

Configuring Listener scenario

The Listener scenario is recommended for users who want to audit only AlwaysOn databases on the Primary node of the Availability Group by registering the Availability Group Listener for auditing in SQL Compliance Manager. **If you want to audit read-only Secondary nodes**, use the [Nodes](#) scenario instead.

Review the following steps to successfully configure your Availability Group Listener for auditing:

1. Install the clustered Agent service on all Availability Group nodes using the SQL Compliance Manager Cluster Configuration Console.
2. Create a clustered resource for the newly installed Agent service in Failover Cluster Manager.
3. Register the Availability Group Listener in SQL Compliance Manager.

1. Install the cluster Agent service on all Availability Group 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.



Before stepping through the following instructions, ensure that the SQL CM Collection Server, the Management Console, and the Repository Databases are already installed.

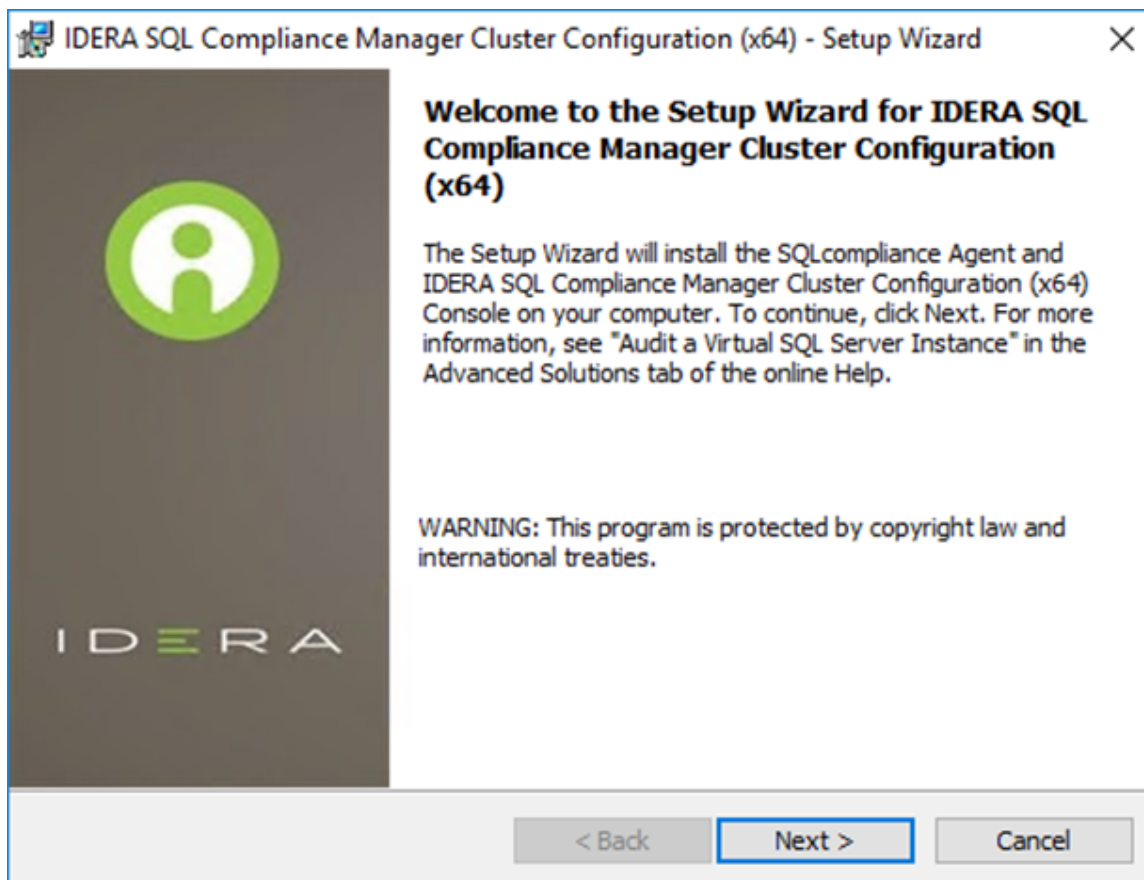
- Please review step 10 in [How to install SQL Compliance Manager](#) to install these components in a standalone server.
- Please review the steps to [Install SQL Compliance Manager Collection Service on Cluster nodes to install these components in a clustered environment](#).

1. From the installation folder of the SQL Compliance Manager Collection Service on the Collection and Repository database server, copy the *SQLComplianceClusterSetup.exe* file onto the nodes of the Availability Group. To install the Cluster Configuration Console on the nodes of the Availability Group, you are going to be auditing. This is located by default at the following path:

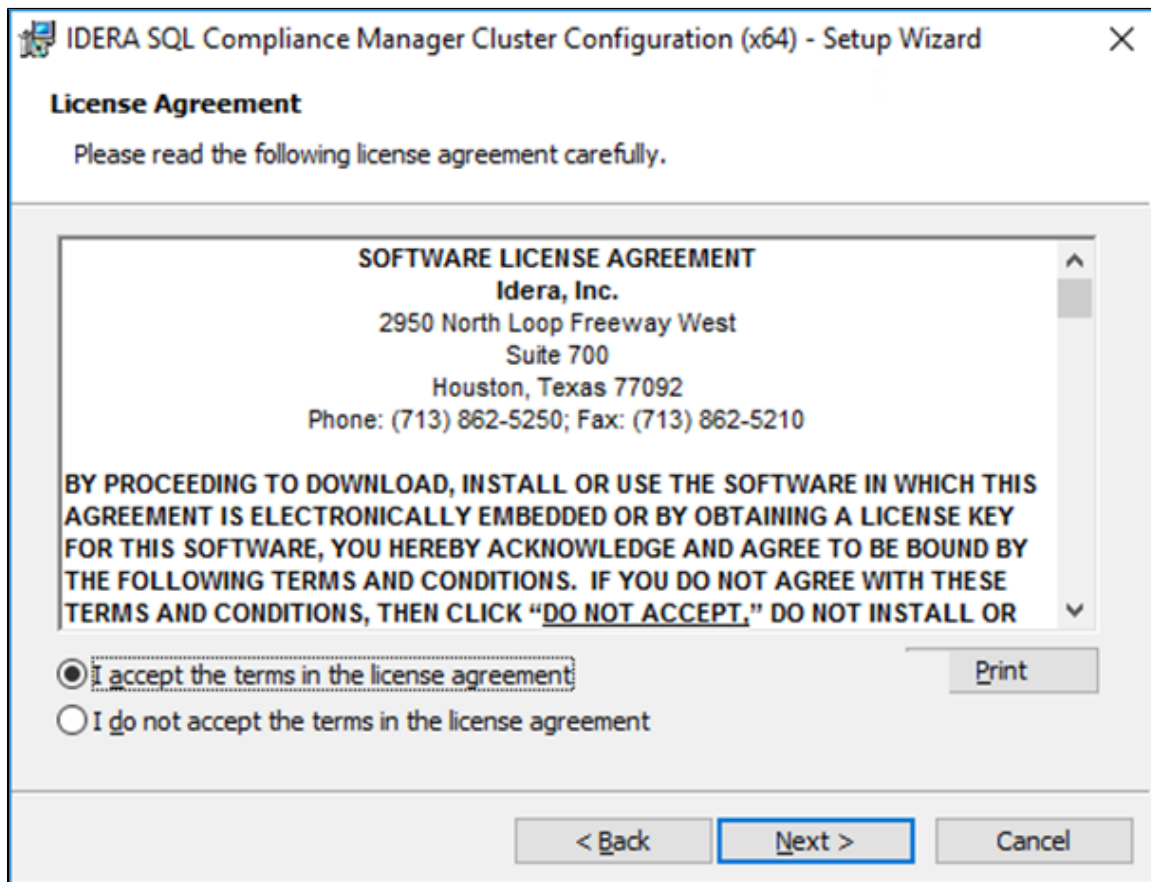
C:\Program Files\Idera\SQLcompliance

	SQLcomplianceClusterSetup-x64	1/21/2021 6:08 AM	Application	10,829 KB
--	-------------------------------	-------------------	-------------	-----------

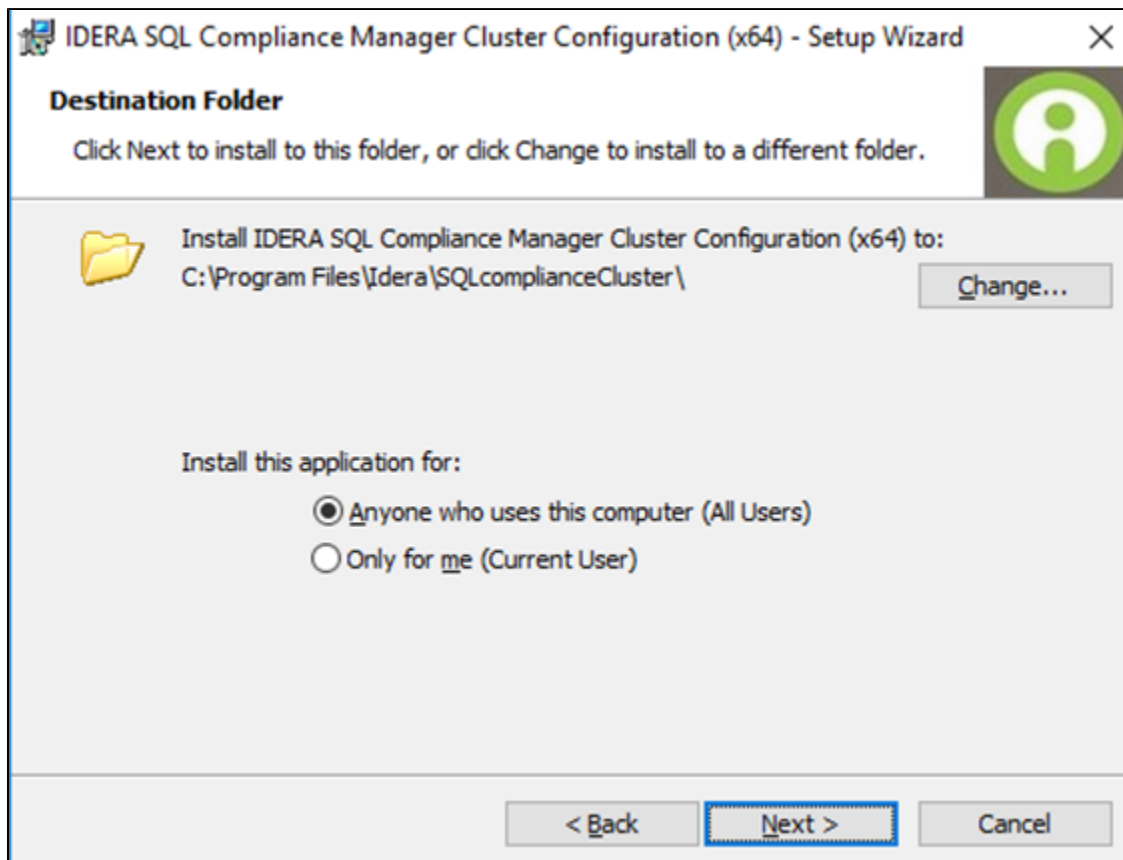
2. Beginning with the primary node of the Availability Group. Run the *SQLcomplianceClusterSetup.exe* to launch the installation wizard.
3. Once the setup wizard launches, click the **Next** button to proceed to the License Agreement.



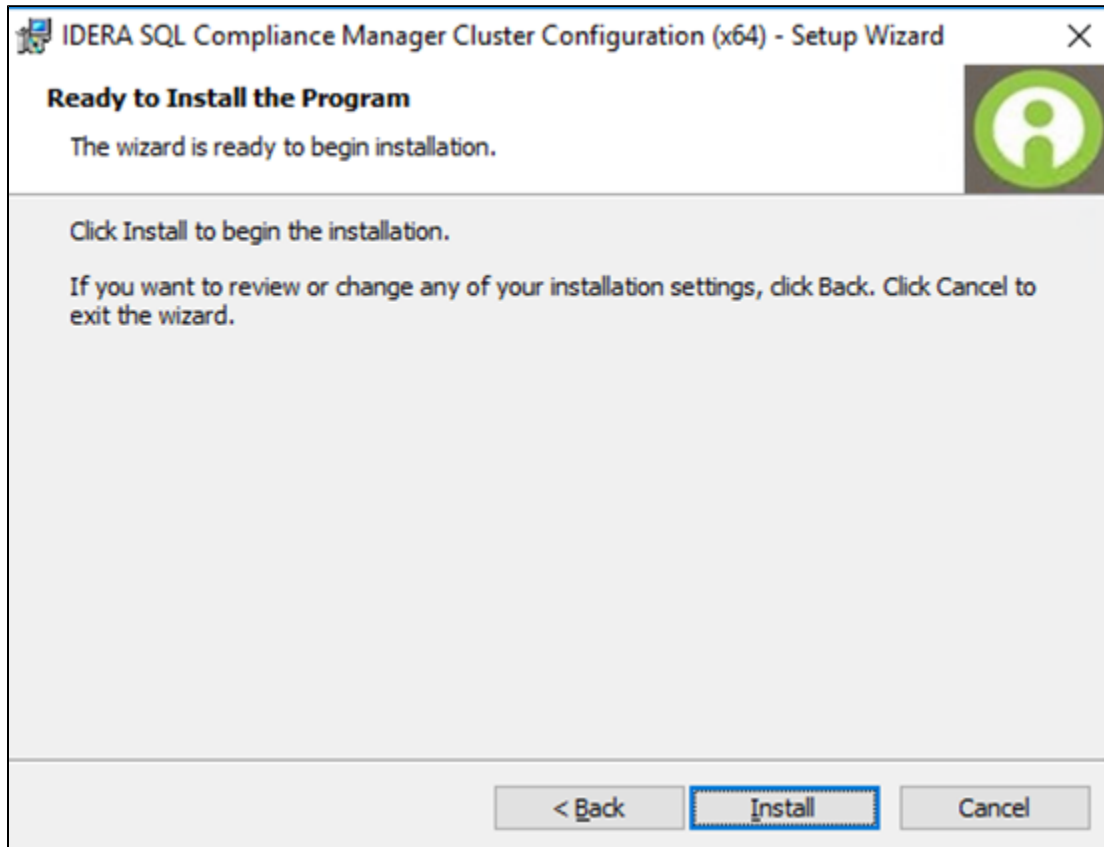
4. Read the license agreement, select the option to accept the license agreement terms, and click **Next**.



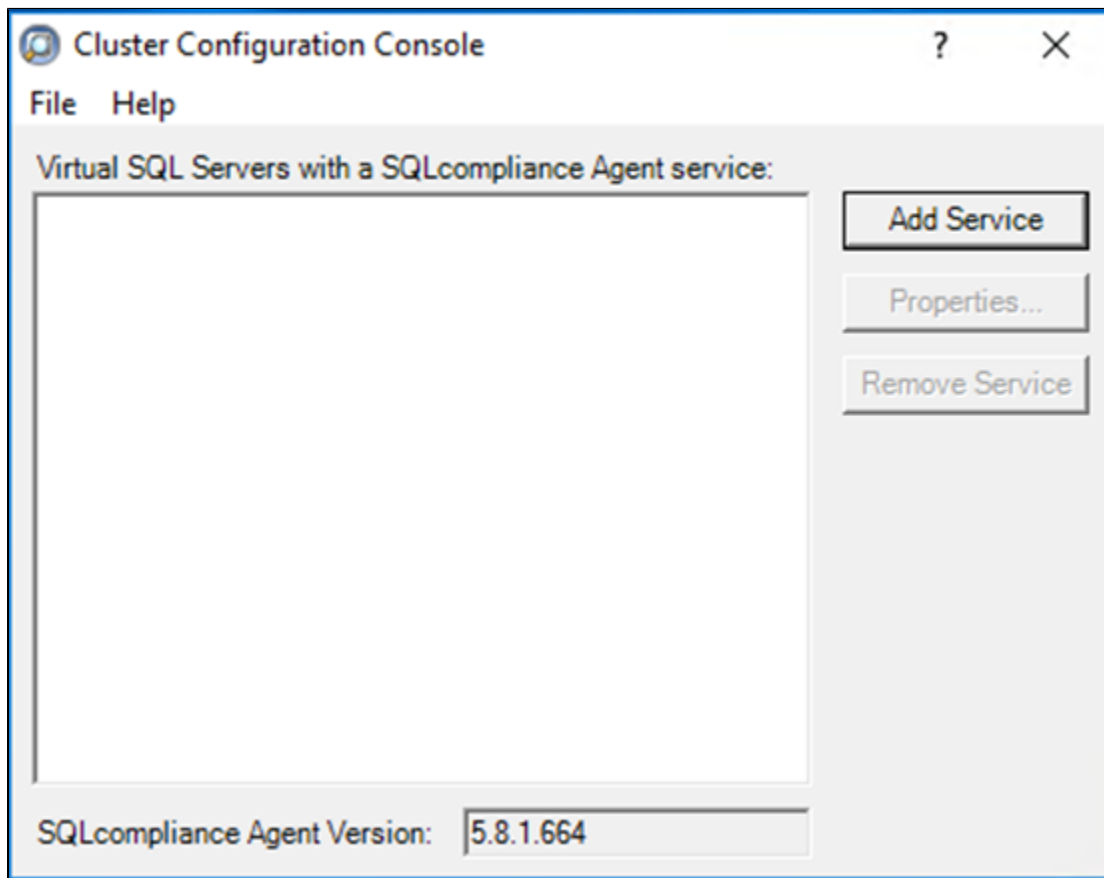
5. Select the destination path in which you want to install the IDERA Cluster Configuration Console.



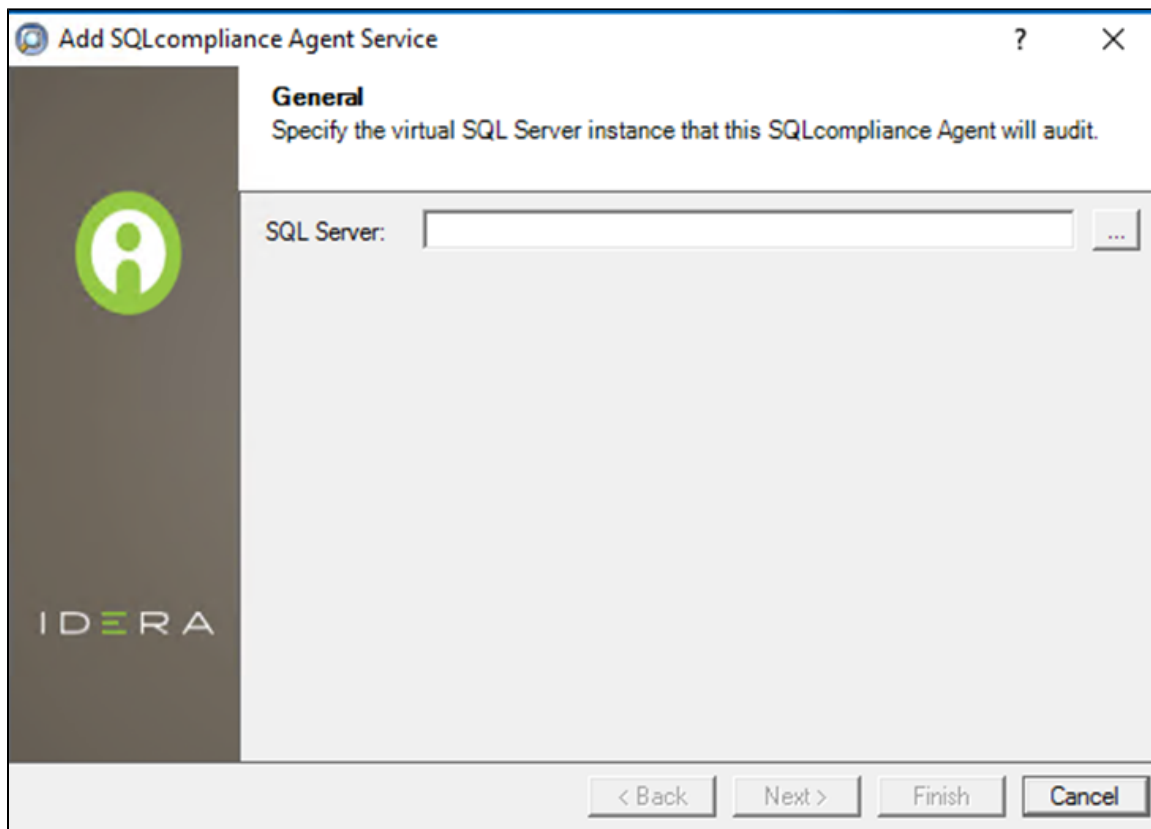
6. Click **Install** to begin the installation.



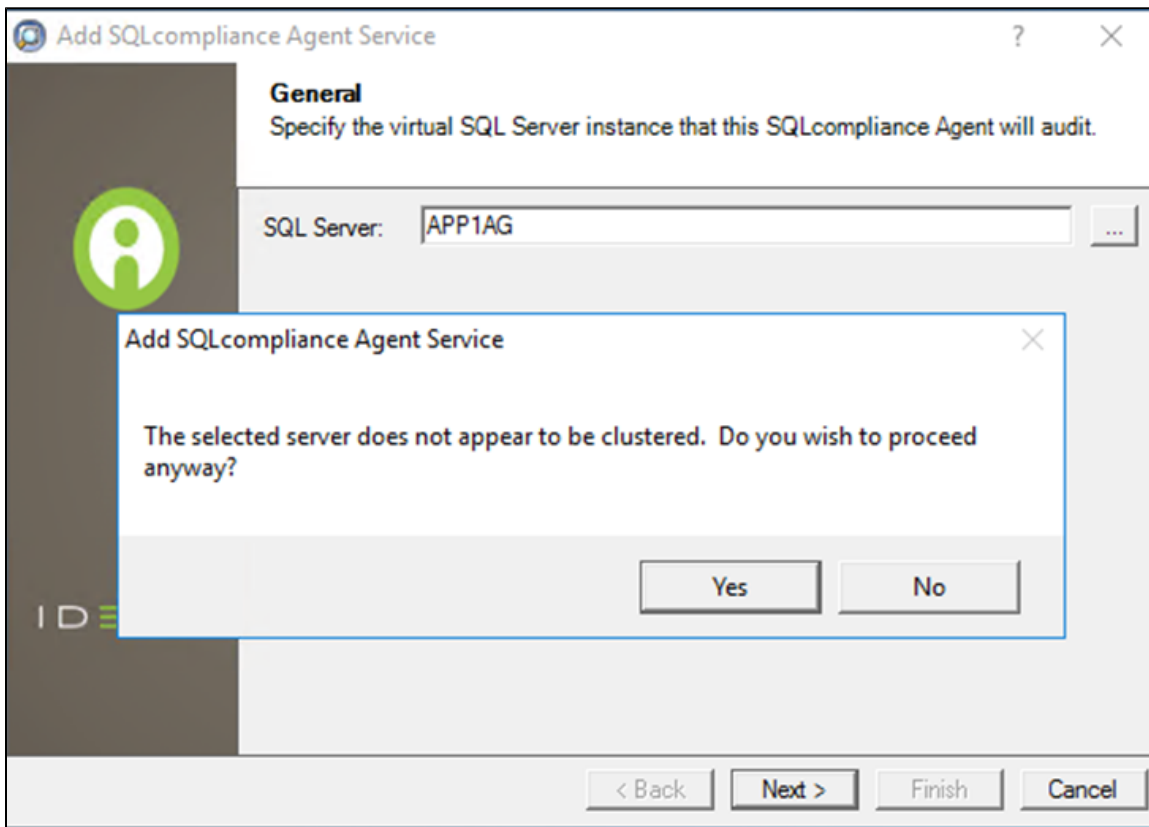
7. The Cluster Configuration Console launches automatically after installation.



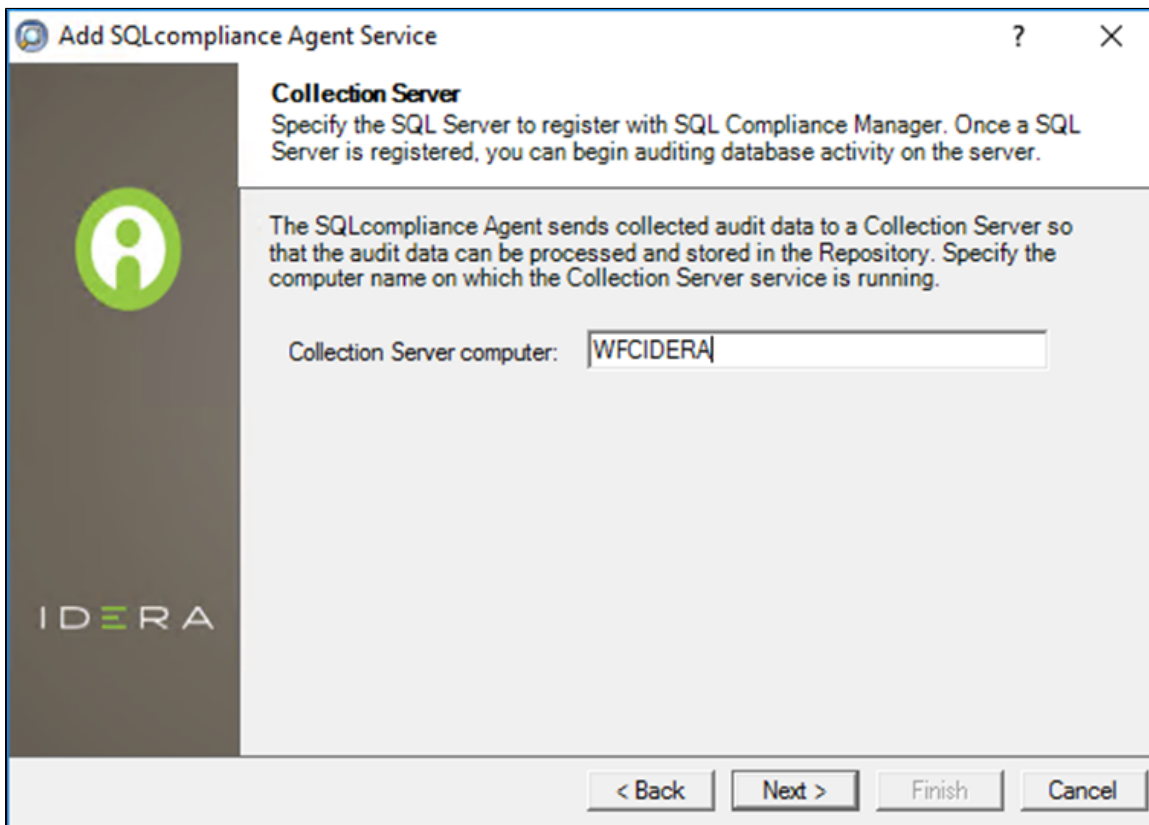
8. Click **Add Service** to register the Availability Group Listener. SQL Compliance Manager displays the **Add SQLcompliance Agent Service - General** window, where the name of the Availability Group Listener to audit will need to be entered into the SQL Server textbox.



9. Once the name of the Availability Group Listener to audit has been entered, click **Next**. If you receive a message stating that the selected SQL Server instance is not clustered, click **Yes** to confirm. When configuring a Listener scenario, this is the correct behavior and ensures that the selected SQL Server instance is hosted on a Windows Failover Cluster.



10. On the **Collection Server** dialog window, specify the server's name where the SQL Compliance Manager Collection Service is installed and click **Next**.



Add SQLcompliance Agent Service

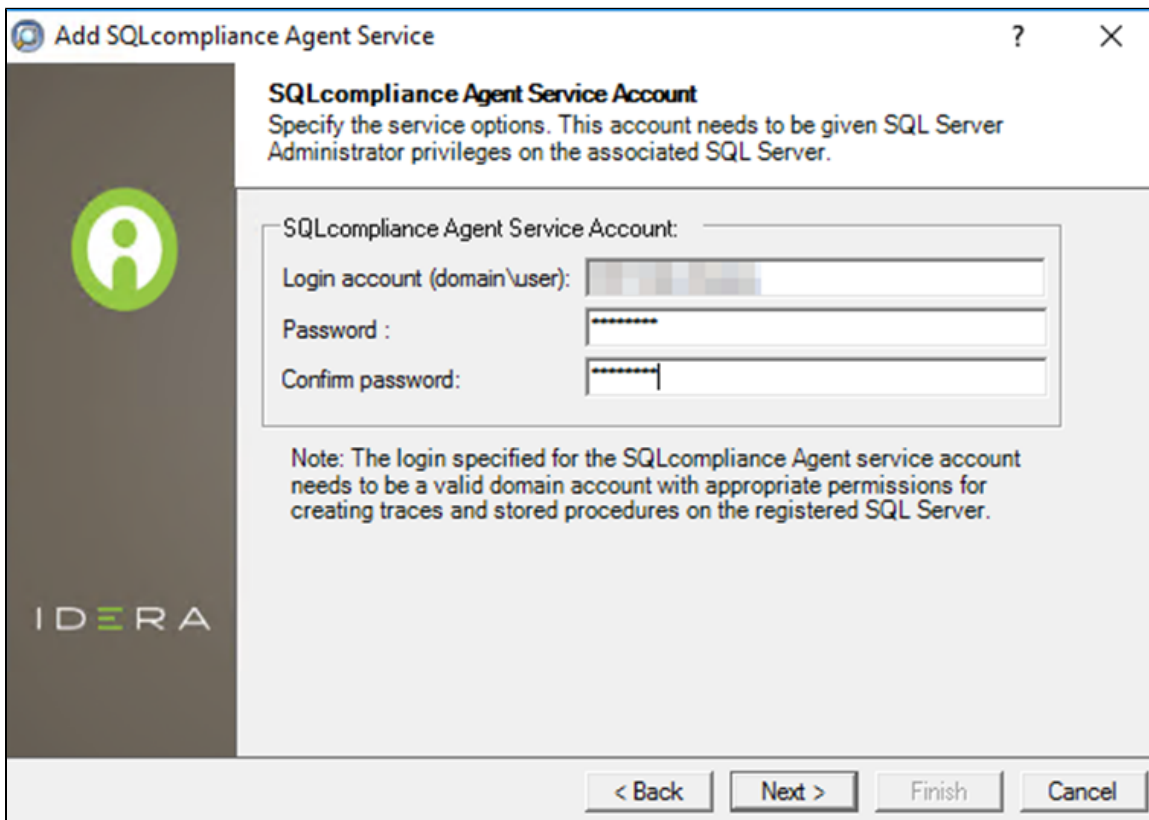
Collection Server
Specify the SQL Server to register with SQL Compliance Manager. Once a SQL Server is registered, you can begin auditing database activity on the server.

The SQLcompliance Agent sends collected audit data to a Collection Server so that the audit data can be processed and stored in the Repository. Specify the computer name on which the Collection Server service is running.

Collection Server computer:

Navigation buttons: < Back, Next >, Finish, Cancel

11. On the **SQLcompliance Agent Service Account** dialog window, specify the login credentials for the Agent service account and click **Next**. This account must have local administrator privileges, and sysadmin permissions on the SQL Server nodes of the Availability Group set up for auditing.



Add SQLcompliance Agent Service

SQLcompliance Agent Service Account
Specify the service options. This account needs to be given SQL Server Administrator privileges on the associated SQL Server.

SQLcompliance Agent Service Account:

Login account (domain\user):

Password:

Confirm password:

Note: The login specified for the SQLcompliance Agent service account needs to be a valid domain account with appropriate permissions for creating traces and stored procedures on the registered SQL Server.

Navigation buttons: < Back, Next >, Finish, Cancel

12. On the **SQLcompliance Agent Trace Directory** dialog window, specify the path where audit trace files will be created for the audit process and click **Next**. Note that the service account specified to run the Agent service must have read and write permissions on this trace directory folder.



The screenshot shows a Windows-style dialog box titled "Add SQLcompliance Agent Service". On the left is a dark vertical bar with a green circular icon containing a white person silhouette and the word "IDERA" in white. The main area has a title "SQLcompliance Agent Trace Directory" and a subtitle "Specify directory for temporary storage of audit data". Below this is a paragraph of text explaining that the agent stores audit data in a trace directory on the host computer and that specifying a directory on a shared disk prevents data loss during a failover. A text box labeled "Trace Directory:" contains the path "C:\Program Files\Idera\SQLcompliance\AgentTraceFiles". Below the text box is a note: "Note: This directory will be created by the SQLcompliance Agent when Before and After data auditing enabled." At the bottom are four buttons: "< Back", "Next >", "Finish", and "Cancel".

Add SQLcompliance Agent Service

SQLcompliance Agent Trace Directory
Specify directory for temporary storage of audit data

The SQLcompliance Agent temporarily stores collected audit data in a trace directory on the computer that hosts the SQL Server instance. Specify a trace directory on a shared data disk in the virtual instance's cluster group. This prevents loss of gathered audit data during a failover.

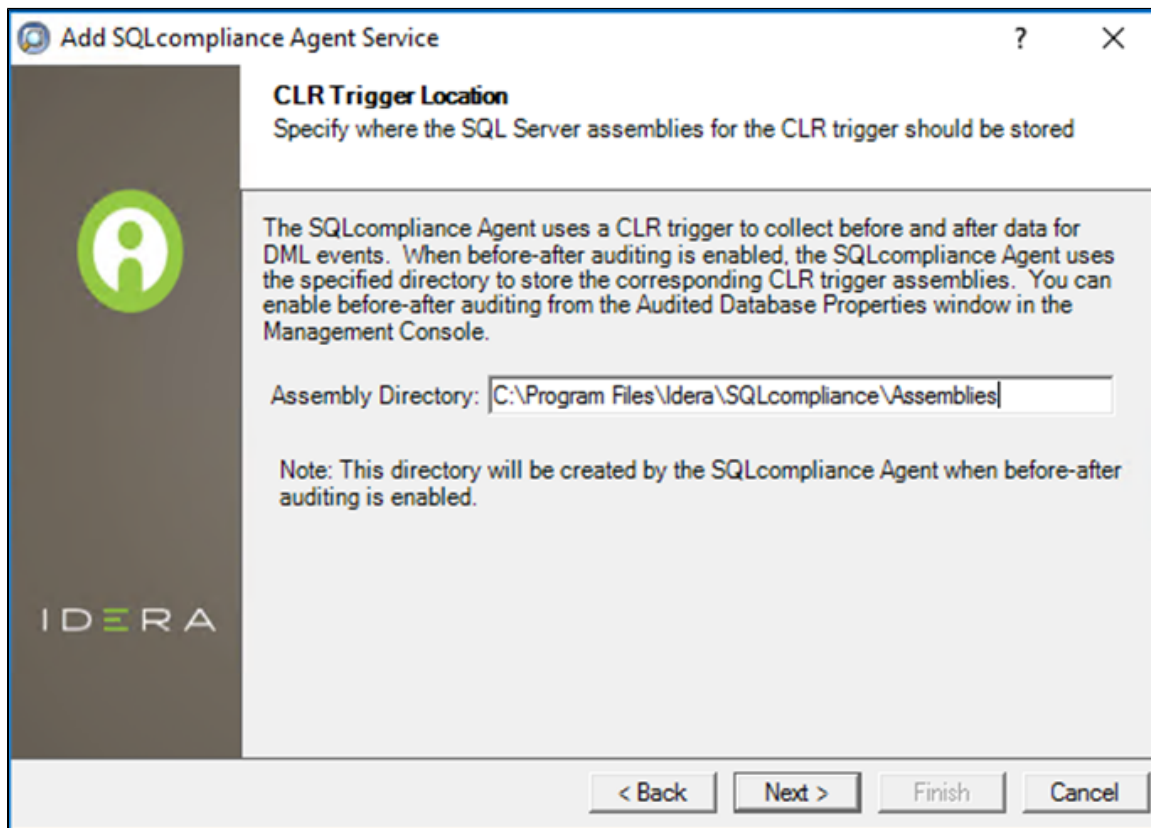
Trace Directory:

Note: This directory will be created by the SQLcompliance Agent when Before and After data auditing enabled.

IDERA

< Back Next > Finish Cancel

13. On the **CLR Trigger Location** dialog window, specify the location where you want the SQL Compliance Manager Agent to store the corresponding CLR trigger assemblies, and click **Next**. Note that the service account specified to run the Agent service must have read and write permissions on this trace directory folder.



Add SQLcompliance Agent Service

CLR Trigger Location
Specify where the SQL Server assemblies for the CLR trigger should be stored

The SQLcompliance Agent uses a CLR trigger to collect before and after data for DML events. When before-after auditing is enabled, the SQLcompliance Agent uses the specified directory to store the corresponding CLR trigger assemblies. You can enable before-after auditing from the Audited Database Properties window in the Management Console.

Assembly Directory:

Note: This directory will be created by the SQLcompliance Agent when before-after auditing is enabled.

IDERA

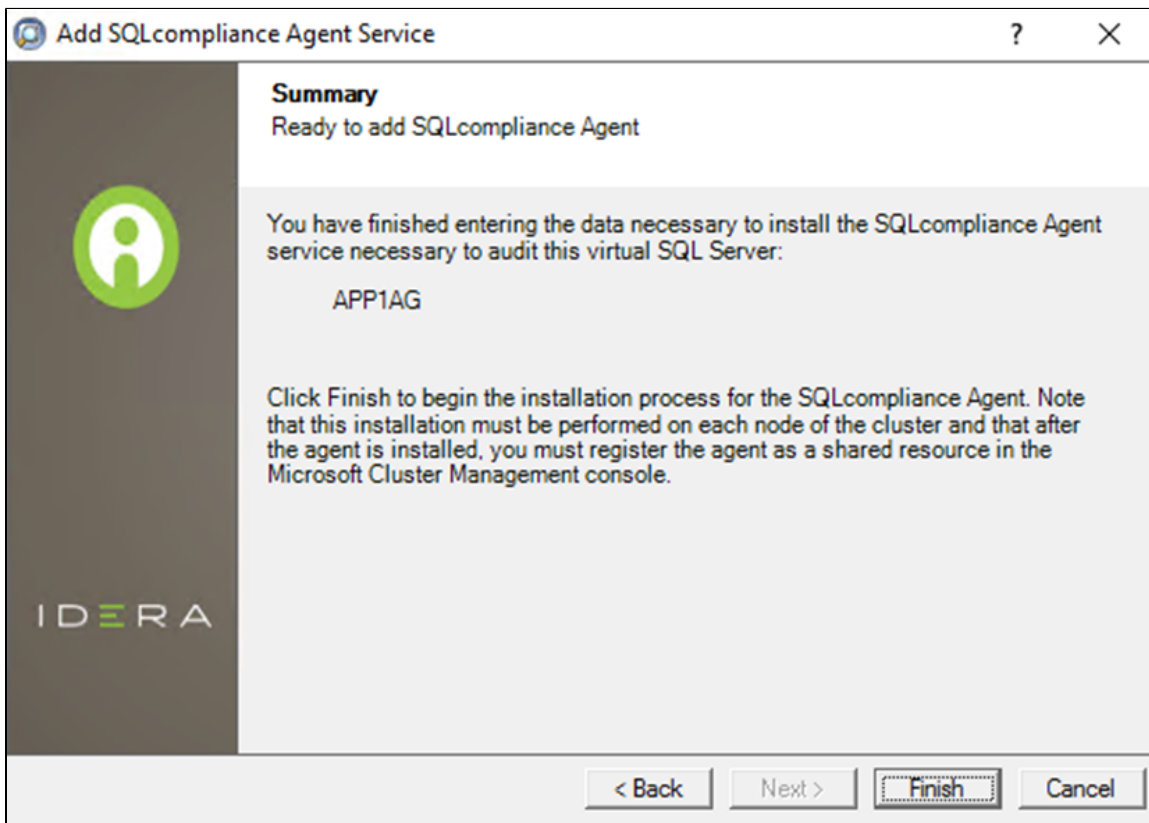
< Back Next > Finish Cancel



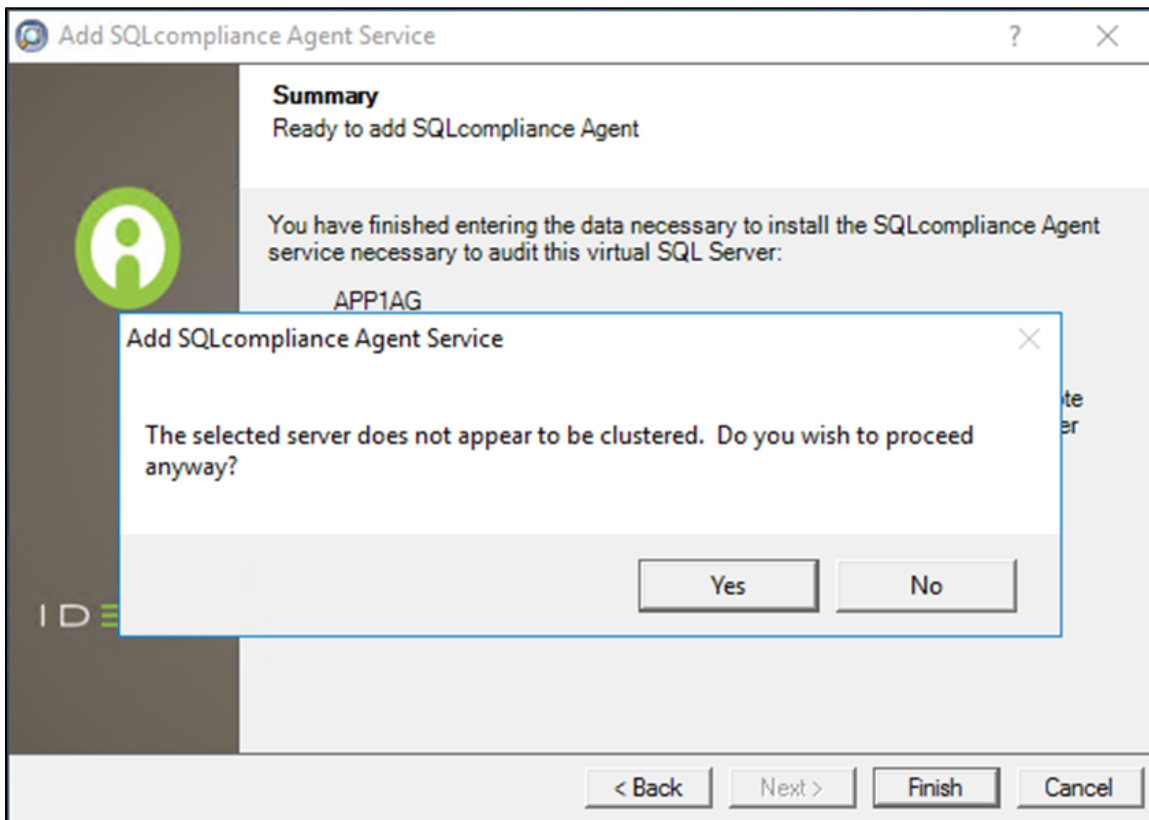
Note

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

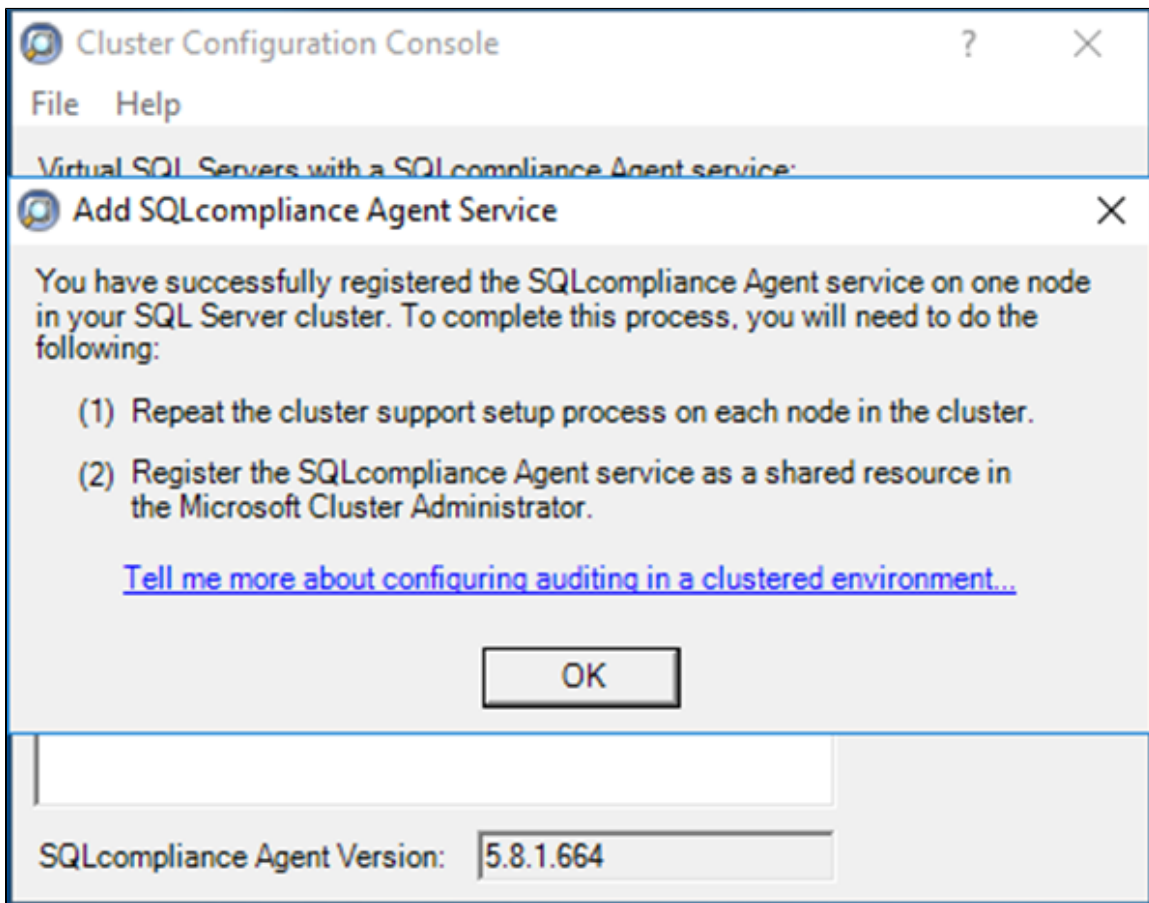
14. Review the configuration **Summary** and click **Finish**.



15. The wizard asks for another confirmation to proceed with the registration of the Availability Group Listener as a virtual cluster server registration, click



16. The IDERA Cluster Configuration Console displays a confirmation message stating that you have successfully added the SQL Compliance Manager Agent. Click **OK**.



Note

Repeat these steps on each remaining node in your AlwaysOn Availability Group. Consider using the same folder structure for the *Agent Trace directory* and the *CLR Trigger location* when setting the Agent up on the secondary nodes. When you are finished configuring all the nodes, proceed with the steps below.

2. Create a clustered resource for the newly installed Agent service in Failover Cluster Manager



The Registry Replication tab is not available in Windows Server 2012.

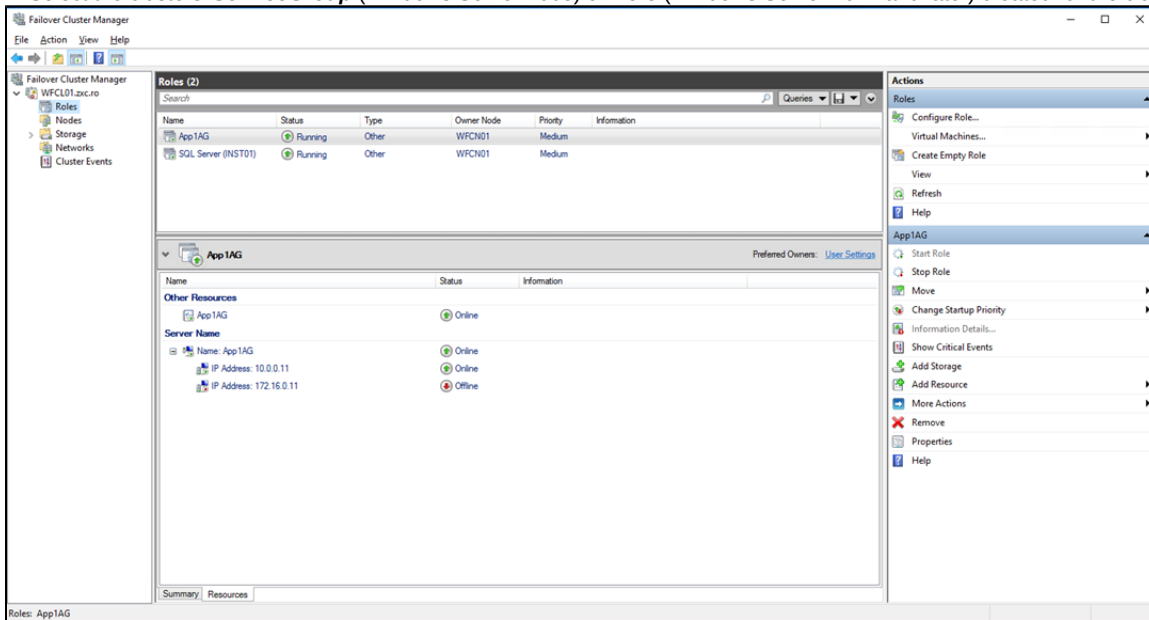
If you are using Windows Server 2012, you must use the "Add-ClusterCheckpoint" PowerShell cmdlet to add the necessary setting.

For more information, see [Add ClusterCheckpoint](#).

Use the following steps only on the Primary node of the AlwaysOn Availability Group before finally registering the Availability Group Listener for auditing into the SQL Compliance Manager console.

1. Launch the **Failover Cluster Manager**

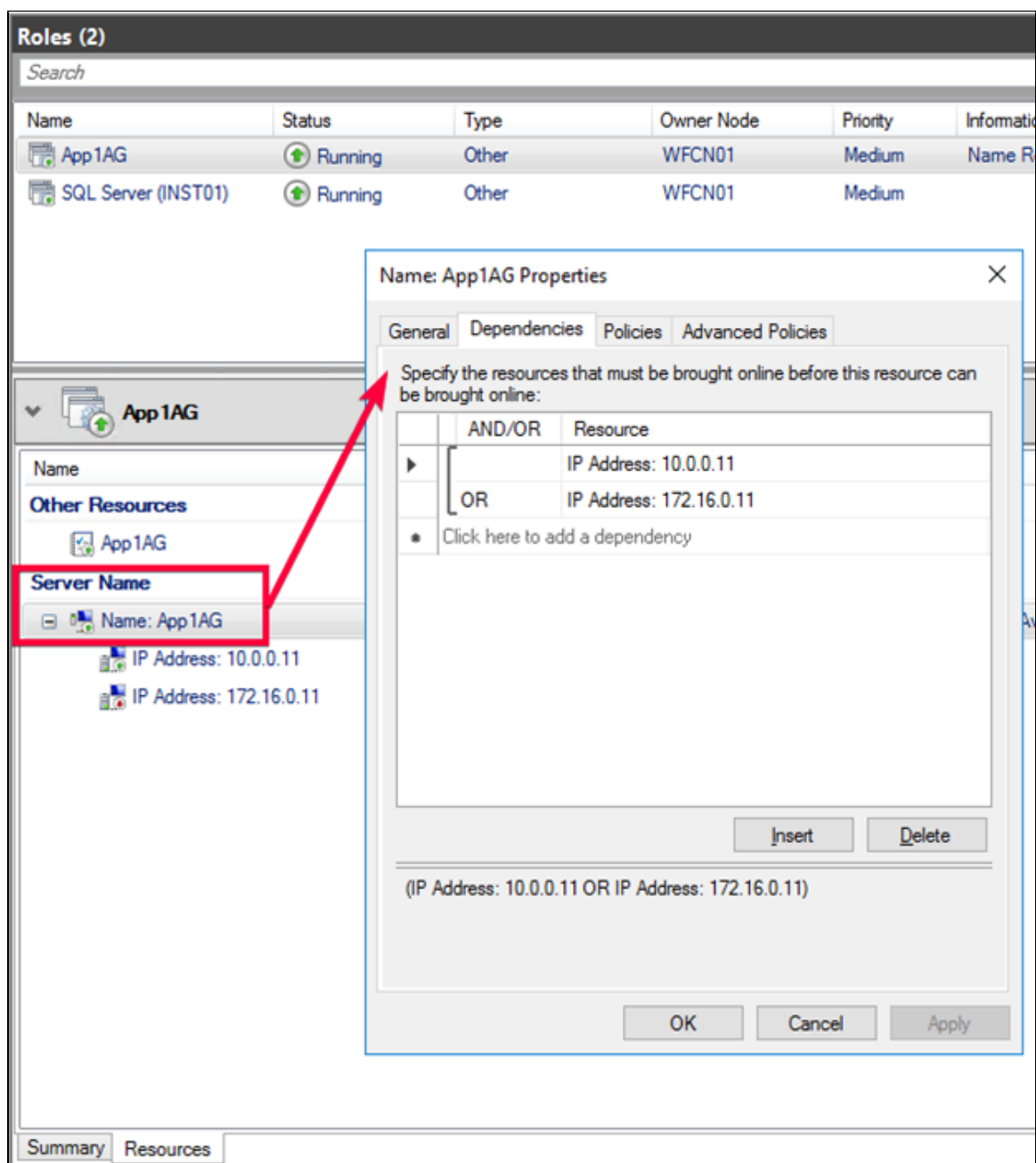
2. Select the clusters' **ServiceGroup** (Windows Server 2008) or **Role** (Windows Server 2012 and later) created for the cluster agent service.



3. On the **Server Name** area, right-click the resource name and click Failover Cluster Manager displays the **Properties** window.

4. Click the **Dependencies**.

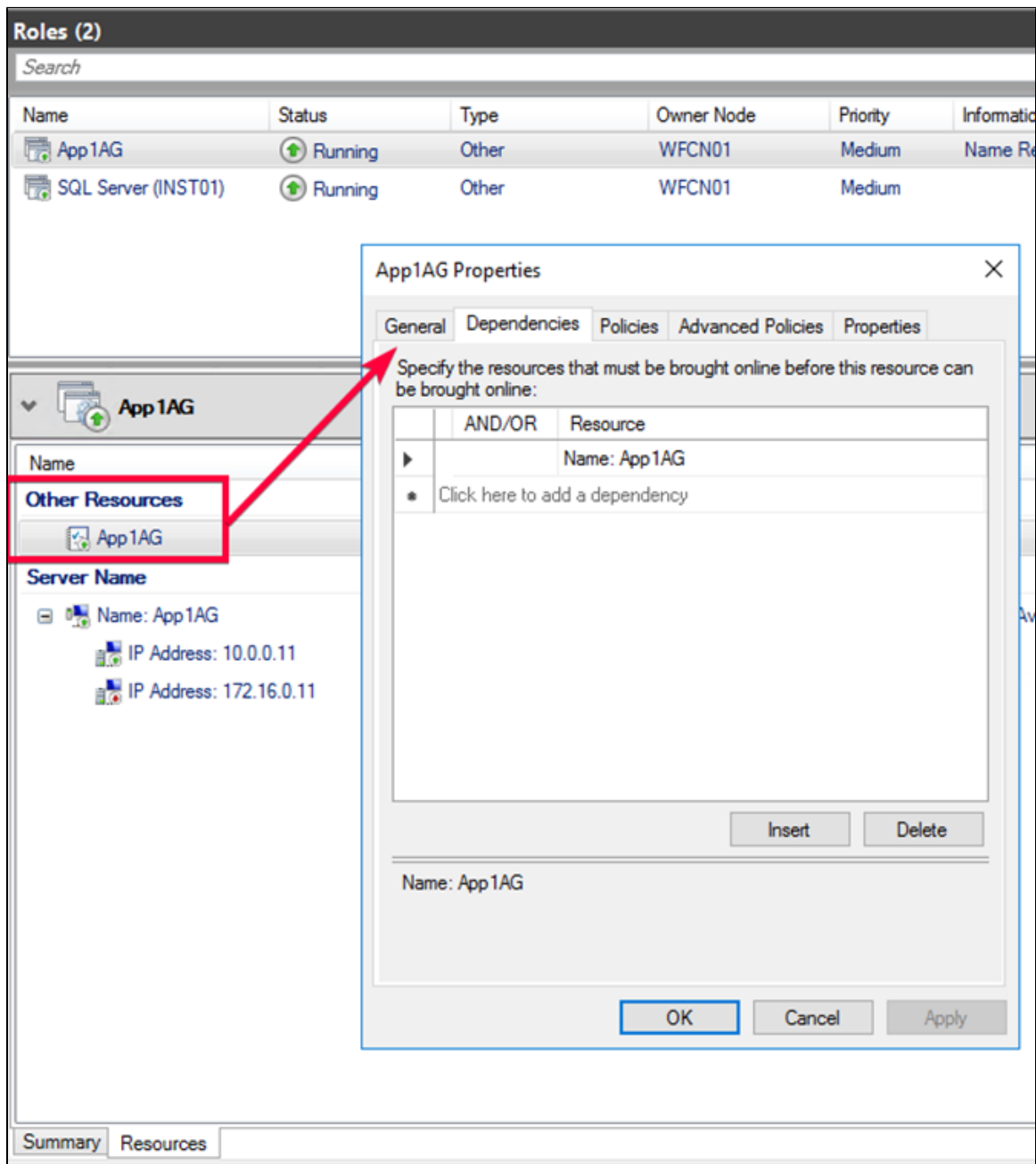
5. Verify that the **Resource** field displays the listener's IP address.



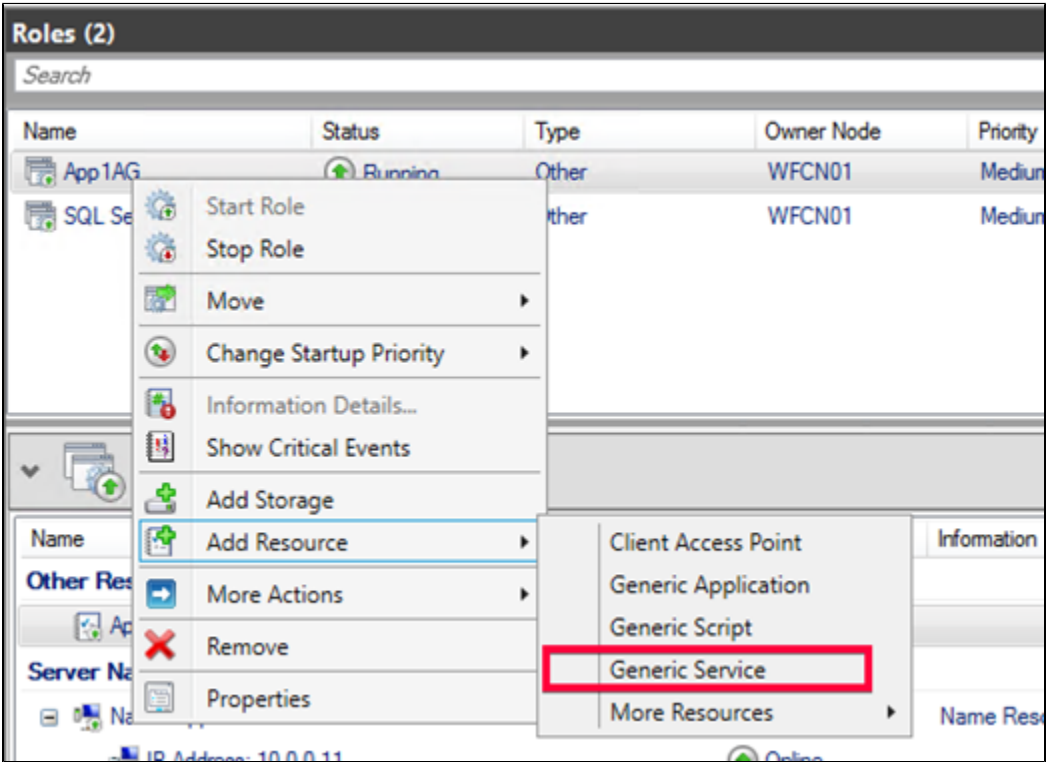
6. On the **Other Resources** area of the **Failover Cluster Manager** window, right-click the resource within the role and select **Properties**. Failover Cluster Manager displays the **Properties** window.

7. Click the **Dependencies**

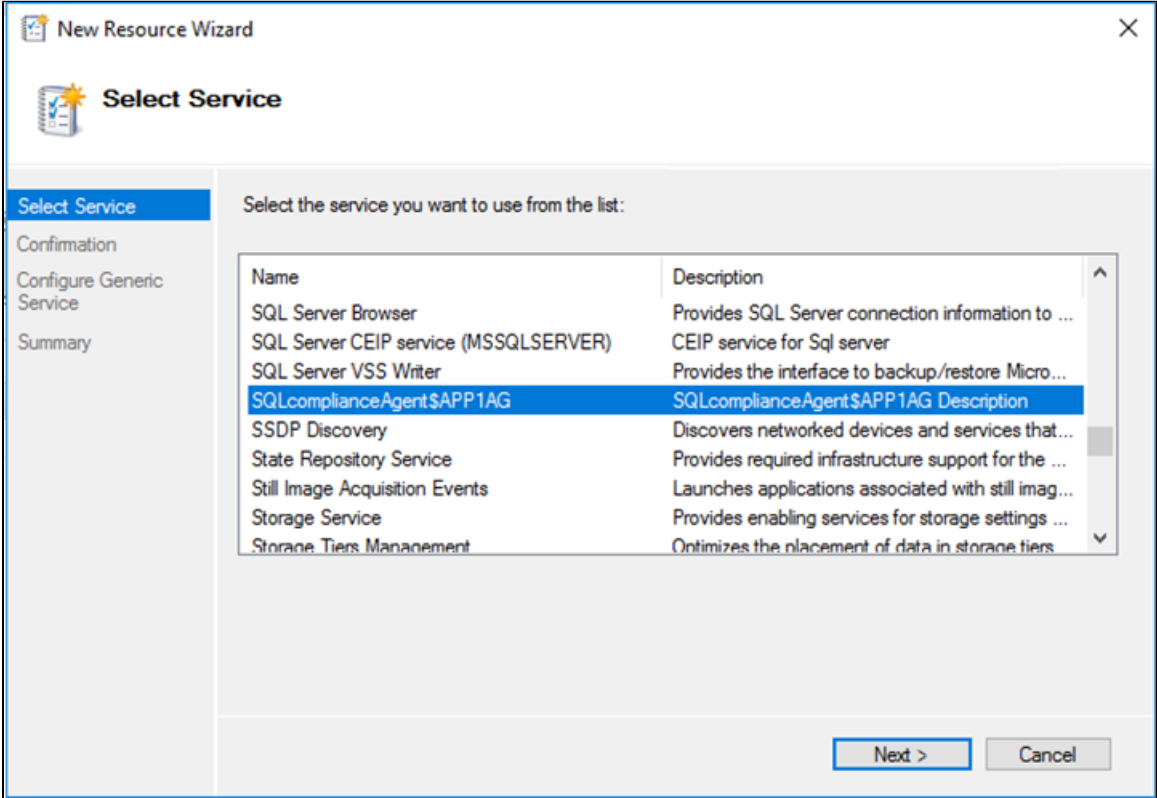
8. Verify that the **Resource** field displays the listener name. Click **Cancel** to close this window.



9. After verifying the resource information, right-click the **Service Group** or **Role** and point to **Add a resource**. Click on **Generic Service**. Failover Cluster Manager displays the **New Resource Wizard**.



10. On the **Select Service** page, select the SQLcompliance Agent service from the available list. The service name is displayed in the format **SQLcomplianceAgents[listener name]**, where **[listener name]** is the SQL Server Availability Group Listener name previously registered into the SQLcompliance Cluster Configuration Console.



11. Click **Next**, continue following the wizard, and click **Finish**.
12. On the **Other Resources** area of the Failover Cluster Manager window, right-click the **SQLcomplianceAgents[listener name]** and select **Bring Online the resource**.

Roles (2)

Search

Name	Status	Type	Owner Node	Priority
App1AG	Partially Runni...	Other	WFCN01	Medium
SQL Server (INST01)	Running	Other	WFCN01	Medium

▼ App1AG

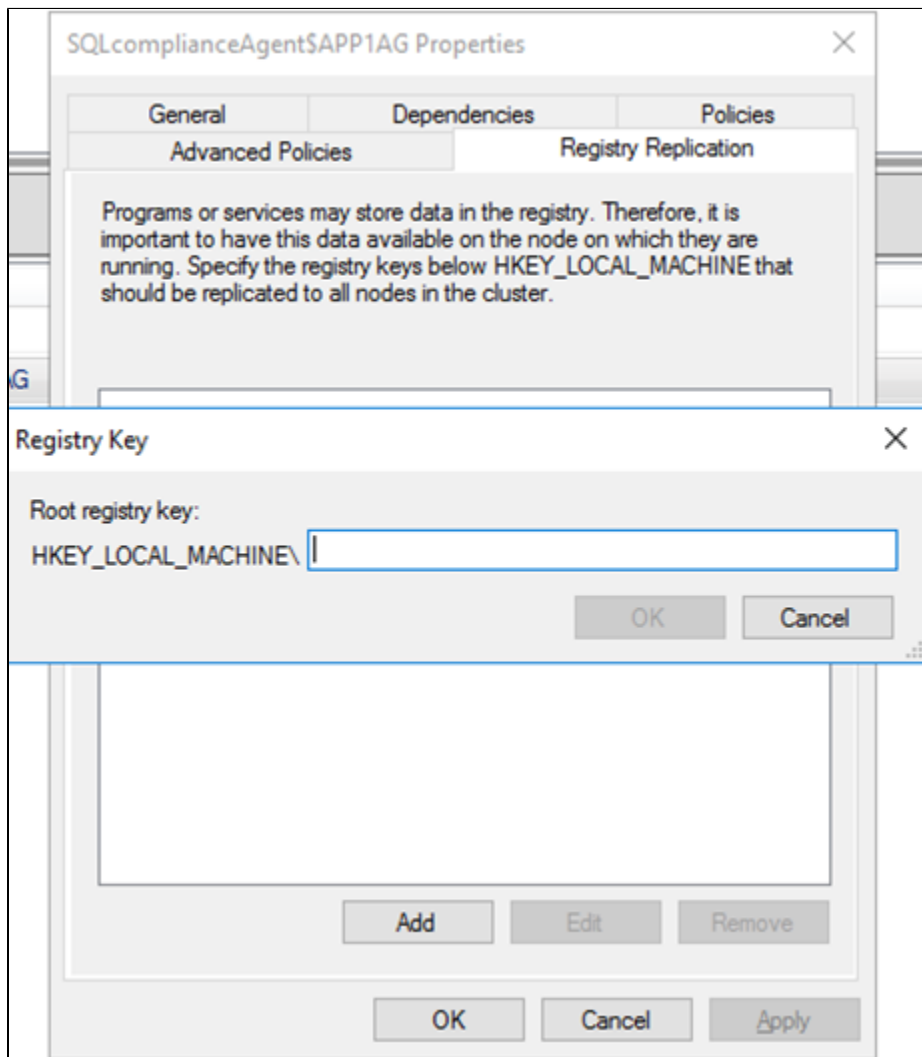
Name	Status	Information
Other Resources		
App1AG	Online	
Server Name		
Name: App1AG	Online	Name Res
IP Address: 10.0.0.11	Online	
IP Address: 172.16.0.11	Offline	
Roles		
SQLcomplianceAgent\$APP1AG	Offline	

Right-click context menu for SQLcomplianceAgent\$APP1AG:

- Bring Online
- Take Offline
- Information Details...
- Show Critical Events
- More Actions
- Remove
- Properties

13. While the cluster service is online, right-click the **SQLcomplianceAgent\$[listener name]** cluster service and click **Properties**.

14. On the **Registry Replication** tab, click **Add**. Failover Cluster Manager displays the **Registry Key** window.

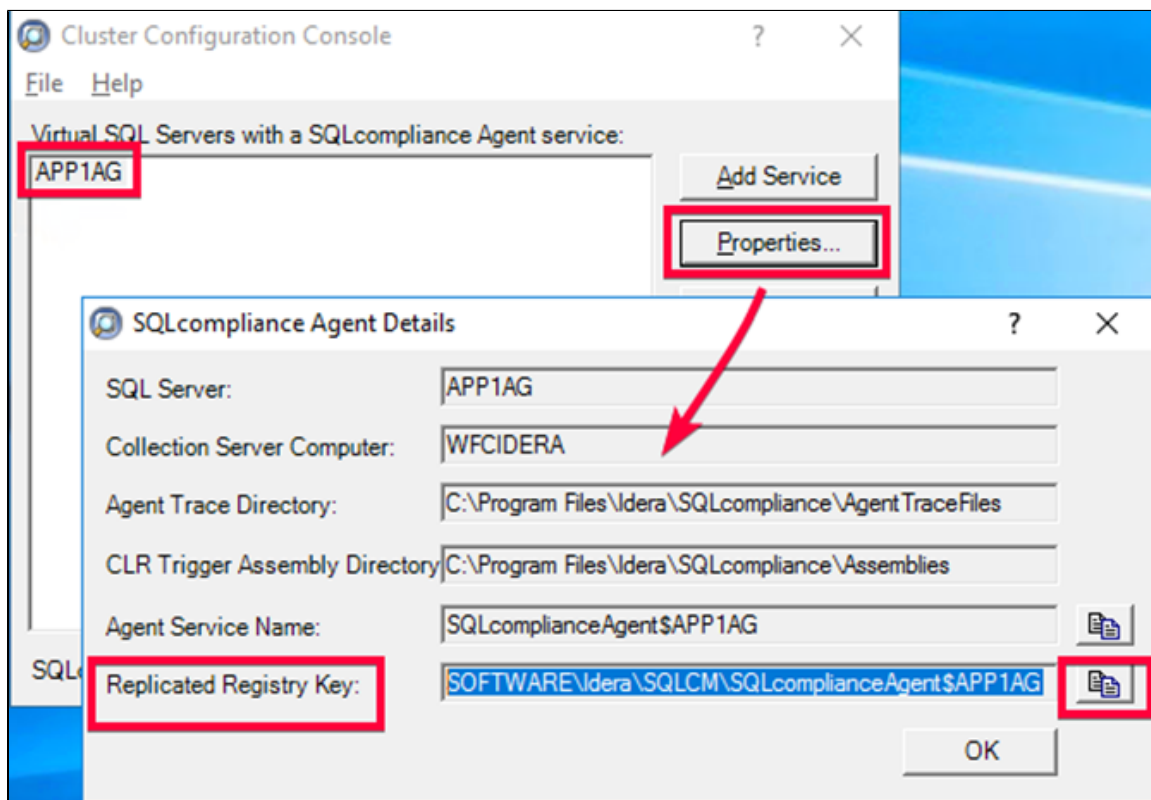


The Registry Replication tab is not available in Windows Server 2012.

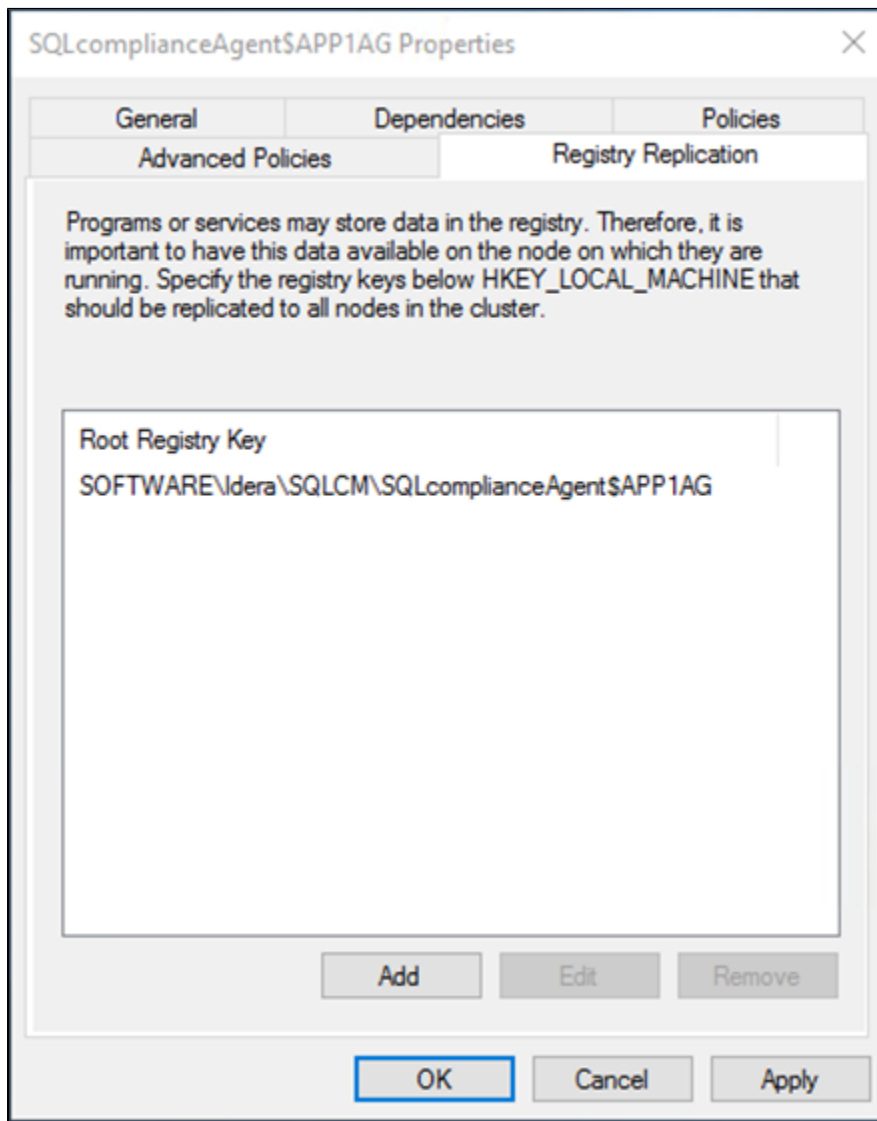
If you are using Windows Server 2012, you must use the "Add-ClusterCheckpoint" PowerShell cmdlet to add the necessary setting.

For more information, see [Add ClusterCheckpoint](#).

15. To obtain the correct path, go to the **IDERA Cluster Configuration Console** and copy the Replicated Registry Key from the **SQLcompliance Agent details**.



16. Click **OK** and copy the registry key path back into the service properties window. The new root registry key appears in the **Registry Replication** tab of the Properties window. Click **Apply** and then **OK** to save changes.



3. Register the Availability Group Listener in SQL Compliance Manager

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

1. Start the IDERA SQL Compliance Manager Management Console and click **New > Registered SQL Server**. SQL Compliance Manager displays the **SQLcm Configuration Wizard - Add Server**.
2. On the **SQL Server** window, specify or browse the Availability Group Listener you want to register with SQL Compliance Manager, and click **Next**.
3. On the **SQL Server Cluster** page, check **This SQL Server instance is hosted by a Microsoft SQL Server Cluster virtual server** box, and click **Next**. This step registers the AG Listener as a virtual cluster SQL Server name.
4. On the **SQLcompliance Agent Deployment** page, verify that the **Manually Deploy** is selected, and click **Next**. This option is required for all virtual SQL Servers.
5. On the **Select Databases** page, check the AlwaysOn database that you want to audit, and click **Next**.
6. SQL Compliance Manager displays the **AlwaysOn Availability Group Details** page, including a list of all nodes where the AlwaysOn database is replicated.



This step is valid only if the database selected for auditing is AlwaysOn. The wizard skips this page for regular databases.

7. **If the AlwaysOn Availability Group Details window is displayed**, click **Next** to continue.
8. On the **Audit Collection Level** page, select the desired audit collection level for the database and click **Next**.
9. SQL Compliance Manager verifies that all the required permissions are in place on the SQL Server instance you want to audit on the Permissions Check page.

10. After all the operations are complete and all permissions checks pass, click **Next**. The **Summary** page displays the audit settings for the SQL Server instance.
11. Click **Finish** to close the wizard. Finally, SQL Compliance Manager displays the newly-added AlwaysOn Availability Group Listener in the **Explore Activity** tree.
12. 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, click **Refresh** in the node context menu to apply the settings to the displayed information.

After configuration, review some [Additional information on SQL Compliance Manager and AlwaysOn Availability Groups](#).

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