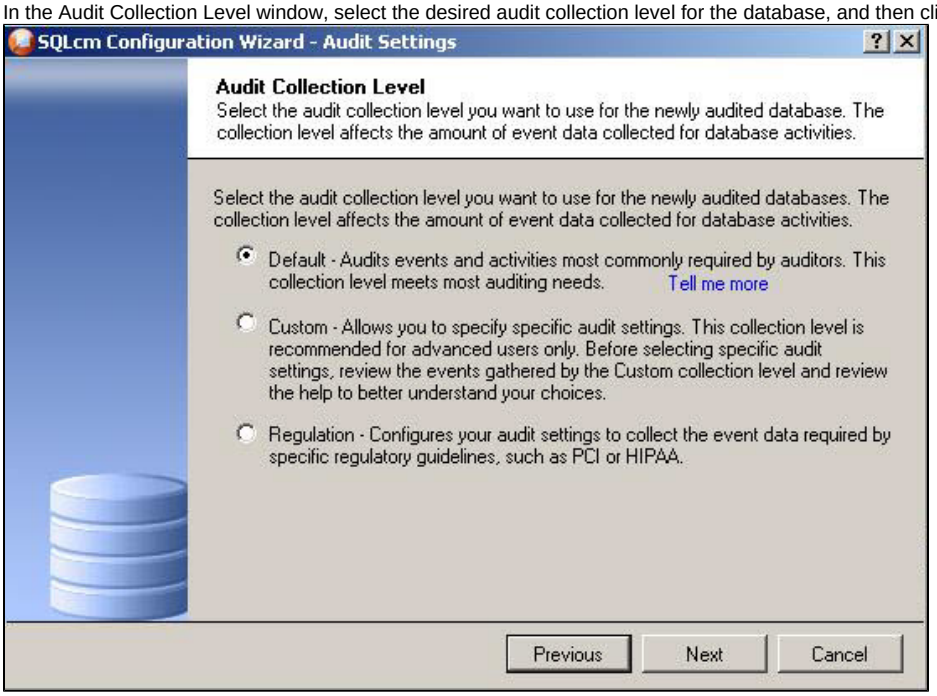


SQL Compliance Manager displays the AlwaysOn Availability Group Details window including a list of all nodes where the AlwaysOn database is

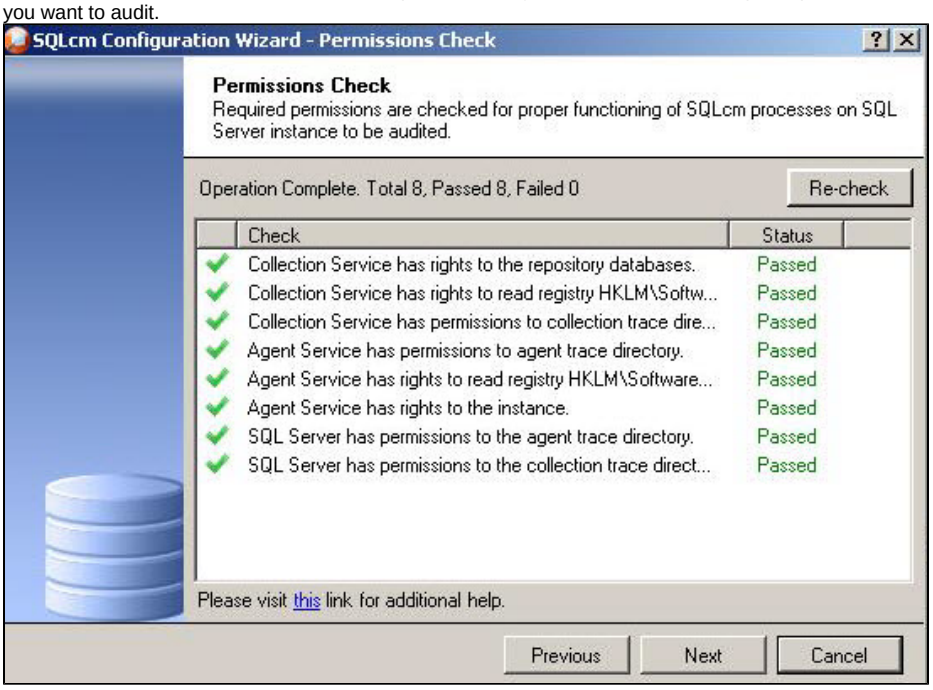
replicated. Note that this window appears only if the database selected for auditing is AlwaysOn. The wizard skips this window for regular databases.



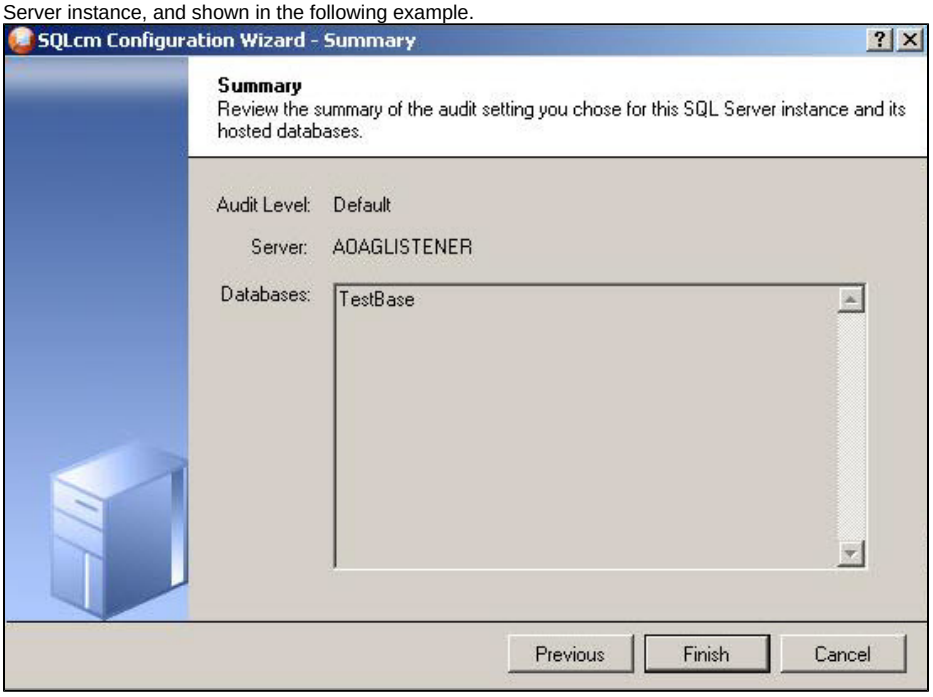
6. ***If the AlwaysOn Availability Group Details window is displayed*** , click **Next** to continue.
7. In the Audit Collection Level window, select the desired audit collection level for the database, and then click **Next**.



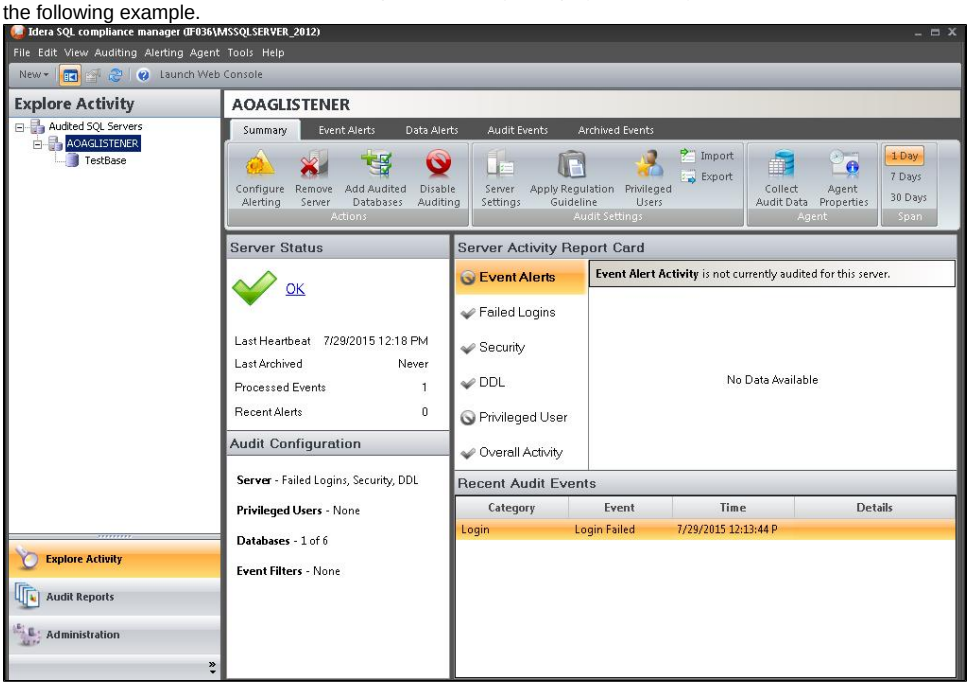
In the Permissions Check window, SQL Compliance Manager verifies that all the required permissions are in place on the SQL Server instance you want to audit.



8. After all operations are complete and all permissions checks pass, click **Next**. The Summary window displays the audit settings for the SQL Server instance, and shown in the following example.



9. Click **Finish** to close the wizard. SQL Compliance Manager displays the newly-added SQL Server instance and AlwaysOn database, as shown in the following example.

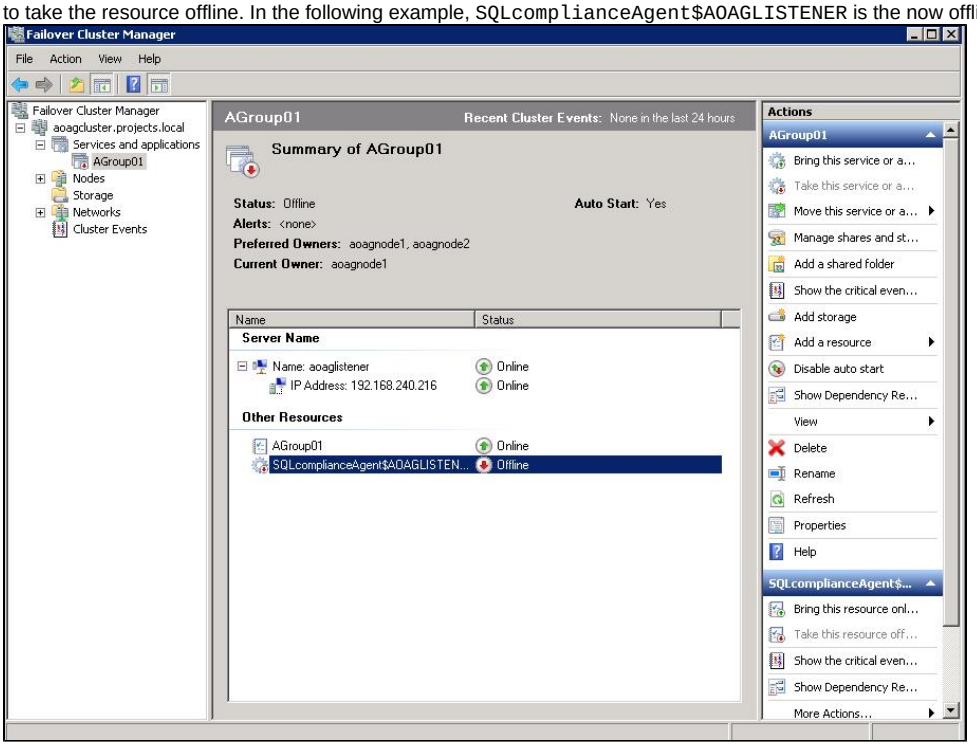


10. Make all necessary audit settings for the listener and AlwaysOn databases, and then update the configuration and begin collecting data. It is recommended to update the configuration before collecting data because users are unaware of which node is PRIMARY. After updating the configuration, be sure to click Refresh in the node context menu to apply the settings to the displayed information.

Removing a Listener from SQL Compliance Manager

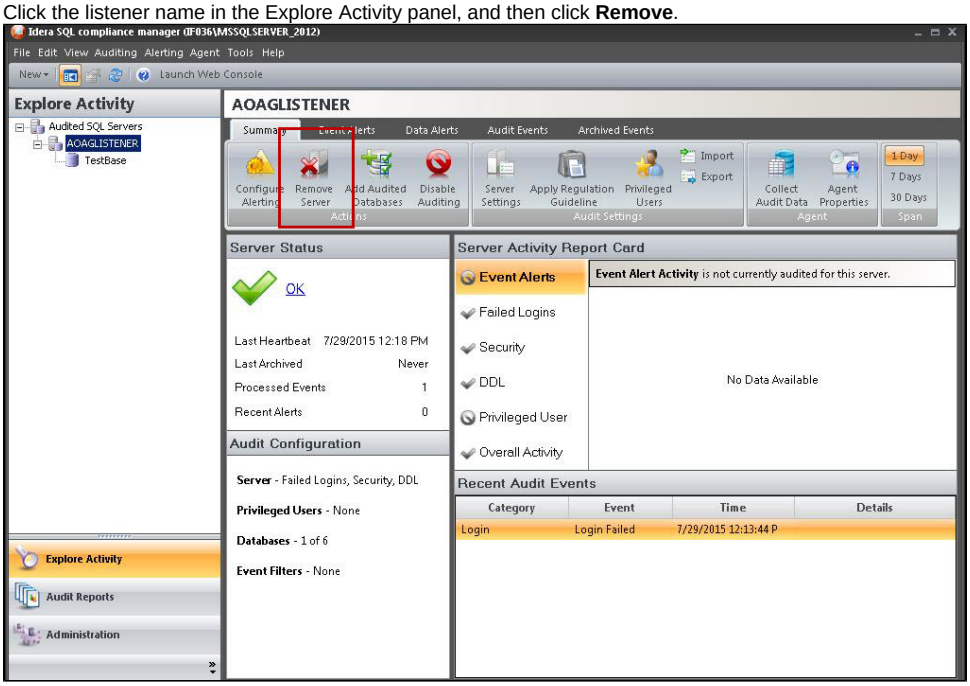
Use the following steps to remove the listener from SQL Compliance Manager auditing.

1. Open Server Manager.
2. In the Server Manager tree, click **Server Manager > Features > Failover Cluster Manager**. The system displays Failover Cluster Manager.
3. Take the cluster service agent *SQLcomplianceAgent$[listener name]* offline by selecting the service in the tree, clicking the cluster service agent in the Other Resources area, and then clicking **Take this resource offline** in the Actions panel. Verify in the confirmation message that you want to take the resource offline. In the following example, `SQLcomplianceAgent$AOAGLISTENER` is the now offline cluster service agent.

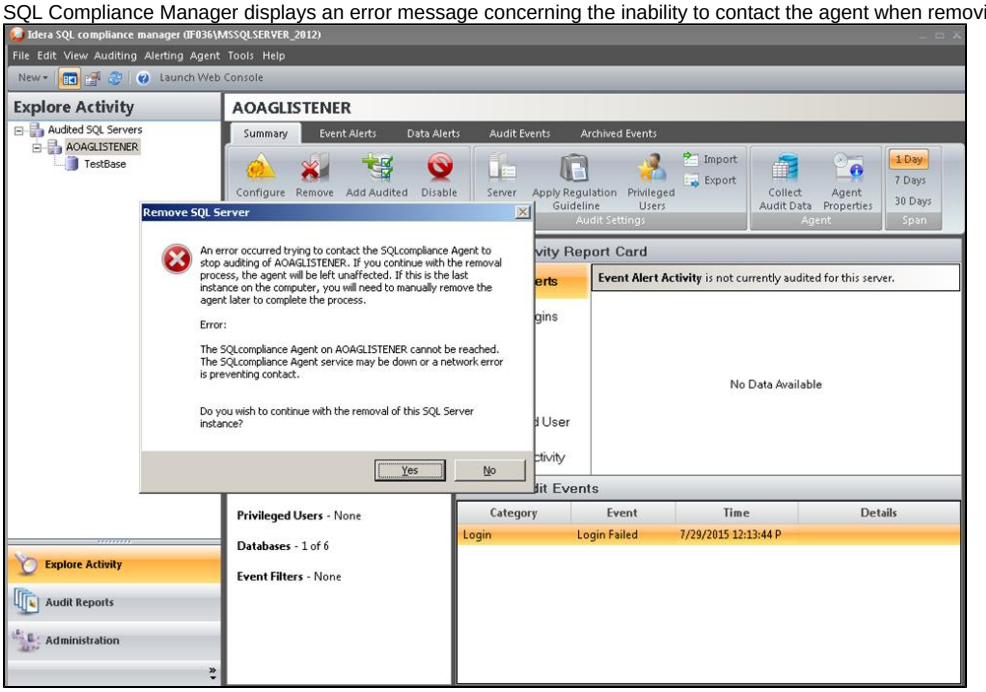


4. Keep Failover Cluster Manager open as you will return to this view after removing the listener from SQL Compliance Manager.
5. Open the SQL Compliance Manager Management Console.

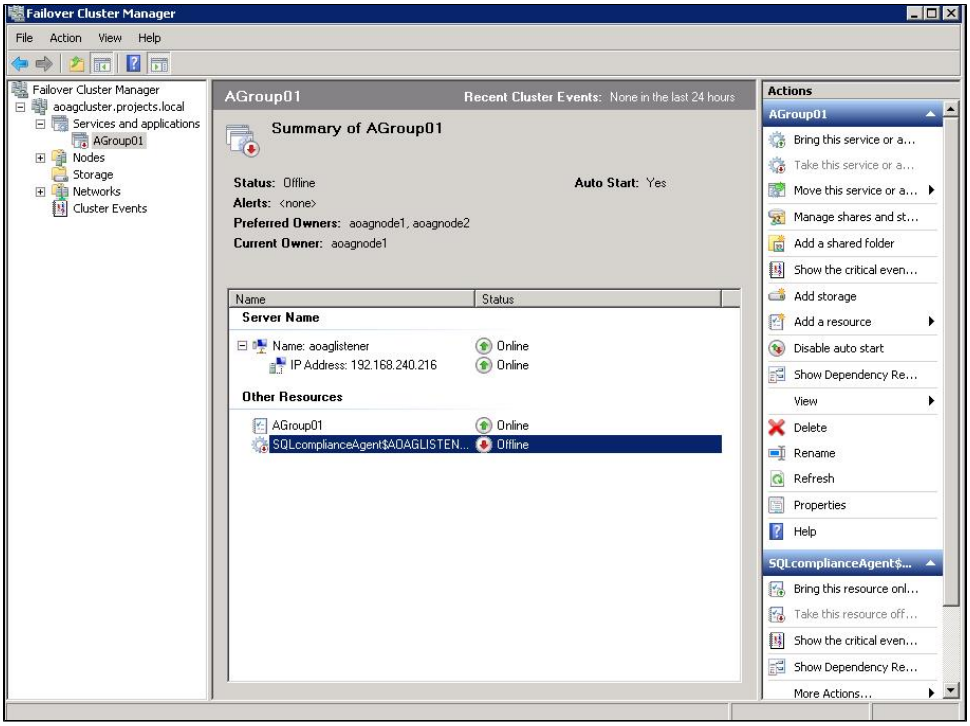
6. Click the listener name in the Explore Activity panel, and then click **Remove**.



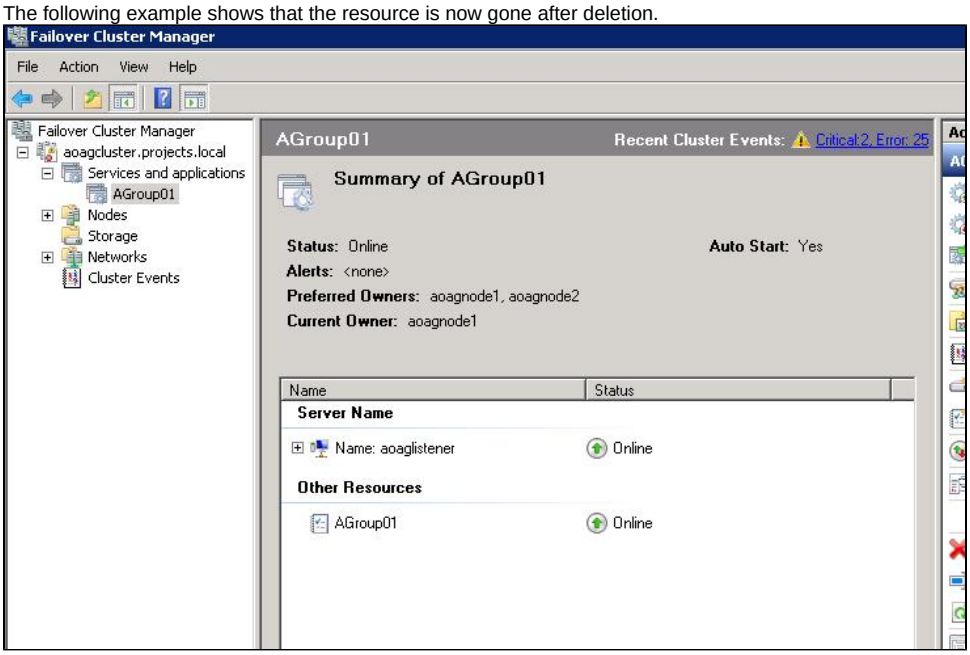
SQL Compliance Manager displays an error message concerning the inability to contact the agent when removing the listener.



7. Click **Yes** to confirm that you want to continue with removal of the instance.
8. ***If you want to re-add this listener for auditing at a later time*** , do not continue with the next steps. ***If you no longer want to use this listener*** , continue with the following steps for all nodes included in the AlwaysOn Availability Group.
9. Return to Failover Cluster Manager.
10. Delete the cluster service agent *SQLcomplianceAgent$[listener name]* by selecting the service in the tree, clicking the cluster service agent in the Other Resources area, and then clicking **Delete** in the Actions panel. Verify in the confirmation message that you want to delete the resource. In the following example, `SQLcomplianceAgent$AOAGLISTENER` is the cluster service agent.

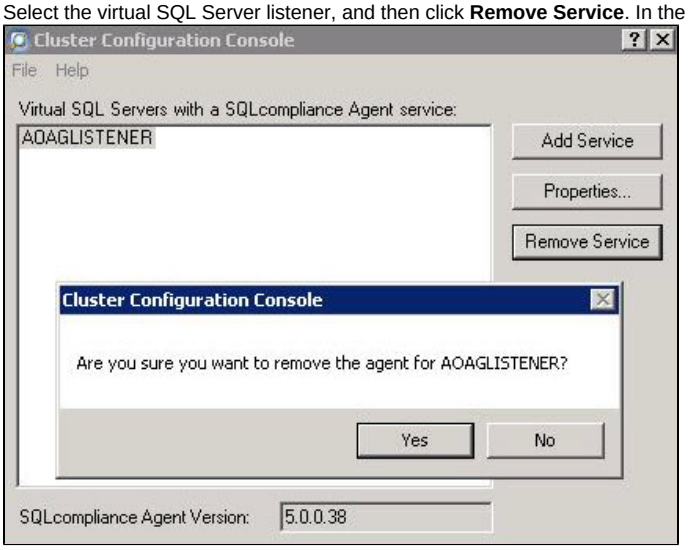


The following example shows that the resource is now gone after deletion.



11. Open the Cluster Configuration Console by clicking **Start > Idera > Cluster Configuration Console**.

12. Select the virtual SQL Server listener, and then click **Remove Service**. In the following example, `AOAGLISTENER` is the listener.



13. Click **Yes** in the confirmation message. The cluster service agent is removed.
14. ***If you no longer need to add listeners*** , uninstall the Cluster Configuration console.

Configuring the Nodes scenario

The Nodes scenario is recommended for users who want to audit regular databases and AlwaysOn databases on nodes that can be in PRIMARY or READONLY SECONDARY nodes.

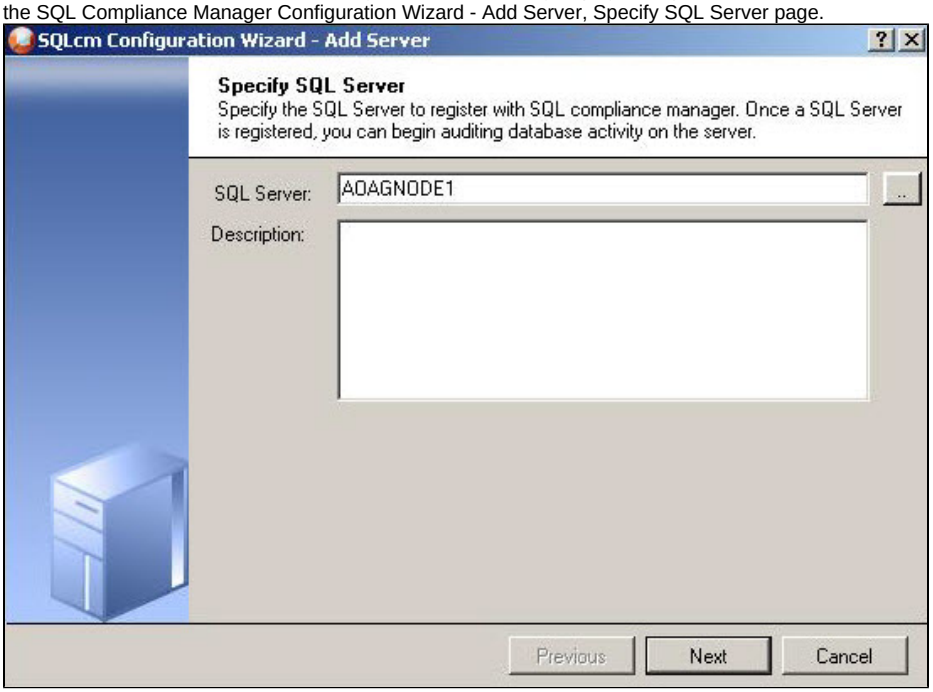
The SQL Compliance Manager administrator adds each node or instance of SQL Server involved in the availability group individually, which is the same process as with any regular SQL Server instance. You can then add any database that you want to audit. While you can automatically deploy the agent through the console, it is recommended that you manually deploy in case the automatic deployment fails. Note that the permissions requirements are the same as for the Listener scenario. For more information about permissions, see Permissions requirements.

AlwaysOn databases running as the secondary replica do not appear in the Add Database wizard unless the replica is marked as read-only. Note that the default status is non-readable.

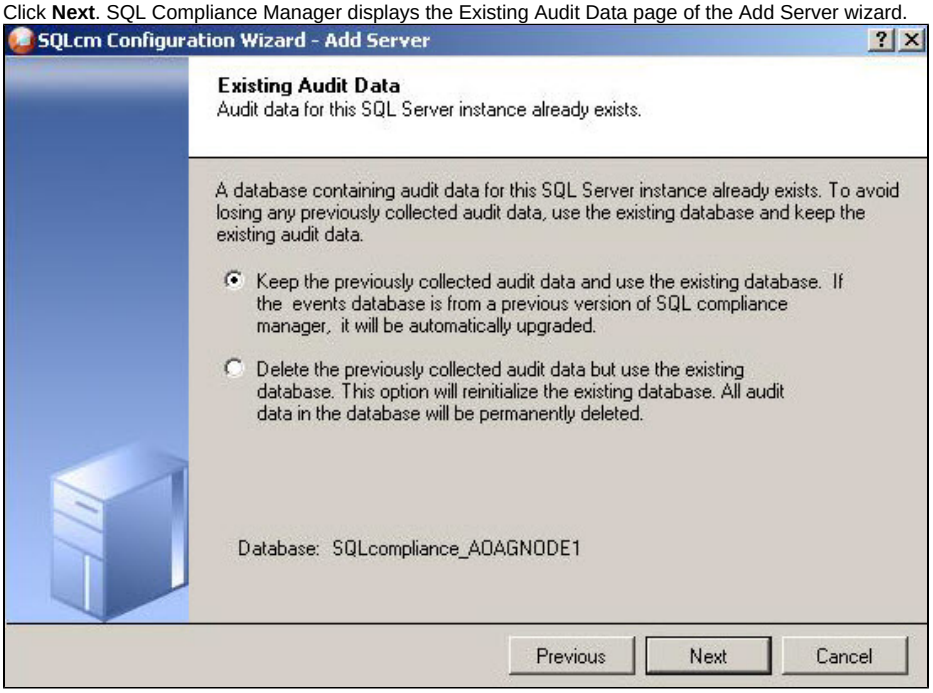
Example of manually deploying the agent

The following example shows the steps necessary to manually deploy the agent service to all AlwaysOn nodes. This example uses `AOAGNODE1` and `AOAGNODE2`, which are in the AlwaysOn group.

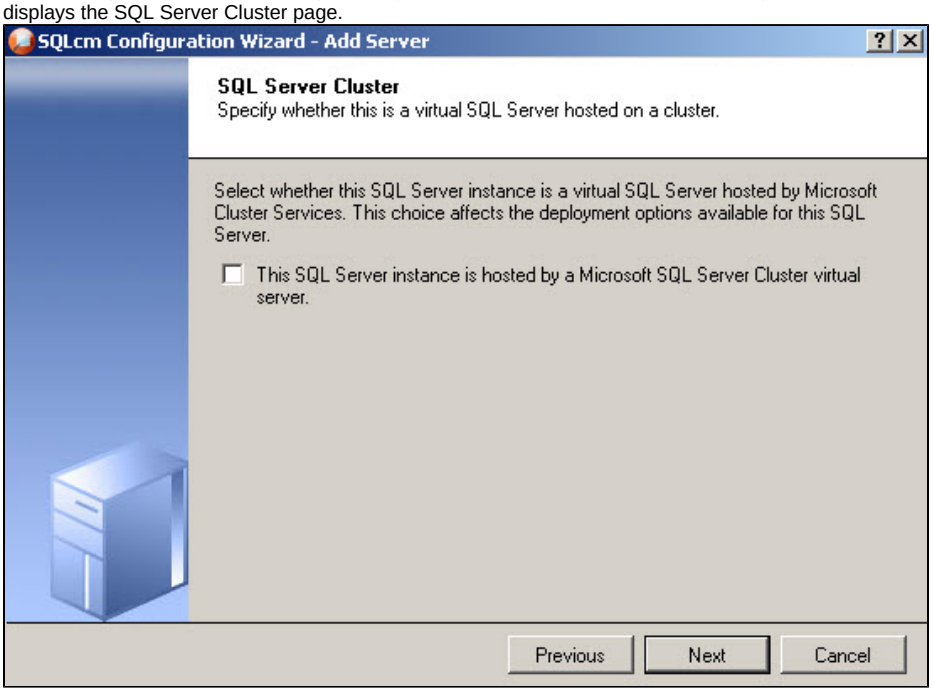
1. Start the SQL Compliance Manager Management Console.
2. Select the SQL Server instance to which you want to manually deploy the agent, and then click **Add Server**. SQL Compliance Manager opens the SQL Compliance Manager Configuration Wizard - Add Server, Specify SQL Server page.



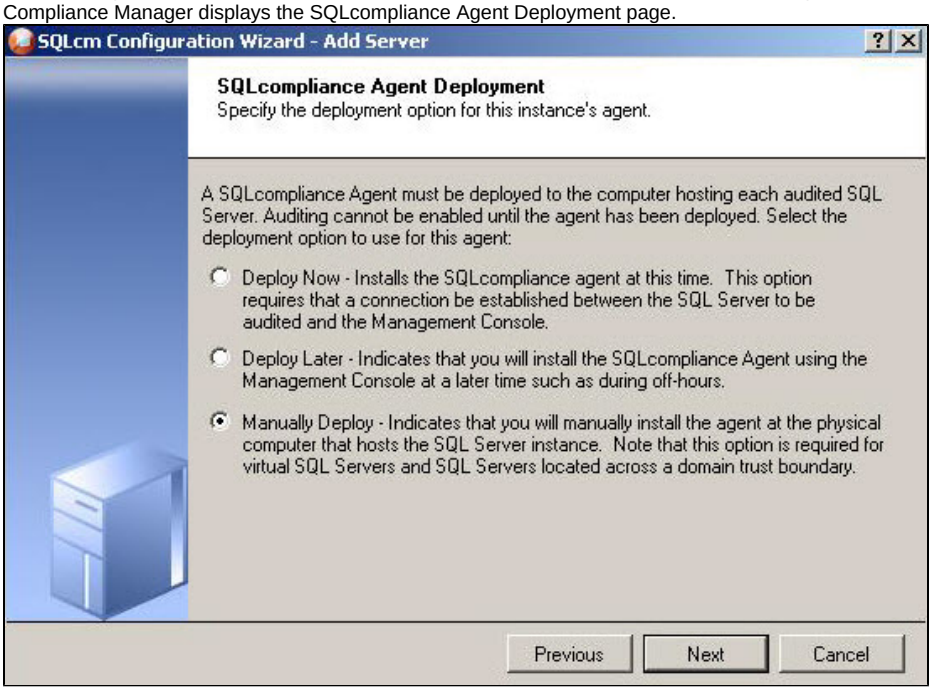
3. Click **Next**. SQL Compliance Manager displays the Existing Audit Data page of the Add Server wizard.



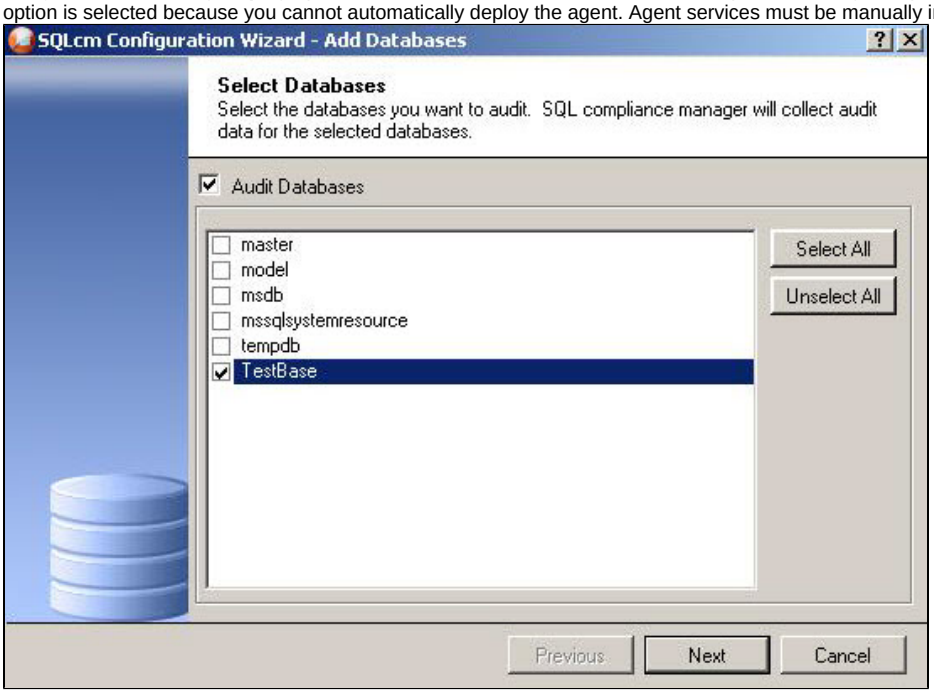
4. Select the option to retain all of the previously-collected audit data and use the existing database, and then click **Next**. SQL Compliance Manager displays the SQL Server Cluster page.



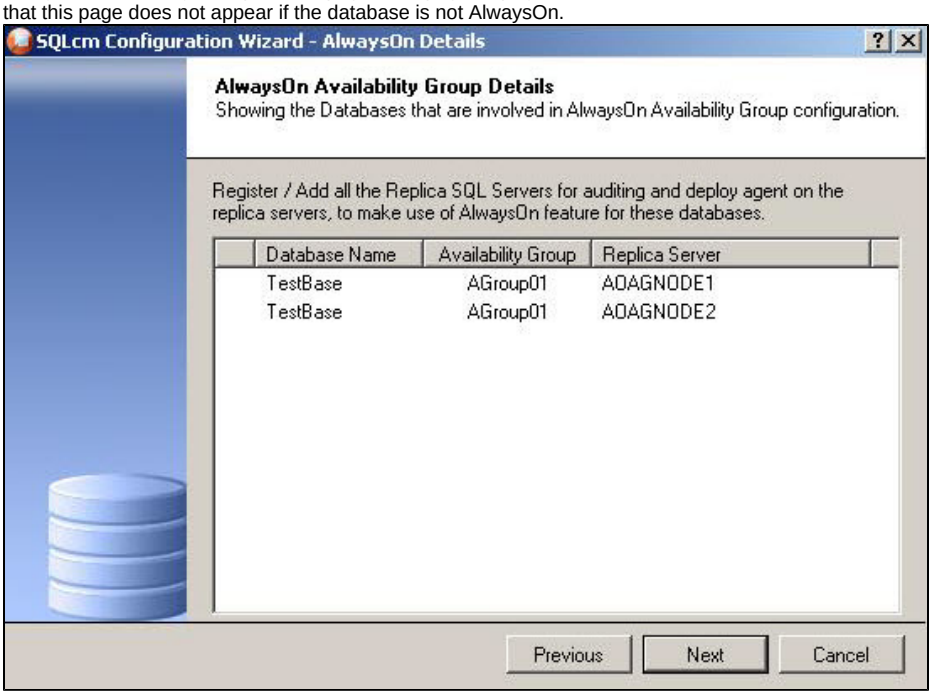
5. Check this option if the instance is a virtual SQL Server, and then click **Next**. For this example, this is a regular SQL Server instance. SQL Compliance Manager displays the SQLcompliance Agent Deployment page.



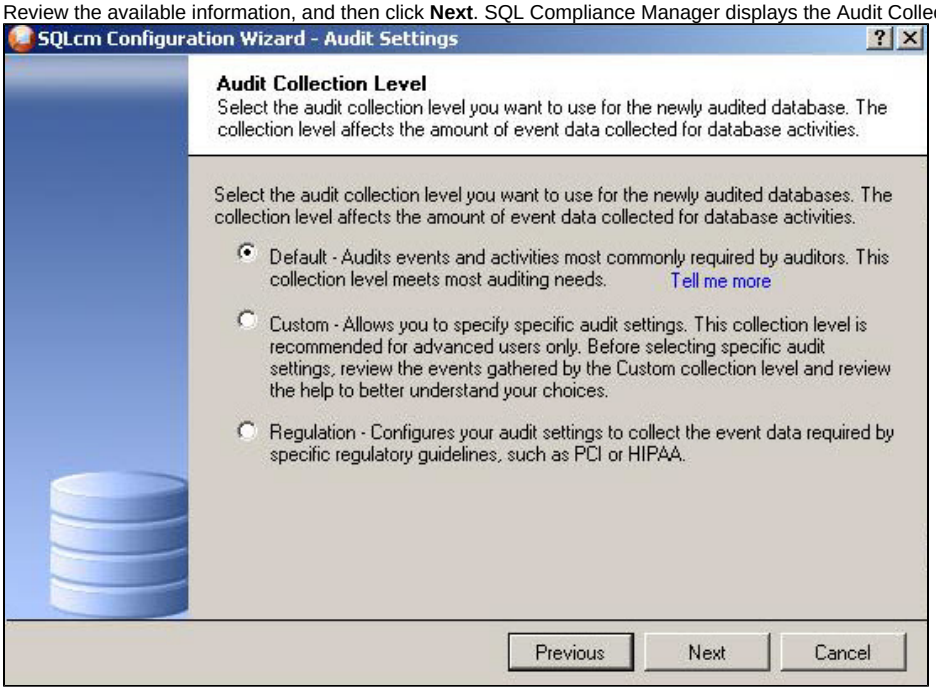
6. Verify that the **Manually Deploy** option is selected, and then click **Next**. SQL Compliance Manager displays the Select Databases page. This option is selected because you cannot automatically deploy the agent. Agent services must be manually installed on each node.



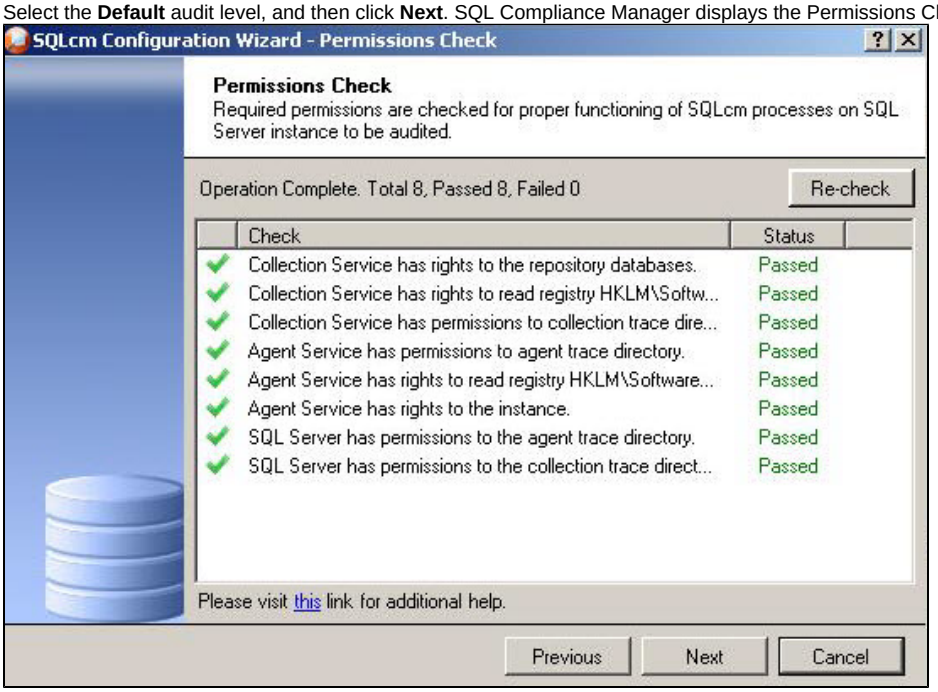
7. Select the AlwaysOn database, and then click **Next**. This example uses the databases `TestBase`. SQL Compliance Manager then displays the AlwaysOn Availability Group Details page. This page displays information about all nodes where the AlwaysOn database will be replicated. Note that this page does not appear if the database is not AlwaysOn.



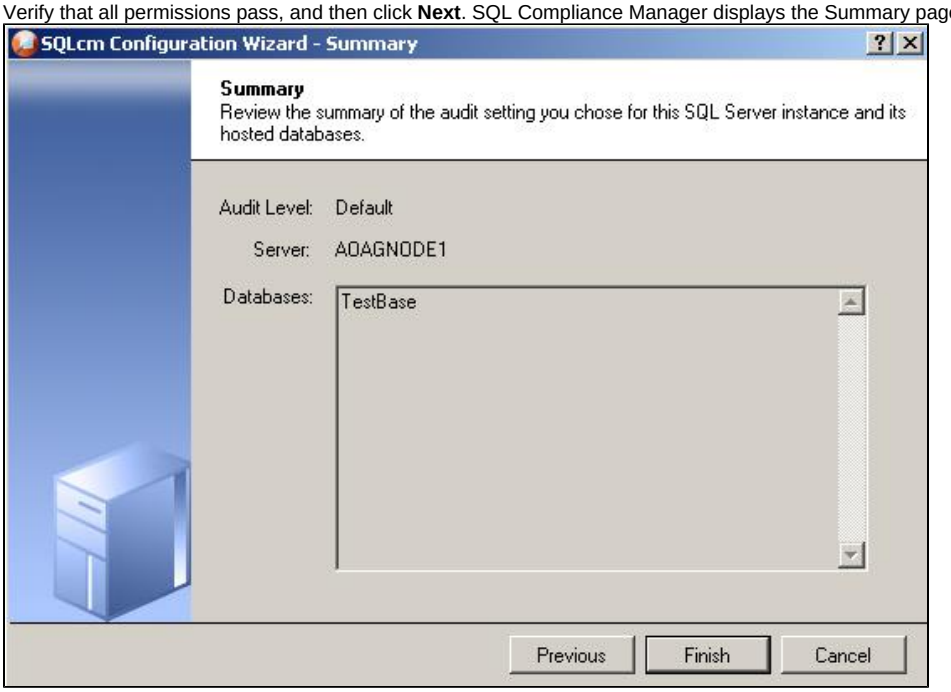
8. Review the available information, and then click **Next**. SQL Compliance Manager displays the Audit Collection Level page.



9. Select the **Default** audit level, and then click **Next**. SQL Compliance Manager displays the Permissions Check page.

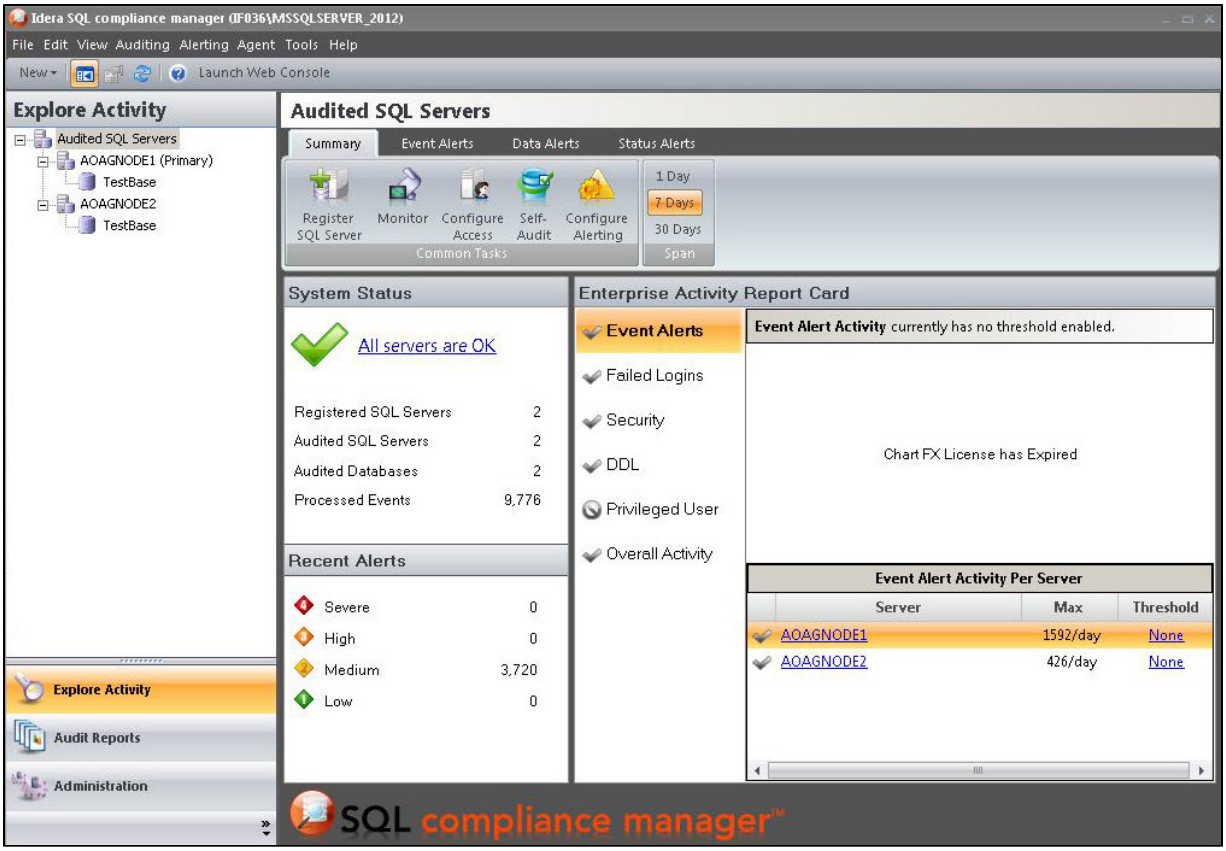


10. Verify that all permissions pass, and then click **Next**. SQL Compliance Manager displays the Summary page.



11. Click **Finish**.

After adding all nodes, the SQL Compliance Manager displays the primary node, as shown in the following image. You also now can audit any AlwaysOn databases in the added nodes if they are in PRIMARY or READ-ONLY SECONDARY roles.



Exporting/importing audit settings for all AlwaysOn nodes

Users can select all of the appropriate audit settings for each AlwaysOn database and export these settings as XML files. You then can import the files into the remaining instances or nodes in the group.

To import the audit settings to each node, click **Import** on the Summary tab. Choose the exported XML file, the information you want to import, and the servers to which you want to apply the settings. Select all the other servers in the availability group as the target for audit settings. After users apply the settings from the file, each member of their availability group is set to audit in exactly the same way as noted in the exported file. This process also allows you to add additional databases that are the part of an availability group on these servers.

Removing an AlwaysOn node from SQL Compliance Manager

To remove an AlwaysOn node from SQL Compliance Manager, first stop the agent service using the Failover Cluster Manager before attempting to remove a node instance from SQL Compliance Manager. This step must be performed if you may want to add back to SQL Compliance Manager the removed node using the Manual Deployment option without any agent deployment. In this case, ignore the error message that appears after you remove the node.