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

(i)

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.
- 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 SQL compliance Agent Service - General window.

🥥 Add SQLcomplia	nce Agent Service	•				? ×
	General Specify the virt	ual SQL Serve	r instance that t	this SQLcomplia	ance Agent v	vill audit.
	SQL Server:					
			< Back	Next >	Finish	Cancel

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.

💭 Add SQLcompliar	nce Agent Service		? ×
	Collection Server Specify the SQL Server to reg Server is registered, you can	gister with SQL compliance manager. Once begin auditing database activity on the serv	a SQL ver.
	The SQLcompliance Agent se that the audit data can be proc computer name on which the	ends collected audit data to a Collection Ser ressed and stored in the Repository. Specifi Collection Server service is running.	verso ythe
	Collection Server computer:	J	
		Kext > Finish	Cancel

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

Add SQLcompliance	e 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.	
	< Back Next > Finish	Cancel

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.

Add SQLcomplia	nce 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: C:\SQLCM\TraceDirectory
	Note: This directory will be created by the SQLcompliance Agent when Before and After data auditing enabled.
	< Back Next > Finish Cancel

 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 SQL compliance Agent Service -CLR Trigger Location window.

Add SQLcomplia	nce Agent Service	x
	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 us the specified directory to store the corresponding CLR trigger assemblies. You c enable before-after auditing from the Audited Database Properties window in the Management Console. Assembly Directory: C:\SQLCM\AssemblyDirectory	ies an
	Note: This directory will be created by the SQLcompliance Agent when before-a auditing is enabled.	fter
	< Back Next > Finish Car	ncel

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.

🔘 Add SQLcomplia	nce Agent Service
	Summary Ready to add SQLcompliance Agent
	You have finished entering the data necessary to install the SQLcompliance Agent service necessary to audit this virtual SQL Server: AUT-200
	Click Finish to begin the installation process for the SQLcompliance Agent. Note that this installation must be performed on each node of the cluster and that after the agent is installed, you must register the agent as a shared resource in the Microsoft Cluster Management console.
	< Back Next> Finish Cancel

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.

💭 Add SQLcompliance Agent Service 📃 🔀
You have successfully registered the SQLcompliance Agent service on one node in your SQL Server cluster. To complete this process, you will need to do the following:
(1) Repeat the cluster support setup process on each node in the cluster.
(2) Register the SQLcompliance Agent service as a shared resource in the Microsoft Cluster Administrator.
Tell me more about configuring auditing in a clustered environment
OK

(1) 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.

File Action View Help						1	
agcluster, projects.local Services and applications Agroup01 Nodes	AGroupU1 Recent Cluster Summary of AGroupU1		er Event	s: None in the	last 24 hours	AGroup01	e or a
Cluster Events	Status: Online Alerts: <none> Preferred Owners: aoagnode2, aoagnod</none>	le1	Gene	acaglistener ral Dependen	Properties icies Policies ies that must be	Advanced Policies	: resource can
	Current Owner: aoagnode2		be t	orought online: AND/OR	Resource IP Address: 19	32.168.240.216	
	Name Server Name	Status	*	Click here to a	add a dependend	cy	
	Mame: acaglistener IP Address: 192.168.240.216 Other Resources	💿 Online 🕐 Online	1				
	AGroup01	💿 Online					
				Address: 1921f	38 240 216	Insert	Delete
						How resource depen	dencies work
						DK Cancel	Apply
						More Actions	• <u>•</u>

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

 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.
- 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, SQLc or plianceAgent \$ADAGLISTENER is the service name.

Select Service	Select the service you want to use from the li	st.
Confirmation	Name	Description
ervice	SQLcomplianceAgent\$A0AGLISTENER	SQLcomplianceAgent\$A0AGLISTENER Description
mmaru	SSDP Discovery	Discovers networked devices and services that use t
ininidiy	System Event Notification Service	Monitors system events and notifies subscribers to C
	Task Scheduler	Enables a user to configure and schedule automated
	TCP/IP NetBIOS Helper	Provides support for the NetBIOS over TCP/IP (NetB
	Telephony	Provides Telephony API (TAPI) support for programs
	Thread Ordering Server	Provides ordered execution for a group of threads wit
	TP AutoConnect Service	ThinPrint .print component for printing with ThinPrint
	TP VC Gateway Service	ThinPrint component that receives print data from de
	TPM Base Services	Enables access to the Trusted Platform Module (TP

- 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 wi	ndow, verify the i	nformation regarding	the new resource,	and then click Finish.

elect Service	The new resou	irce as was successfully created and configured.	
Confirmation			
onfigure Generic ervice			
ummary	Service:	SQLcomplianceAgent\$AOAGLISTENER (SQLcomplianceAgent\$AOAGLISTENER)	
	Resource:	Generic Service	
	Parameters:	Files\Idera\SQLcomplianceCluster\SQLc SQLcomplianceAgent\$AOAGLISTENER	omplianceAgent.exe"
			-

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.



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. ick ÕK.

Type SOFTWARE \Idera \SQLcompin	lance as the registry Ke	ey value, and then c
Registry Key		×
Root registry key:		1246
HKEY_LOCAL_MACHINE	Ndera\SQLcompliance	
	ОК	Cancel
The new root registry key appears in t	the Registry Replication	tab of the Propertie
SQLcomplianceAgent\$A0AGLISTENER P	roperties	X

window, as shown in the following example.

	Dependencies	Policies
Advanced Po	licies	Registry Replication
Programs or services mportant to have this unning. Specify the should be replicated	may store data in the reg s data available on the no registry keys below HKEY to all nodes in the cluster.	istry. Therefore, it is de on which they are '_LOCAL_MACHINE that
Root Registry Key		
SOFTWARE\Idera	\SQLcompliance	15
	Add	Edit Remove

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.

- Start the SQL Compliance Manager Management Console, and then click New > Registered SQL Server.
 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.

😡 SQLcm Configura	tion Wizard -	Add Server	<u>? ×</u>
	Specify SQ Specify the S is registered, g	L Server QL Server to register with SQL compliance mana you can begin auditing database activity on the s	ager. Once a SQL Server server.
	SQL Server: Description:	AOAGLISTENER	
		Previous	ext Cancel

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.

😡 SQLcm Configura	tion Wizard - Add Server	×
	SQL Server Cluster Specify whether this is a virtual SQL Server hosted on a cluster.	
	Select whether this SQL Server instance is a virtual SQL Server hosted by Microsoft Cluster Services. This choice affects the deployment options available for this SQL Server.	
	This SQL Server instance is hosted by a Microsoft SQL Server Cluster virtual server.	
	Previous Next Cancel	

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.

🥥 SQLcm Configura	ation Wizard - Add Server	? ×
	SQLcompliance Agent Deployment Specify the deployment option for this instance's agent.	
	A SQLcompliance Agent must be deployed to the computer hosting each audited SC Server. Auditing cannot be enabled until the agent has been deployed. Select the deployment option to use for this agent:	λΓ
	C Deploy Now - Installs the SQLcompliance agent at this time. This option requires that a connection be established between the SQL Server to be audited and the Management Console.	
	O Deploy Later - Indicates that you will install the SQLcompliance Agent using the Management Console at a later time such as during off-hours.	4
	Manually Deploy - Indicates that you will manually install the agent at the physic computer that hosts the SQL Server instance. Note that this option is required virtual SQL Servers and SQL Servers located across a domain trust boundary.	:al for
	Previous Next Cance	4

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.

Select Databases Select the databases you want to audit. SQL complian data for the selected databases.	nce manager will collect audit
🔽 Audit Databases	
 master model msdb mssqlsystemresource tempdb ✔ TestBase 	Select All Unselect All

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

GSQLcm Configuration	Wizard - AlwaysOn	Details		<u>?</u> >
AS	IwaysOn Availability howing the Databases I	Group Details that are involved in Ale	waysOn Availability Group (configuration.
R	egister / Add all the Rep plica servers, to make u	olica SQL Servers for a use of AlwaysOn featu	auditing and deploy agent o re for these databases.	on the
	Database Name	Availability Group	Replica Server	
	TestBase	AGroup01	AOAGNODE1	
		Previo	us Next	Cancel

- 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.

SQLcm Configuration	Wizard - Audit Settings	? ×
A Si Cr	udit Collection Level elect the audit collection level you want to use for the newly audited o pllection level affects the amount of event data collected for database	latabase. The activities.
Se	elect the audit collection level you want to use for the newly audited d election level affects the amount of event data collected for database	atabases. The activities.
	Default - Audits events and activities most commonly required by collection level meets most auditing needs. Tell me more	auditors. This
	Custom - Allows you to specify specific audit settings. This collect recommended for advanced users only. Before selecting specific settings, review the events gathered by the Custom collection leve the help to better understand your choices.	tion level is audit vel and review
	 Regulation - Configures your audit settings to collect the event despecific regulatory guidelines, such as PCI or HIPAA. 	ata required by
	Previous Next	Cancel

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.

Upe	aration Complete, Total 8, Passed 8, Failed 0	Re-c
	Check	Status
V	Collection Service has rights to the repository databases.	Passed
	Collection Service has rights to read registry HKLM\Softw	Passed
✓	Collection Service has permissions to collection trace dire	Passed
V	Agent Service has permissions to agent trace directory.	Passed
V	Agent Service has rights to read registry HKLM\Software	Passed
4	Agent Service has rights to the instance.	Passed
	SQL Server has permissions to the agent trace directory.	Passed
1	SQL Server has permissions to the collection trace direct	Passed

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.

😡 SQLcm Configura	tion Wizard -	Summary			? ×
	Summary Review the s hosted datab	cummary of the audit s bases.	setting you chose for	this SQL Server	instance and its
	Audit Level: Server:	Default AOAGLISTENER			
	Databases:	TestBase			A
]			<u>.</u>
			Previous	Finish	Cancel

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**.



TestBase Ren	Configure Remove Add Audited Nove SQL Server	Disable Server Apply Disable Server Apply Plance Agent to e with the removal is the last	Regulation Videline Audit Settings Report Card	Timport Collect	t Agent ta Properties Agent Span
	Instance on the computer, you will need to manu agent later to complete the process. Error: The SQLcomplance Agent on AOAA(ISTENER or The SQLcomplance Agent on AOAA(ISTENER or The SQLcomplance Agent service may be down is preventing contact. Do you wish to continue with the removal of this instance?	ally remove the gins not be reached. or a network error 1 Us	er y	No Data Avail	able
		Lit E	vents		
	Privileged Users - None	Category	Event	Time	Details
	Databases - 1 of 6	Login	Login Failed	7/29/2015 12:13:44 P	
Audit Reports	Event Filters - None				

- 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.



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.

DAGLISTENER	Add Service
	Properties
	Remove Servic
Cluster Configuration Console	×
	gent for AOAGLISTENER?
Are you sure you want to remove the ag	

- 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 AOAGN ODE2, 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.

- Agreen connigu	lacion mizara - A		<u></u>
	Specify SQL Specify the SQ is registered, y	. Server IL Server to register with SQL compliance ma ou can begin auditing database activity on th	anager. Once a SQL Server ie server.
	SQL Server:	AOAGNODE1	
	Description:		
<			

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

SQLCm Configu	ation Wizard - Add Server	<u> </u>
	Existing Audit Data Audit data for this SQL Server instance already exists.	
	A database containing audit data for this SQL Server instance alre losing any previously collected audit data, use the existing databas existing audit data.	ady exists. To avoid e and keep the
	Keep the previously collected audit data and use the existing the events database is from a previous version of SQL comp manager, it will be automatically upgraded.	database. If liance
	C Delete the previously collected audit data but use the existing database. This option will reinitialize the existing database. All data in the database will be permanently deleted.	audit
	Database: SQLcompliance_A0AGN0DE1	
	Previous Next	Cancel

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.

😡 SQLcm Configur	ation Wizard - Add Server	? ×
	SQL Server Cluster Specify whether this is a virtual SQL Server hosted on a cluster.	
	Select whether this SQL Server instance is a virtual SQL Server hosted by Microsof Cluster Services. This choice affects the deployment options available for this SQL Server.	it
	This SQL Server instance is hosted by a Microsoft SQL Server Cluster virtual server.	
	Previous Next Cancel	

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 SQL compliance Agent Deployment page.

😡 SQLcm Configurat	tion Wizard - Add Server	? ×
	SQLcompliance Agent Deployment Specify the deployment option for this instance's agent.	
•	A SQLcompliance Agent must be deployed to the computer hosting each audit Server. Auditing cannot be enabled until the agent has been deployed. Select deployment option to use for this agent:	ed SQL the
-	C Deploy Now - Installs the SQLcompliance agent at this time. This option requires that a connection be established between the SQL Server to be audited and the Management Console.	
	C Deploy Later - Indicates that you will install the SQLcompliance Agent usin Management Console at a later time such as during off-hours.	ng the
	Manually Deploy - Indicates that you will manually install the agent at the p computer that hosts the SQL Server instance. Note that this option is requiritual SQL Servers and SQL Servers located across a domain trust bound	vhysical uired for tary.
	Previous Next C	ancel

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.

SQLcm Config	iration Wizard - Add Databases	?
	Select Databases Select the databases you want to audit. SQL complian data for the selected databases.	nce manager will collect audit
	Audit Databases	
	☐ master ☐ model	Select All
	msdb mssqlsystemresource tempdb	Unselect All
	✓ TestBase	
	Previous	Next Cancel

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.

ty Group Details that are involved in Ak eplica SQL Servers for a use of AlwaysOn featur Availability Group AGroup01 AGroup01	waysOn Availability Group of auditing and deploy agent of re for these databases. Replica Server AOAGNODE1 AOAGNODE2	configuration.
eplica SQL Servers for a use of AlwaysOn featur Availability Group AGroup01 AGroup01	auditing and deploy agent o re for these databases. Replica Server AOAGNODE1 AOAGNODE2	on the
Availability Group AGroup01 AGroup01	Replica Server AOAGNODE1 AOAGNODE2	
AGroup01 AGroup01	AOAGNODE1 AOAGNODE2	
AGroup01	A0AGNODE2	
P		
Previo	us Next	Cancel
ck Next SQL Compl	liance Manager displays	the Audit Coller
ttings	lance manager displaye	? ×
/el		
on level you want to us	e for the newly audited dat	abase. The
he amount of event dal	ta collected for database a	ctivities.
on level you want to use ne amount of event dat	e for the newly audited data a collected for database ac	abases. The ctivities.
vents and activities mo eets most auditing nee	ist commonly required by au ds. Tell me more	uditors. This
you to specify specific a r advanced users only, he events gathered by understand your choic	audit settings. This collectio Before selecting specific a the Custom collection level es.	n level is udit and review
figures your audit settin y guidelines, such as P	gs to collect the event data CI or HIPAA.	a required by
	Previo ck Next. SQL Comp ttings rel on level you want to us he amount of event dat wents and activities mo reets most auditing nee you to specify specific a r advanced users only. he events gathered by understand your choic figures your audit settin y guidelines, such as P	Previous Next ck Next. SQL Compliance Manager displays ttings rel on level you want to use for the newly audited dat he amount of event data collected for database a on level you want to use for the newly audited dat he amount of event data collected for database a on level you want to use for the newly audited dat he amount of event data collected for database a on level you want to use for the newly audited dat he amount of event data collected for database a on level you want to use for the newly audited dat he amount of event data collected for database a on level you want to use for the newly audited dat he amount of event data collected for database a on level you want to use for the newly audited data he amount of event data collected for database a on level you want to use for the newly audited data he amount of event data collected for database a on level you want to use for the newly audited data he amount of event data collected for database a wents and activities most commonly required by a ueets most auditing needs. Tell me more you to specify specific audit settings. This collection a he events gathered by the Custom collection level understand your choices. figures your audit settings to collect the event data y guidelines, such as PCI or HIPAA.

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

	Check	Status
-	Collection Service has rights to the repository databases.	Passed
V .	Collection Service has rights to read registry HKLM\Softw	Passed
-	Collection Service has permissions to collection trace dire	Passed
4	Agent Service has permissions to agent trace directory.	Passed
-	Agent Service has rights to read registry HKLM\Software	Passed
-	Agent Service has rights to the instance.	Passed
1	SQL Server has permissions to the agent trace directory.	Passed
1	SQL Server has permissions to the collection trace direct	Passed

SQLcm Configura	tion Wizard - 9	ummary	?>
	Summary Review the su hosted databa	mmary of the audit setting you chose for theses.	is SQL Server instance and its
	Audit Level: Server:	Default AOAGNODE1	
	Databases:	TestBase	<u>_</u>
			<u> </u>
		Previous	Finish Cancel

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.

Explore Activity	SQL-N1								
Audited SQL Servers	Summary	Eve	nt Alerts	Data Alerts		Audit Events	Archive	d Events	
SQL-2012		*	- Star	Q		Server Settings Apply Regulation	Guideline	😤 Import	
Healthcare	Configure Alerting	Remove Server	Add Audited Databases	Disable Auditing	2	Privileged Users			Audit Da
SQL-N2		Ą	ctions			Audit (Settings		

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.

SQL Compliance Manager audits all activity on your server. Learn more > >

IDERA Website	Products	Purchase	Support	Community	About Us	Resources	Legal
---------------	----------	----------	---------	-----------	----------	-----------	-------