PowerScribe® 360 Reporting

Hot Spare
Installation Configuration and Management

PN 889715 ***October 12, 2018***

PN 889715

Printed in U. S. A. October 12, 2018

Trademarks

Copyright Notice

Disclaimer

Table of Contents

Best Practices

- Nuance recommends following Microsoft best practices as outlined in

  Microsoft TechNet General Security Advice and Best Practices

- ***PowerScribe 360 Reporting*** stores data containing Protected Health Information (PHI) in the product databases as well as in various locations throughout the file system. Nuance recommends encrypting ***PowerScribe 360 Reporting*** at the operating system and/or storage system levels to ensure that PHI is encrypted consistent with the customer's data encryption policies.
- ***PowerScribe 360 Reporting*** is compatible with several currently supported versions of Microsoft Windows Server operating systems, Nuance recommends using the latest compatible version listed in the ***PowerScribe 360 Reporting*** System Specifications, currently ***Windows Server 2016***.
- ***PowerScribe 360 Reporting*** is compatible with several currently supported versions of Microsoft SQL Server, Nuance recommends using the latest compatible version listed in the ***PowerScribe 360 Reporting*** System Specifications, currently ***SQL Server 2016***.
- Nuance recommends that all ***PowerScribe 360 Reporting*** network communication be secured and encrypted using Hypertext Transfer Protocol Secure (HTTPS). Nuance also recommends that the customer obtain a certificate from a trusted Certificate Authority consistent with the customer security policies.
- Nuance fully supports all third-party hardware and software updates related to critical security fixes immediately upon release. Nuance recommends that customers apply third party updates consistent with their internal security policies.
- ***PowerScribe 360 Reporting*** supports Lightweight Directory Access Protocol (LDAP). Nuance recommends the use of LDAP for end-user authentication to ***PowerScribe 360 Reporting*** to ensure consistency with the customer's authentication and password management policies.
- During the ***PowerScribe 360 Reporting*** installation process several system level users and associated passwords need to be created. Nuance recommends that the Customer's site administer provides the system level passwords consistent with the customer's internal password policies. Nuance recommends the use of strong/complex passwords consistent with the customer's password management policies.
- Nuance recommends that any Passwords created during ***PowerScribe 360 Reporting*** installation and configuration only be communicated over secure encrypted channels and/or stored in secure encrypted locations.
- Nuance does not recommend exposing network services to untrusted networks unless otherwise advised by Nuance documentation or Support.

Notations

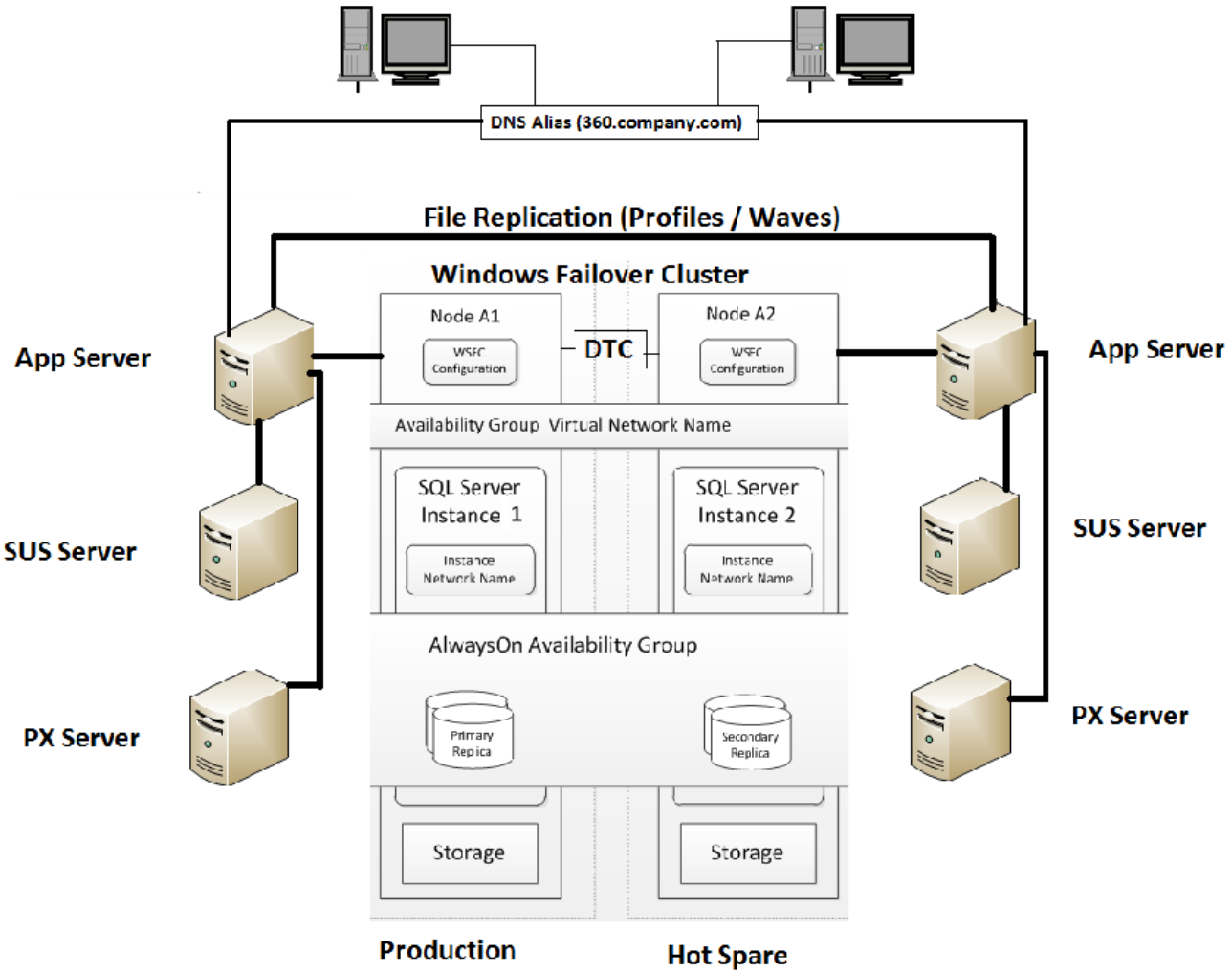
This section defines notations that are uses throughout the document.

Best Practice 	This **Best Practice** icon indicates the recommended Nuance procedure to follow when installing or configuring the Nuance PowerScribe 360 application. For example: ● PowerScribe 360 Reporting supports Lightweight Directory Access Protocol (LDAP). Nuance recommends the use of LDAP for end-user PS360 access. ● During the PowerScribe 360 Reporting installation process several system level users and passwords need to be created. The Customer's site administer should provide system level passwords consistent with the customer's internal password policies. Passwords should only be communicated over secure encrypted channels and/or stored in secure encrypted locations. ● Microsoft General Security Advice and Best Practices. ● Client workstations rebooting recommendations. ● Nuance Anti-Virus recommendations.
 ***IMPORTANT***	The **IMPORTANT** icon indicates important information you don't want miss.
	The **NOTE** icon provides auxiliary information or further explanation to the adjacent paragraph(s).
	This **STOP** icon is an indication that a necessary requirement is to be met before you proceed to the next step.

Introduction

Validated Configuration

The following diagram represents the validated configuration for a PowerScribe 360 Reporting Hot Spare system. Variations of this configuration are not currently supported.



NOTE

The Hot Spare with AlwaysOn, will operate most efficiently when MSSQL is on a separate server. It is required that the Hot Spare Application and SQL servers match the production system exactly.

If the facility has a Level I server or Level II system where the Application and SQL are installed and run on the same server, the Hot Spare may also have the Application and SQL on the same server. If, this configuration impacts performance (due to circumstances outside of the application), the Client will need to separate the SQL functions to a separate server from the PS360 Application.

- You must have PowerScribe 360 Reporting fully installed on both the Production system and hot spare system.
- Once you complete configuring SQL AlwaysOn, you will need to configure the replication of the file data between the Application servers.
- Nuance Hot Spare only supports a Basic Availability Group (BAG) with one active SQL and one passive SQL. Microsoft SQL 2016 standard will support this configuration. This configuration requires the SQL servers be installed using Windows Server Failover Clustering (WSFC).
- Nuance only supports SQL Always only when configured in Asynchronous (Disaster Recovery) Mode. If run in Synchronous mode, latency will occur and performance will be negatively impacted. You can read more information from Microsoft about Availability Modes for Always On Availability.

Upgrading Mirrored Hot Spare Installations

Before implementing the new Hot Spare solution, perform the following:

1. You should have already upgraded both systems independently, ensuring that the OS and SQL versions are the correct versions.
2. If not already performed, you must complete the following:
   a. Break the mirror between the production and Hot Spare systems.
   b. Disable the Hot Spare Windows scheduler jobs used to replicate profiles, waves, and logs.
   c. Upgrade the SQL Application to SQL 2014 Enterprise or 2016 Standard Edition.
   d. Stop the RadBridge, IIS and all other Application relevant services and set them to manual start.
3. Delete the database on the Hot Spare system. This is necessary to enable Always on, but must be done after the system / server is upgraded.

Configure Client Alias

In order to properly use Hot Spare, the 360 system connections need to be installed and configured to use a DNS.

The Alias is configured in the site's DNS (Domain Name Server). The Alias will redirect communications to the proper server. This allows all clients to connect to the proper system without reconfiguring during a hot spare scenario.

Example:

Alias Set up in Network Domain Name Service (DNS) = PS360
Prod Application Server = Application1
Hot Spare Application Server = Application2
RadPortal Configuration:

Portal URL = http://PS360.Company.Com/RadPortal
DragonUsers Directory = http:// PS360.Company.Com/DragonUsers

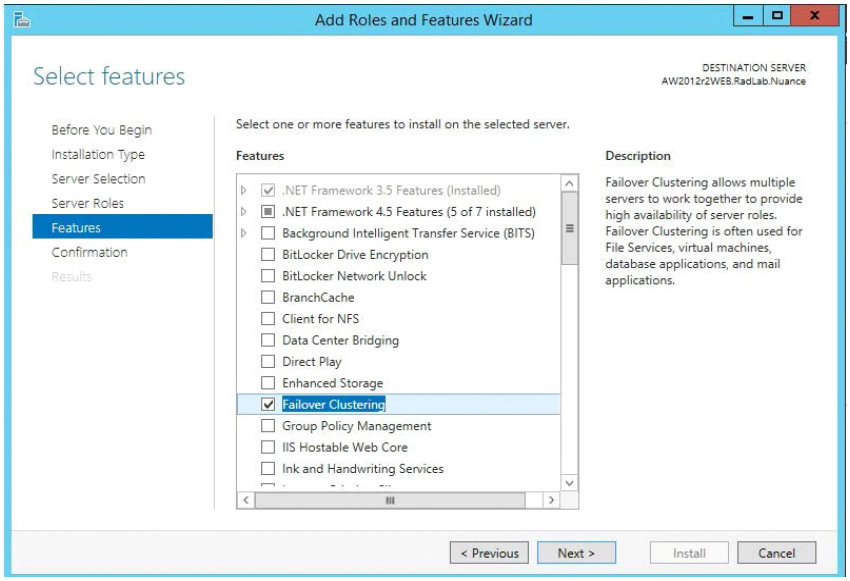
Installing and Configuring SQL Cluster

At this time, you should have two stand-alone Microsoft SQL servers which you will now make into a cluster.

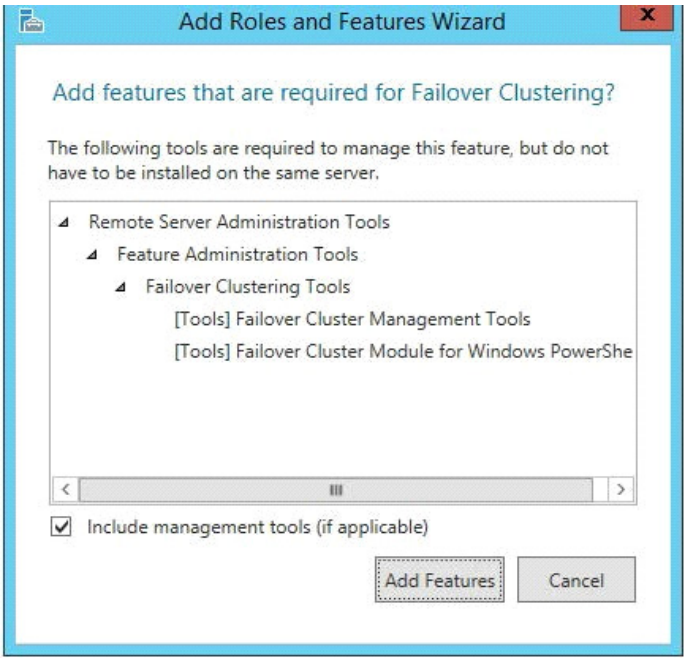
Add Role and Features

This must be done on the two SQL servers that will be configured for Windows Server Failover cluster and SQL AlwaysOn.

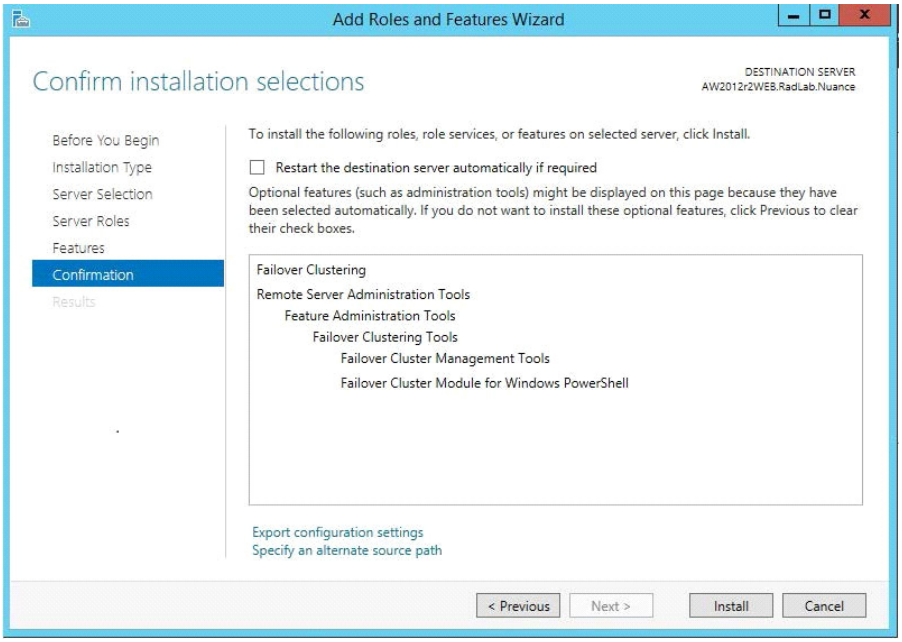
1. Open the Server Manager console and select Add roles and features. The Add Roles Features Wizard displays.
2. Under Features, select **Failover Clustering**.



3. Click **Add Feature** for Failover Clustering.

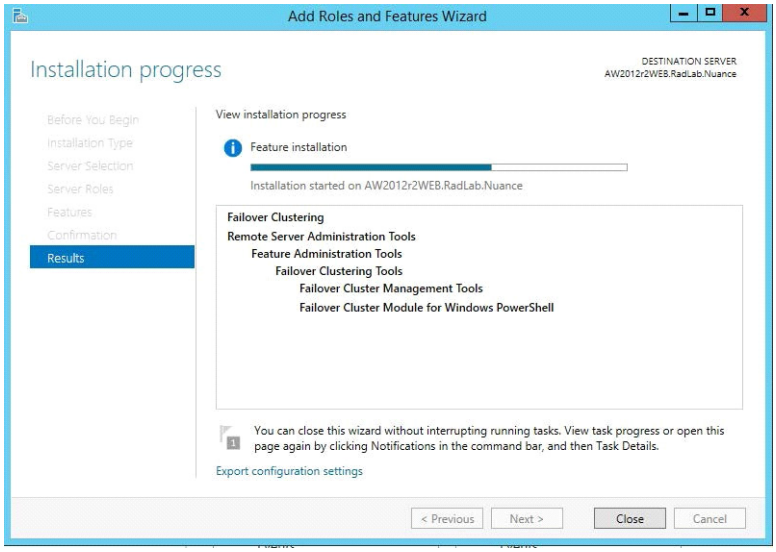


4. Click **Next**.



5. Click **Install**.

The Installation Progress dialog displays.

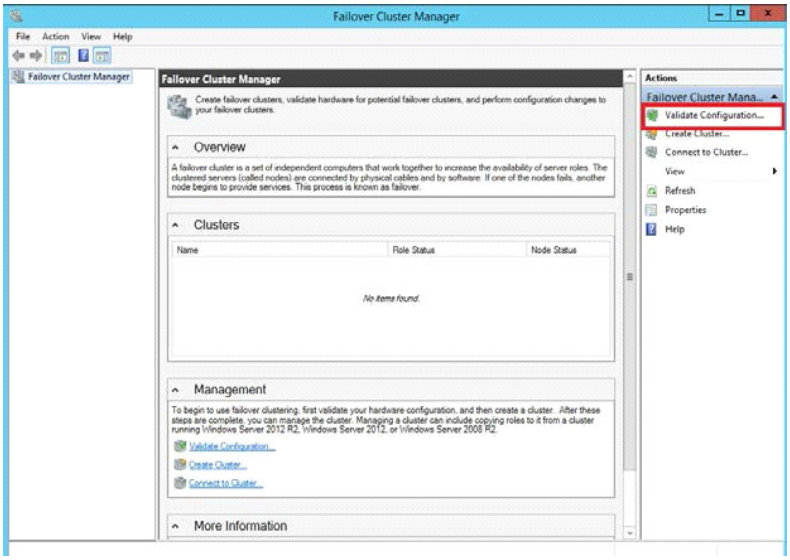


6. When finished, click **Close**.

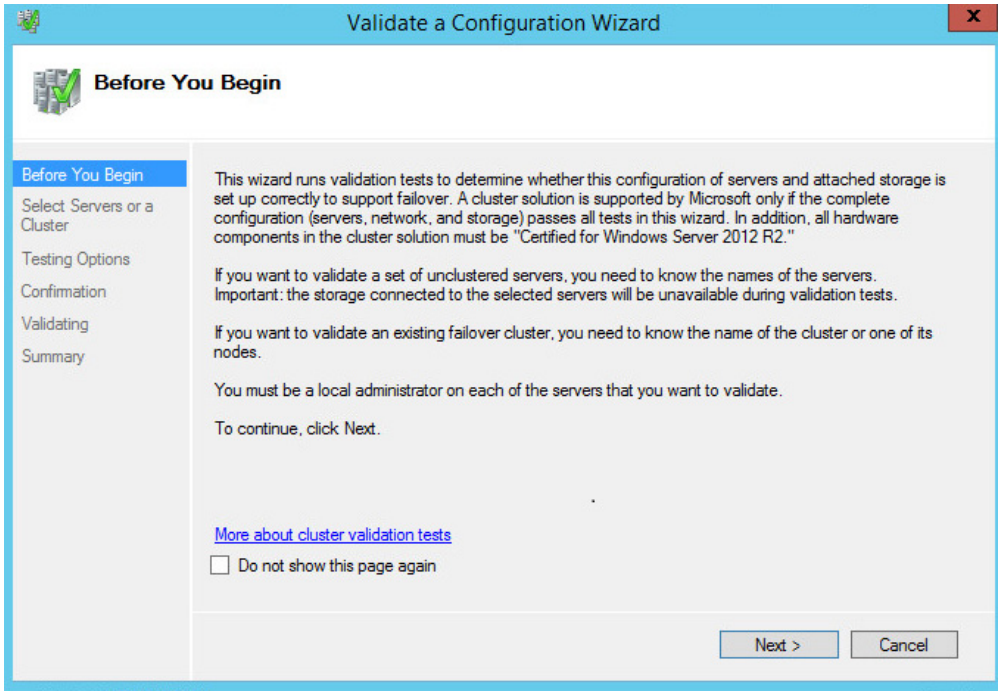
Configuring the Failover Cluster

Prior to configuring the Windows Server Failover Cluster, it is assumed that you have the appropriate rights in Active Directory. For a complete listing of the different Active Directory permissions to create a Windows Server Failover Cluster Failover Cluster Step-by-Step Guide: Configuring Accounts in Active Directory.

1. Open Server Manager.
2. Click **Tools**.
3. Click **Failover Cluster Manager**.
4. Under Failover Cluster Manager, click **Validate Configuration**.

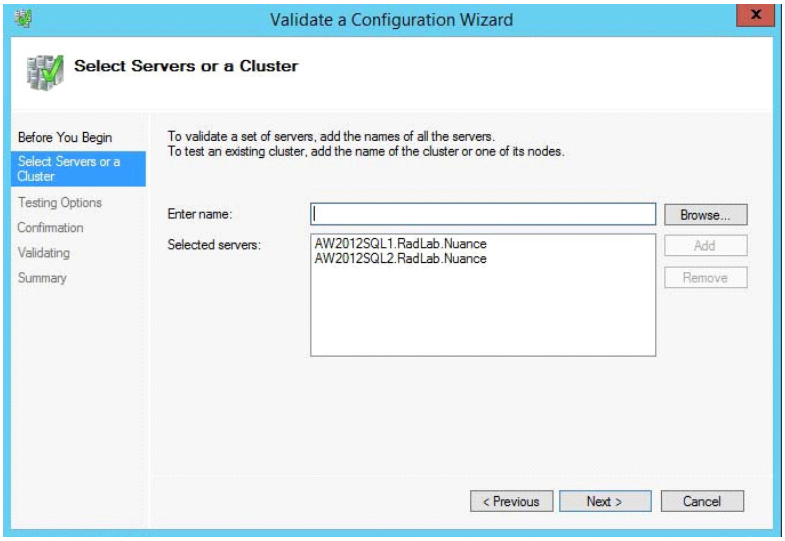


5. Click **Next**.



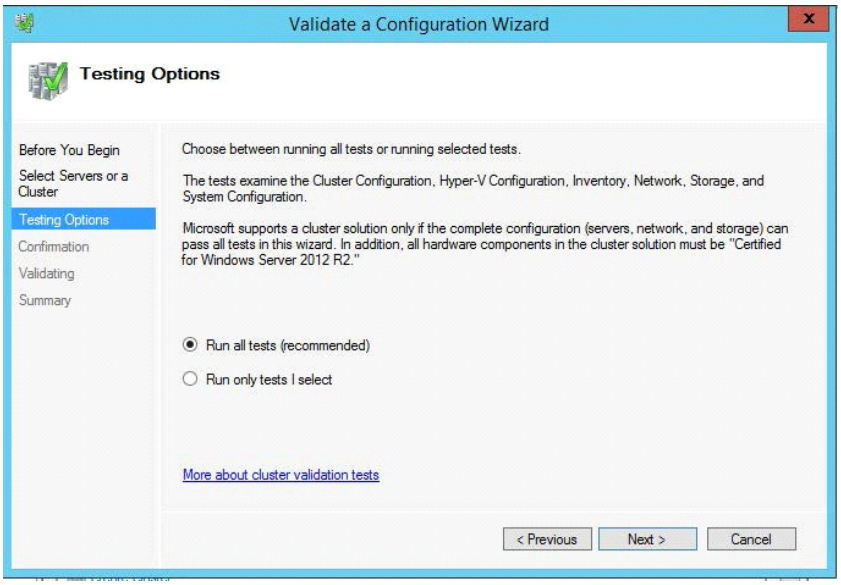
6. Click **Next**.
7. In the Select Servers or a Cluster dialog, add the server host names of the SQL Server instances that you want to configure as replicas in your Availability Group.

   You can use the Browse button to find them.
8. Click **Next**.

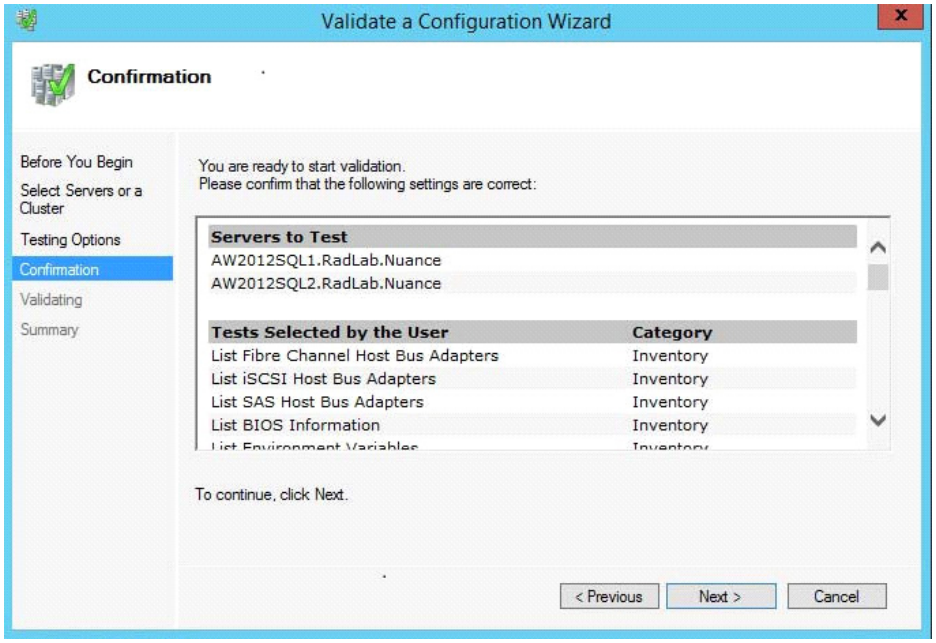


9. On the Testing Options dialog, make sure that the option **Run all tests (recommended)** is selected.

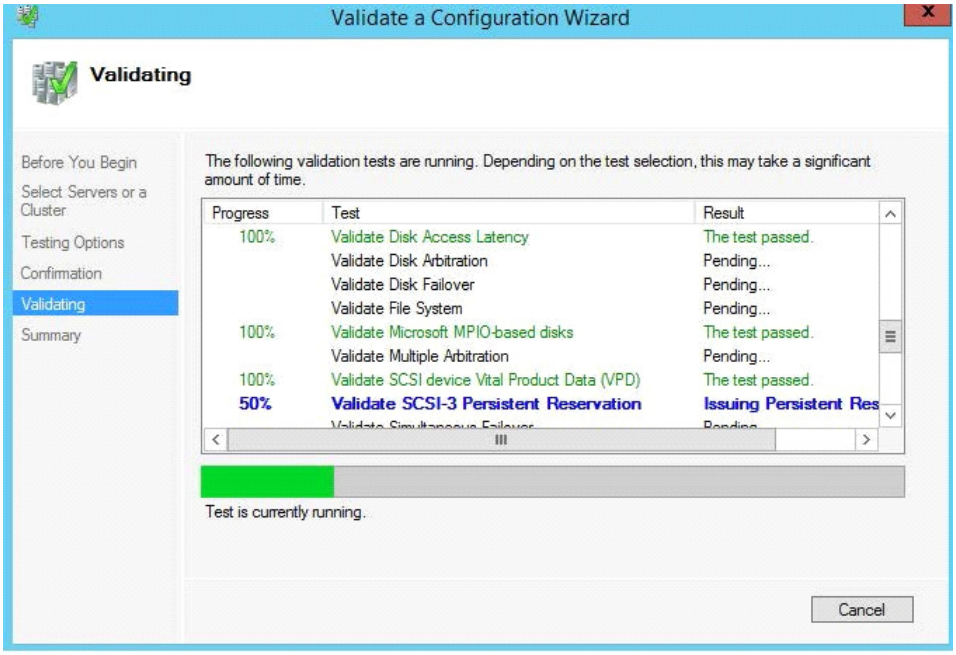
10. Click **Next**.



11. On the Confirmation dialog, click **Next**.



The Validating dialog displays.

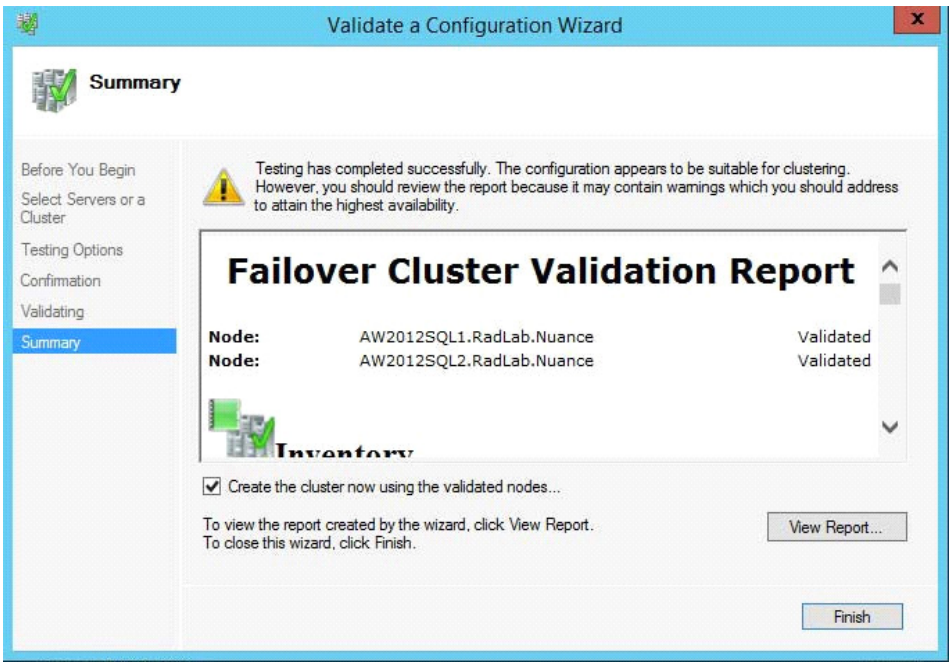


Tests can take some time to complete.

NOTE

12. Once tests are complete, review the results.

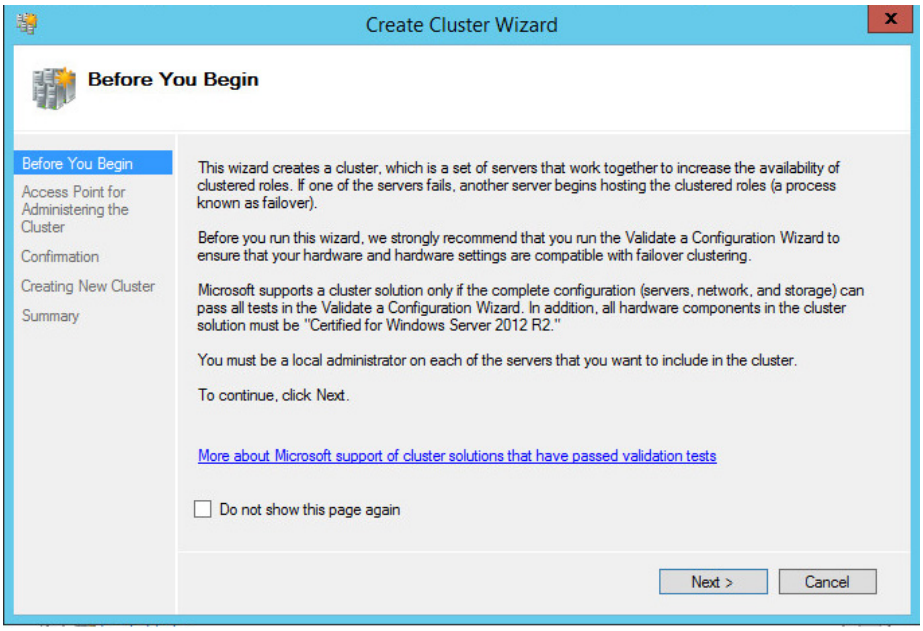
    You can click view report or just scroll through the results. If there are any errors, they must be fixed and then run the Validation Wizard again before continuing.



13. Check **Create the cluster now using the validated nodes**.

14. Click **Finish**.

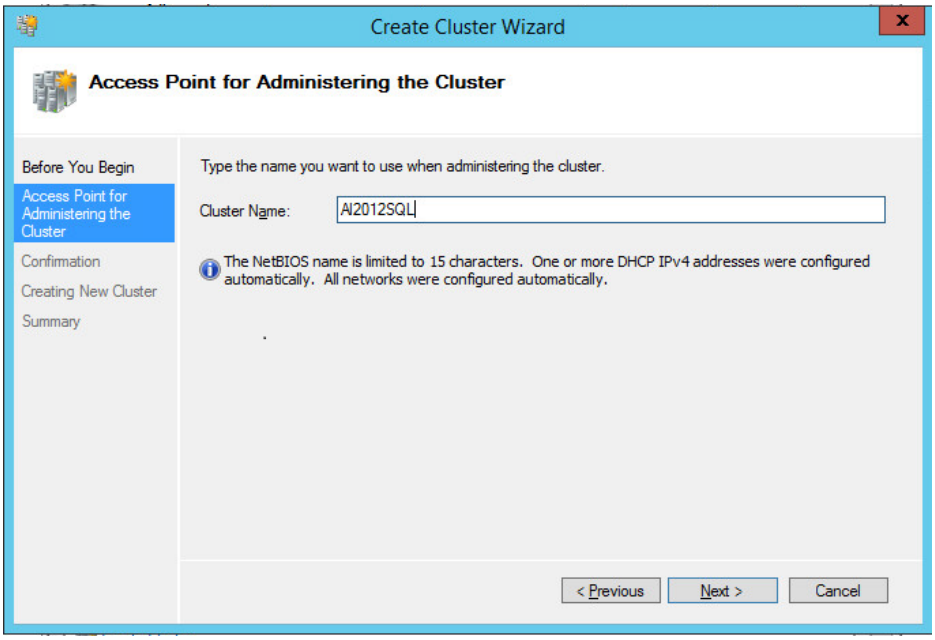
    The Before You Begin dialog displays.



15. Click **Next**.

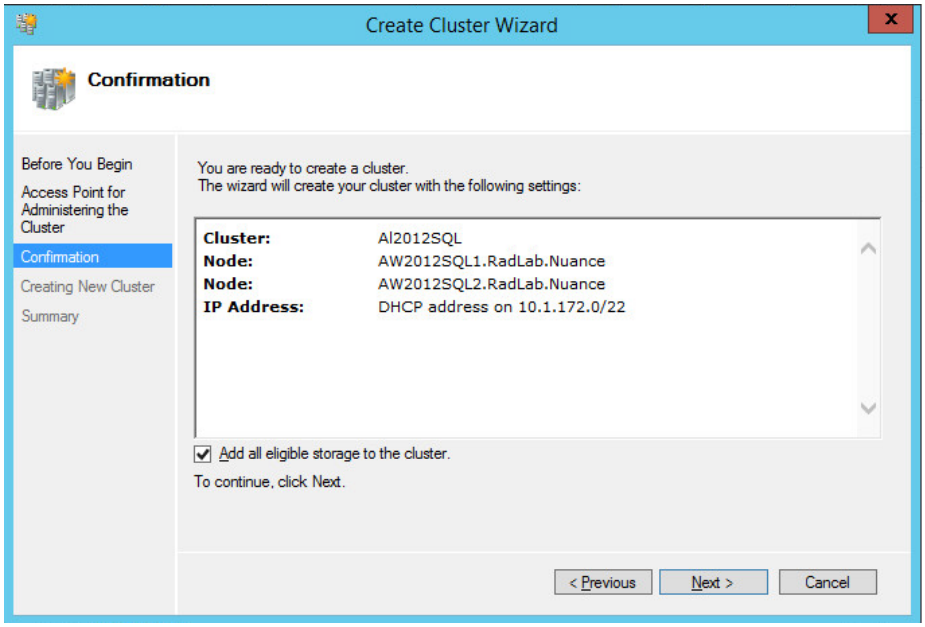
16. On the Access Point for Administering the Cluster dialog, enter the virtual server name and virtual IP address of your Windows Server Failover Cluster.

NOTE *In this testing DHCP is used.*



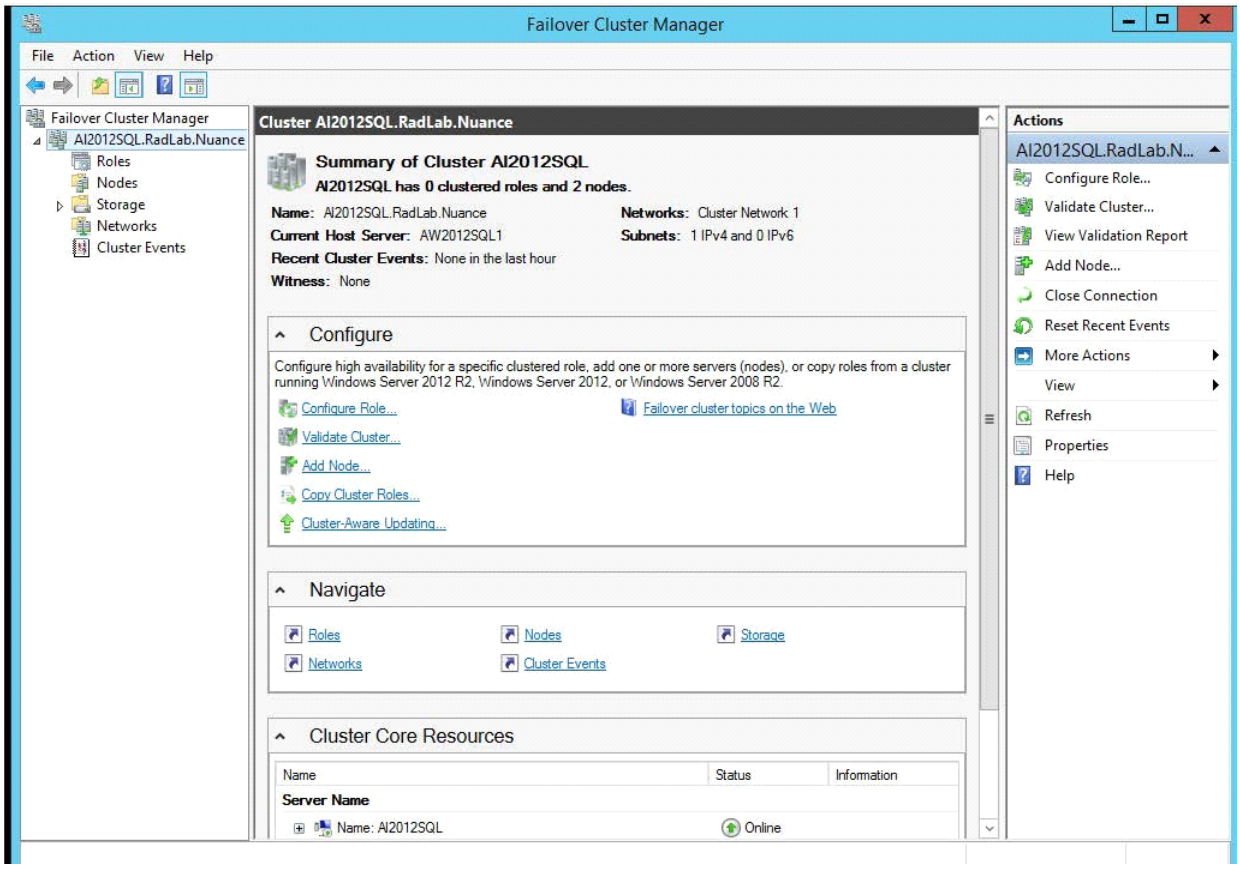
17. On the Confirmation dialog, click **Next**.

This will create the Windows Failover Cluster using the servers that you added as nodes of the cluster and then add DNS and Active Directory entries for the cluster host name.



18. Review the results of the Summary page to verify that the Cluster was created successfully.
19. Click **Finish**.

20. On the Failover Cluster Manager, you will see the cluster listed.



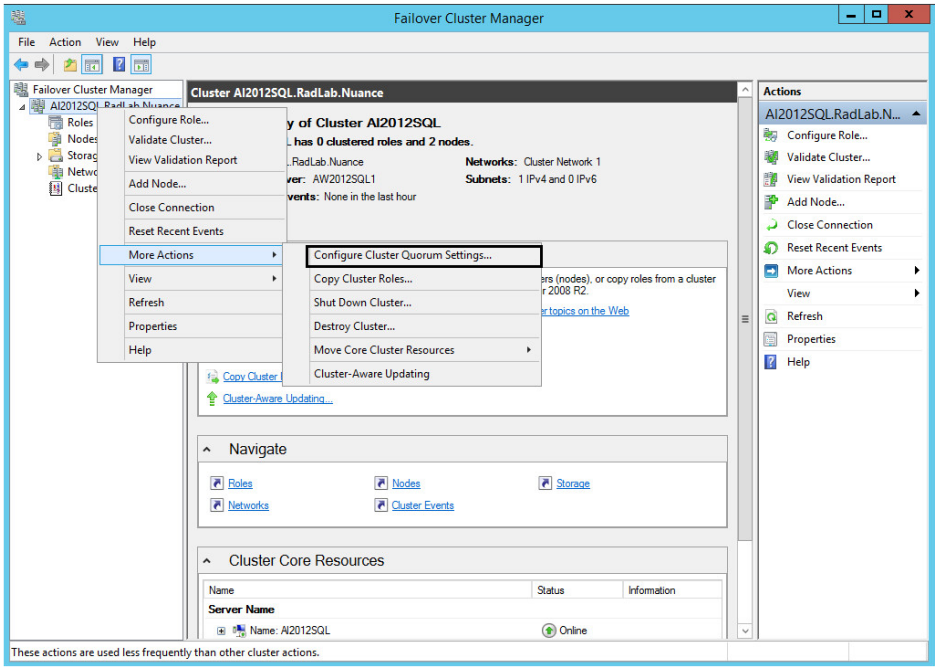
NOTE

When creating the cluster Quorum, it is no longer required to only use shared storage. Windows Server 2012 has the ability to configure the Quorum using either a shared storage location or a standard file share.

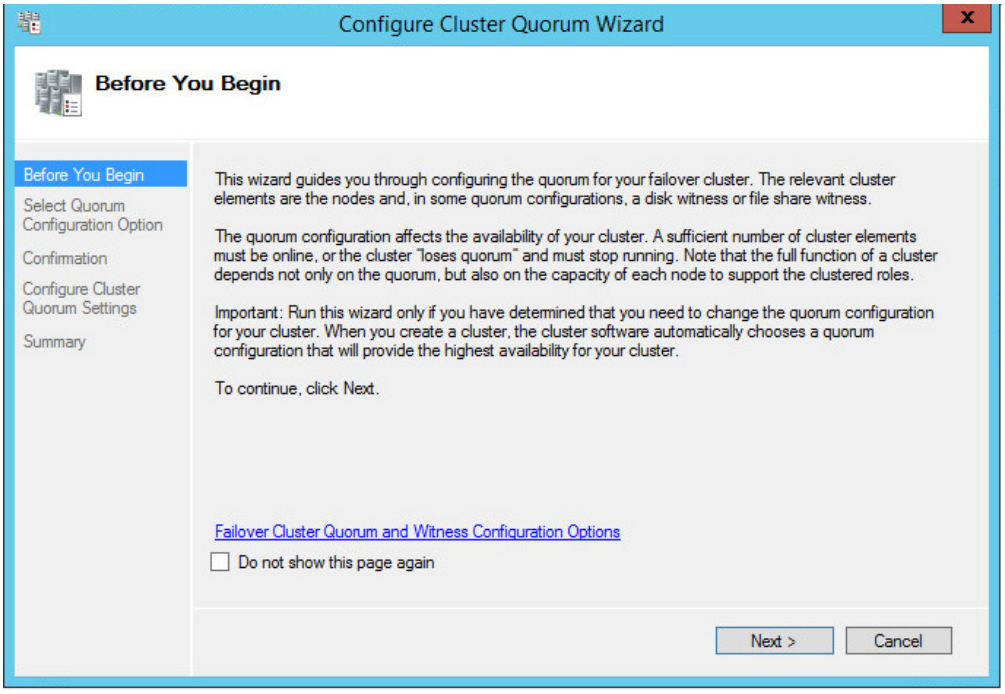
NOTE

This tests installs on a File share that is pointing at our NAS.

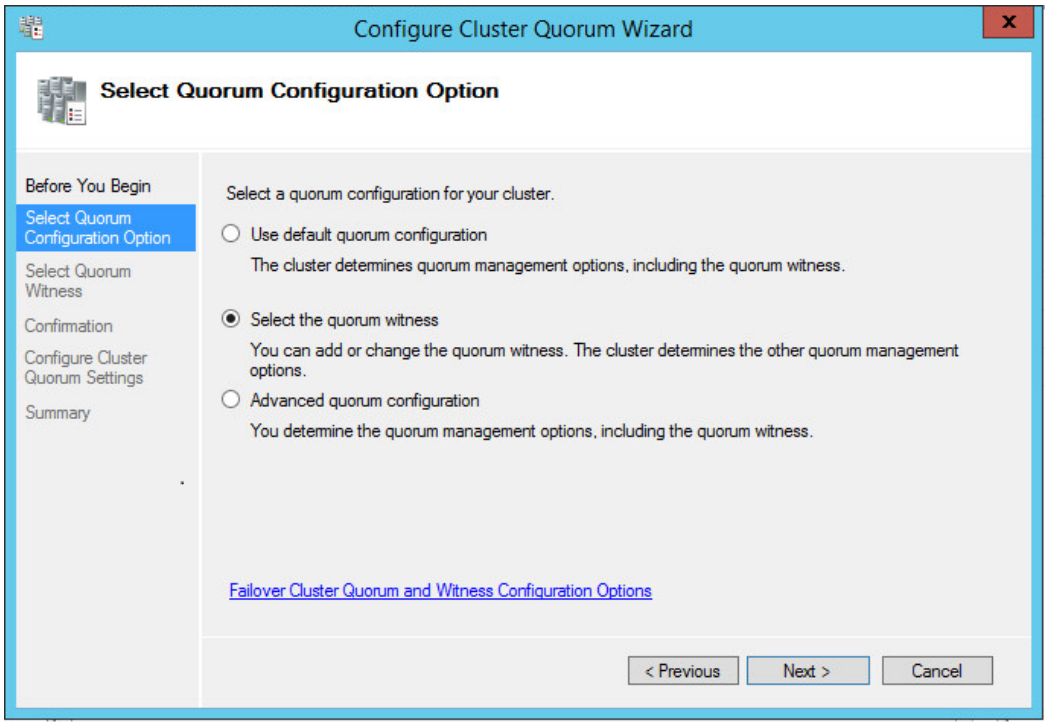
1. To create a File shared Witness Quorum right-click the cluster name in the Failover Cluster Manager, and select More Actions, and then click **Configure Cluster Quorum Settings**.



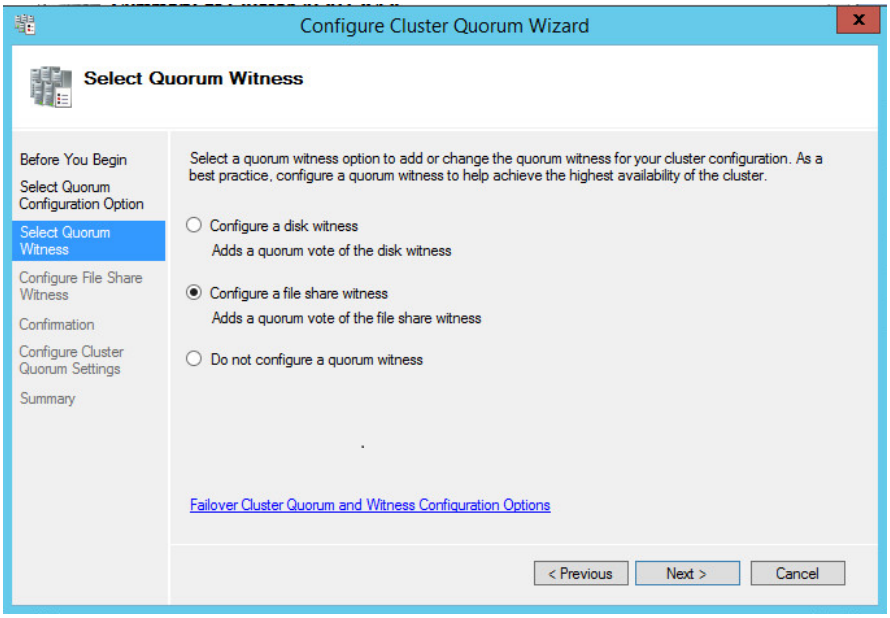
2. Click **Next** on the Before you Begin dialog.



3. On the select Quorum Configuration dialog, click the **Select the quorum witness** option, and click **Next**.

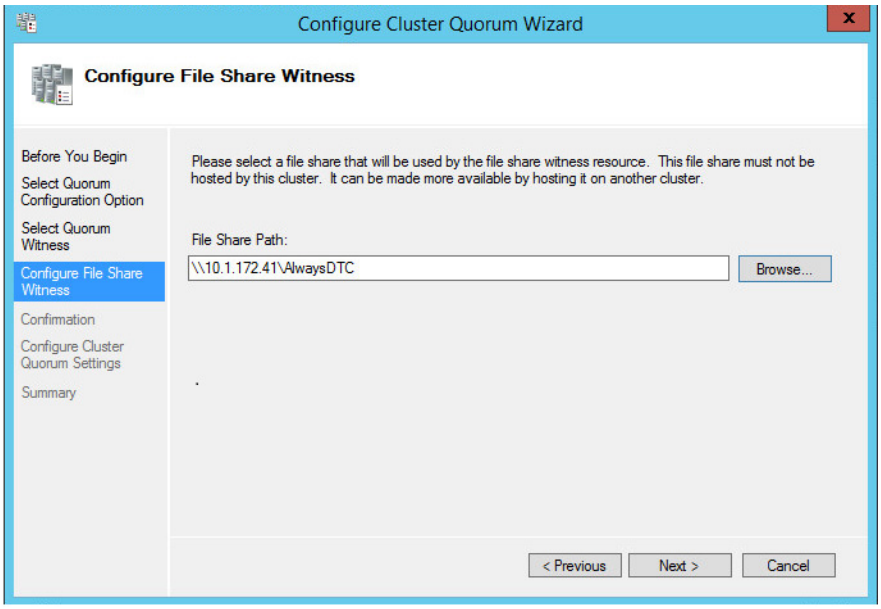


4. On the Select Quorum Witness dialog, select **Configure a File Share Witness**, and click **Next**.

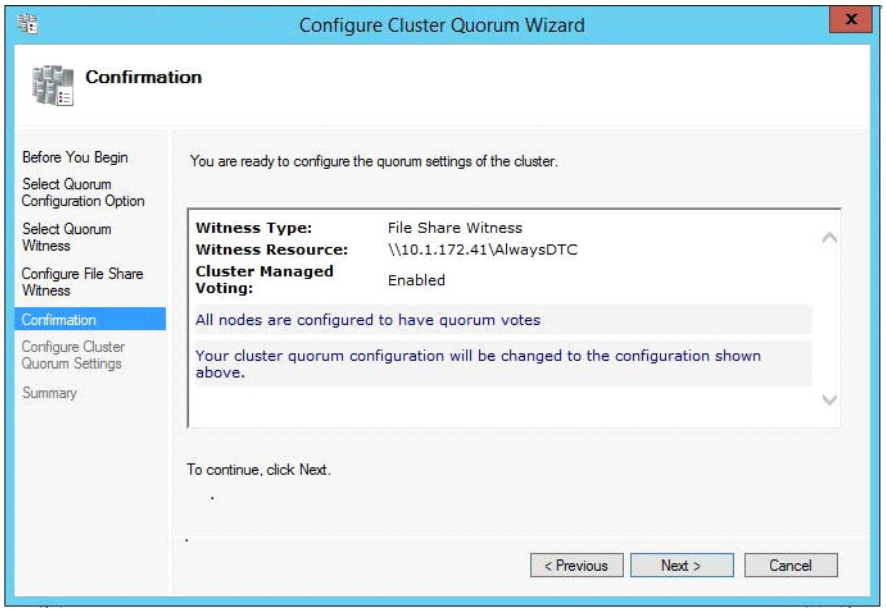


5. On the Configure File Share Witness dialog, enter the path or click Browse to find the location you have selected to where you want to point. This should be a safe location. In this example, it points to NAS.

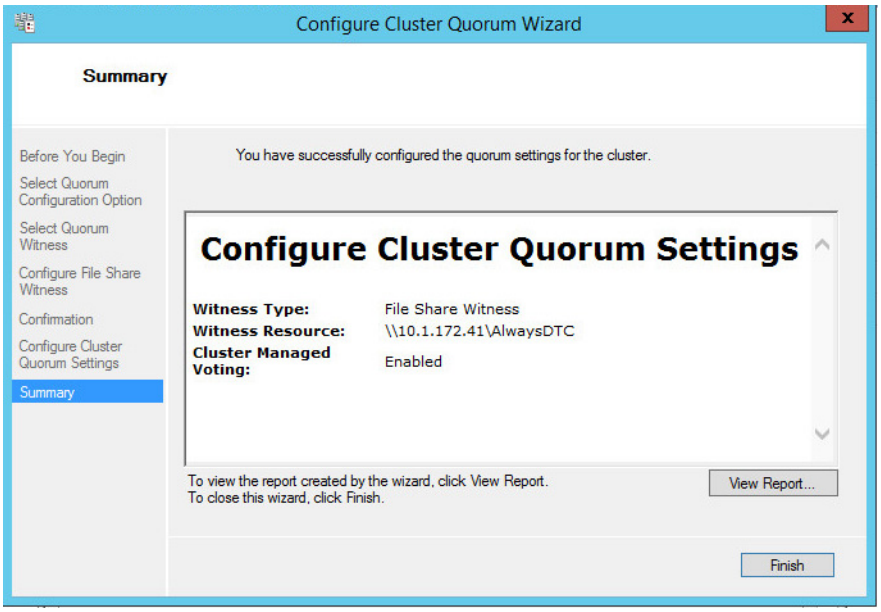
6. Click **Next**.

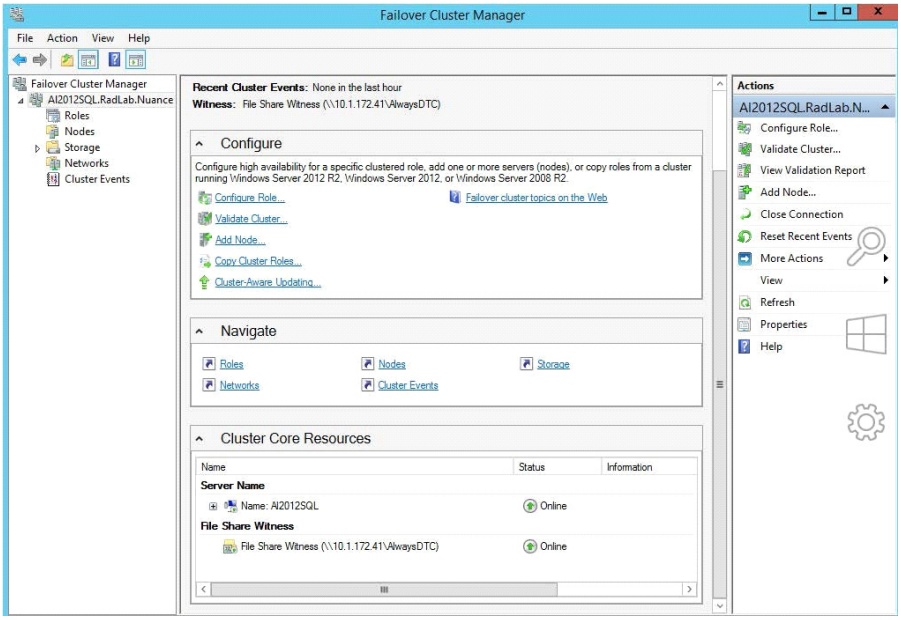


7. On the Confirmation dialog, review and if correct, click **Next**.



8. On the Summary dialog, review for any errors and click **Finish**.





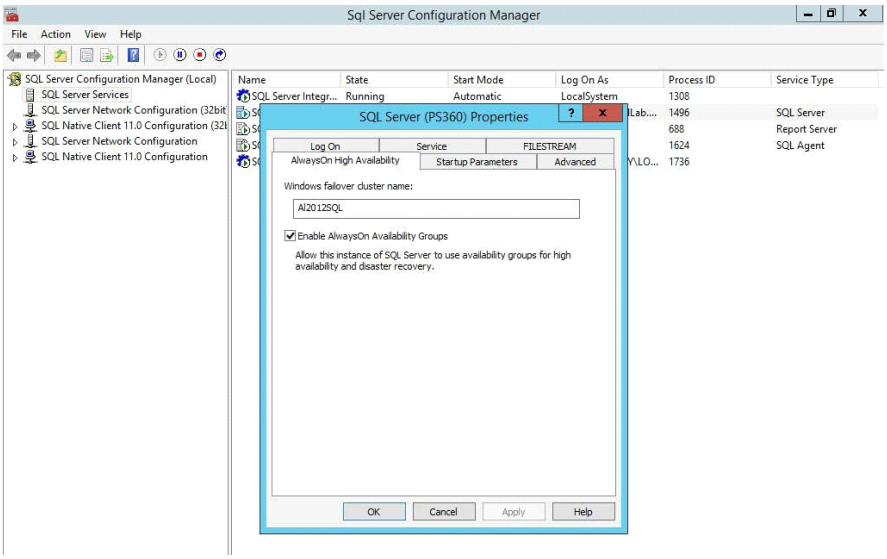
SQL Server AlwaysOn Availability

Enable AlwaysOn

Before continuing, Enable SQL AlwaysOn Availability Groups Feature on all of the SQL Server instances that you will configure as replicas in your Availability Group.

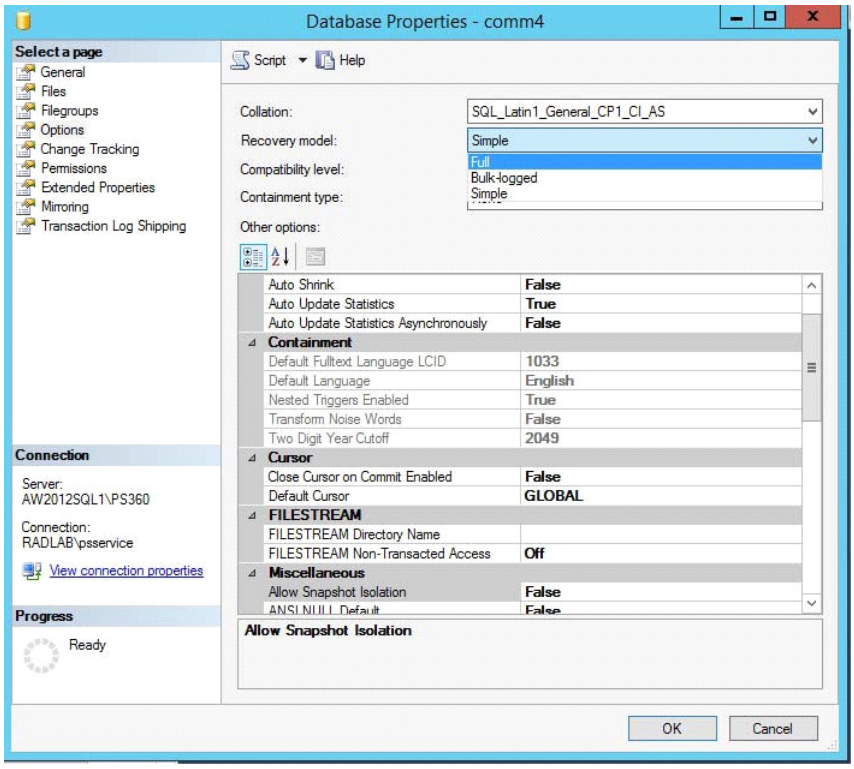
1. Open SQL Server Configuration Manager, and right-click SQL Server service, and then click **Properties**.
2. Select the AlwaysOn High Availability tab, and check **Enable AlwaysOn Availability Groups**.

   This needs to be done on all of the SQL Server instances that you will configure as replicas in your Availability Group.
3. Click **OK**.
4. You must restart the SQL Service for settings to take effect.



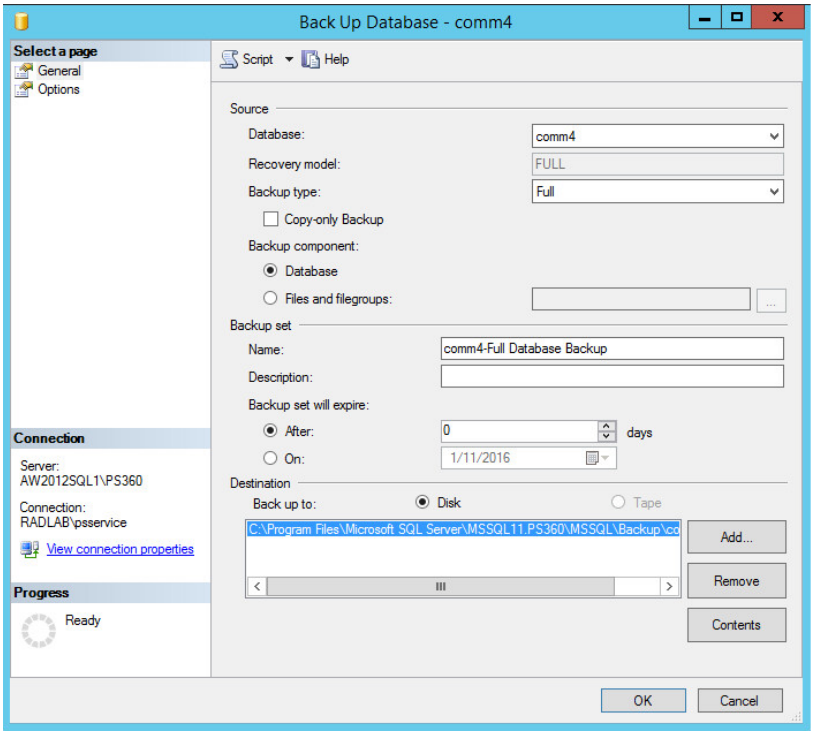
5. At this point install the Comm4 Database using the standard procedure on each of the SQL servers.
6. After this is complete delete the Comm4 database off of the secondary SQL server. Note we are doing this to add all the jobs, and the PSuser and to the server.
7. Next, prep the Primary servers Comm4 database to be used with SQL AlwaysOn. For the Database to be available for Always on, the database must be set to full recovery mode and have had a backup job run against it.
8. In SQL Enterprise manager, right-click the Comm4 database, select **Properties**, and then click **Options**.

9. On the Options dialog, click the down arrow for the Recovery mode, and select **Full**, and then click **OK**.



10. To run a backup job, right-click the Comm4 Database, select All tasks, and then select backup Database.

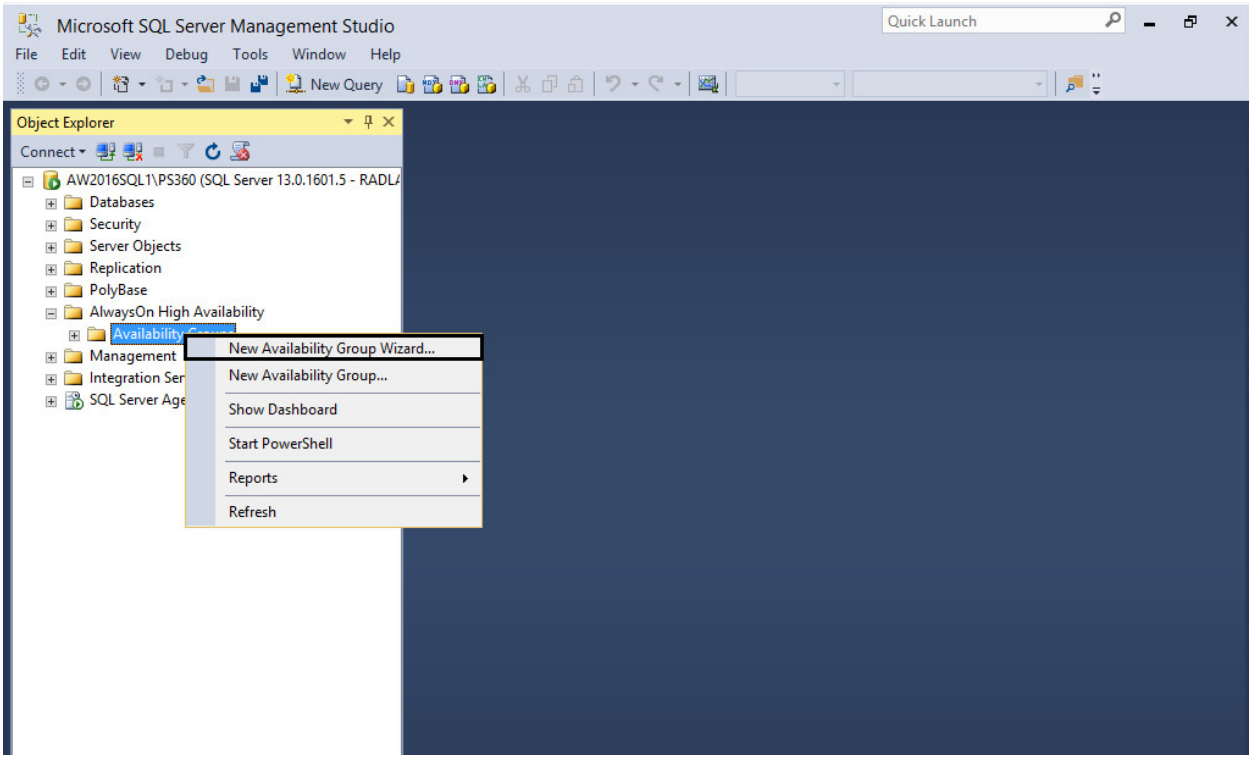
The database backup can be placed on any drive.



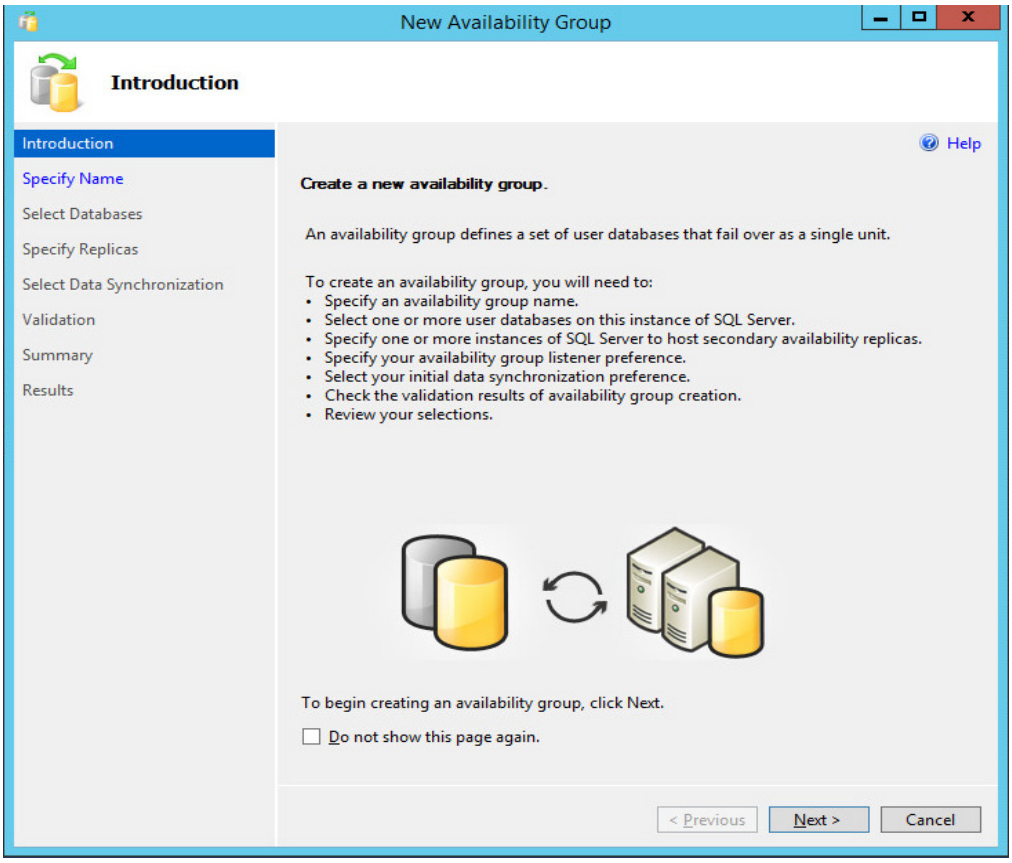
Create and Configure SQL Server 2016 AlwaysOn Availability Groups

To Create and Configure SQL Server 2016 AlwaysOn Availability Groups Log in to SQL Enterprise Manager. In Object Explorer, expand the AlwaysOn High Availability folder Right click on the AlwaysOn High Availability then click on New Availability Group wizard.

If you receive a massage that the AlwaysOn Availability Groups Feature in not activated check to see that the Enable SQL Server 2016 AlwaysOn Availability Groups Feature is turned on all of the SQL Server service instances and that the service has been restarted.

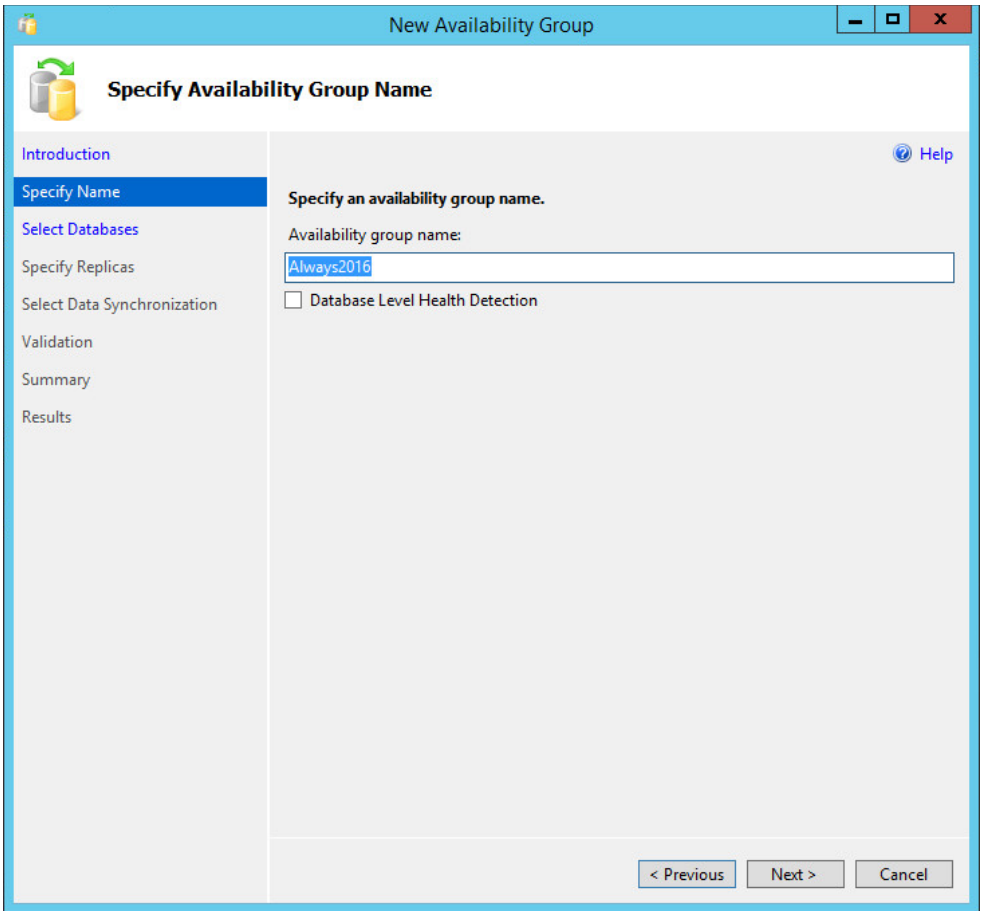


Click Next on the Introduction page

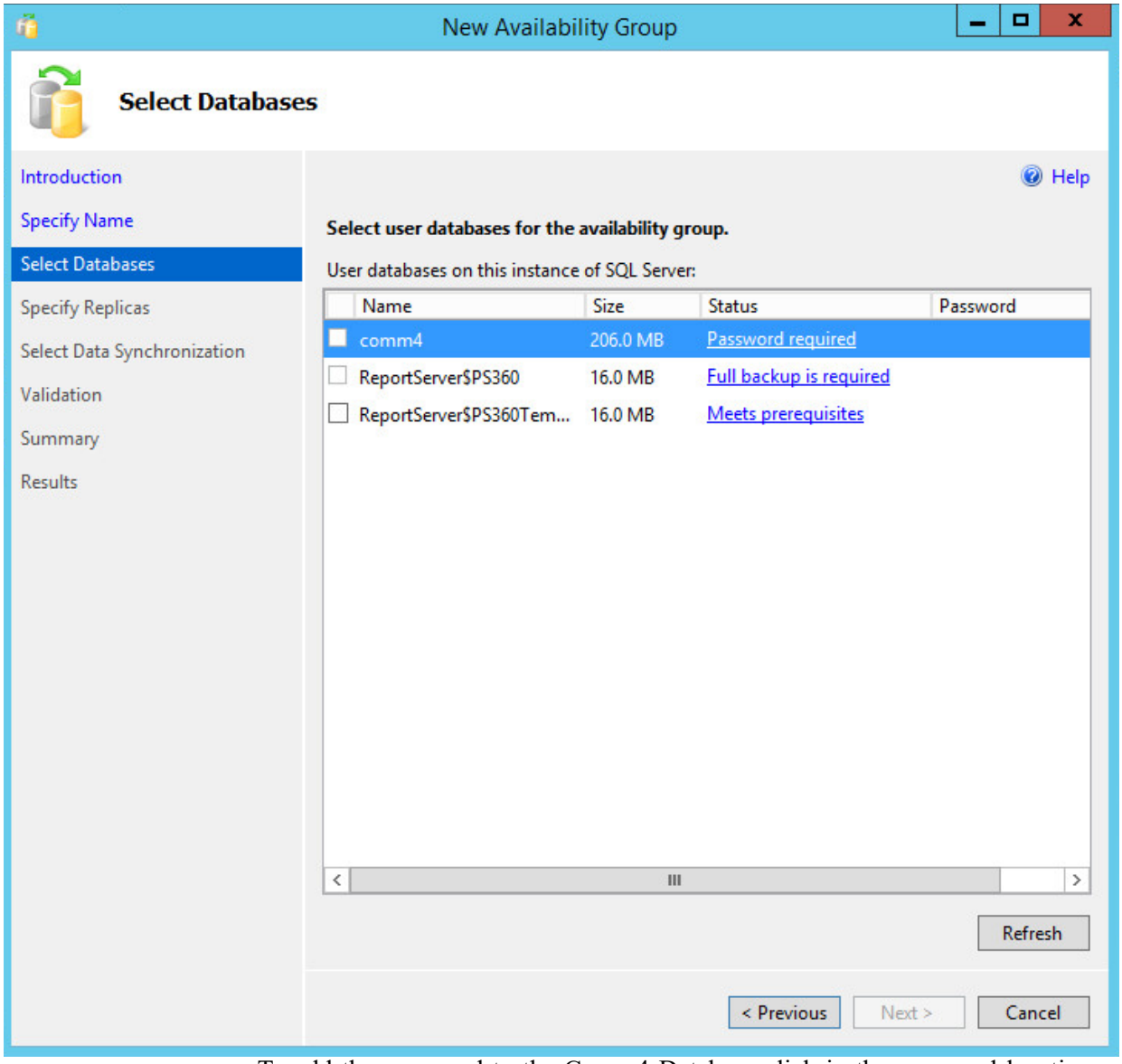


In the Specify Availability Group Name page, enter the name of the Availability Group in the Availability group name field.

Click Next.

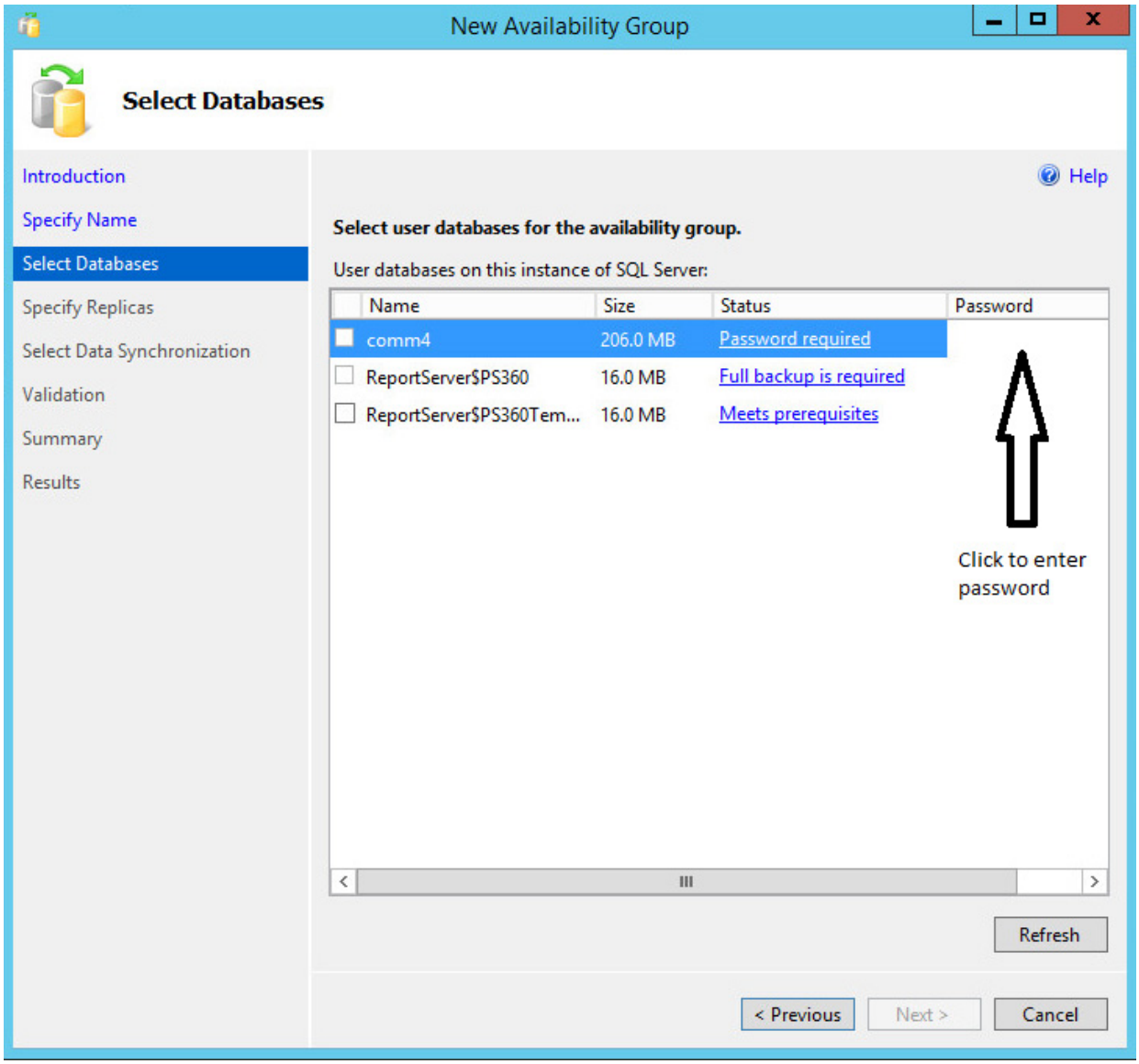


One of the Enhancements of SQL Server 2016 AlwaysOn Availability Group is that the New Availability Group Wizard Adds Support for Encrypted Database if you select an encrypted database for inclusion in an availability group, the New Availability Group wizard detects that the database is defined with a database master key and prompts the administrator for the database master key password.



To add the password to the Comm4 Database click in the password location on the Comm4

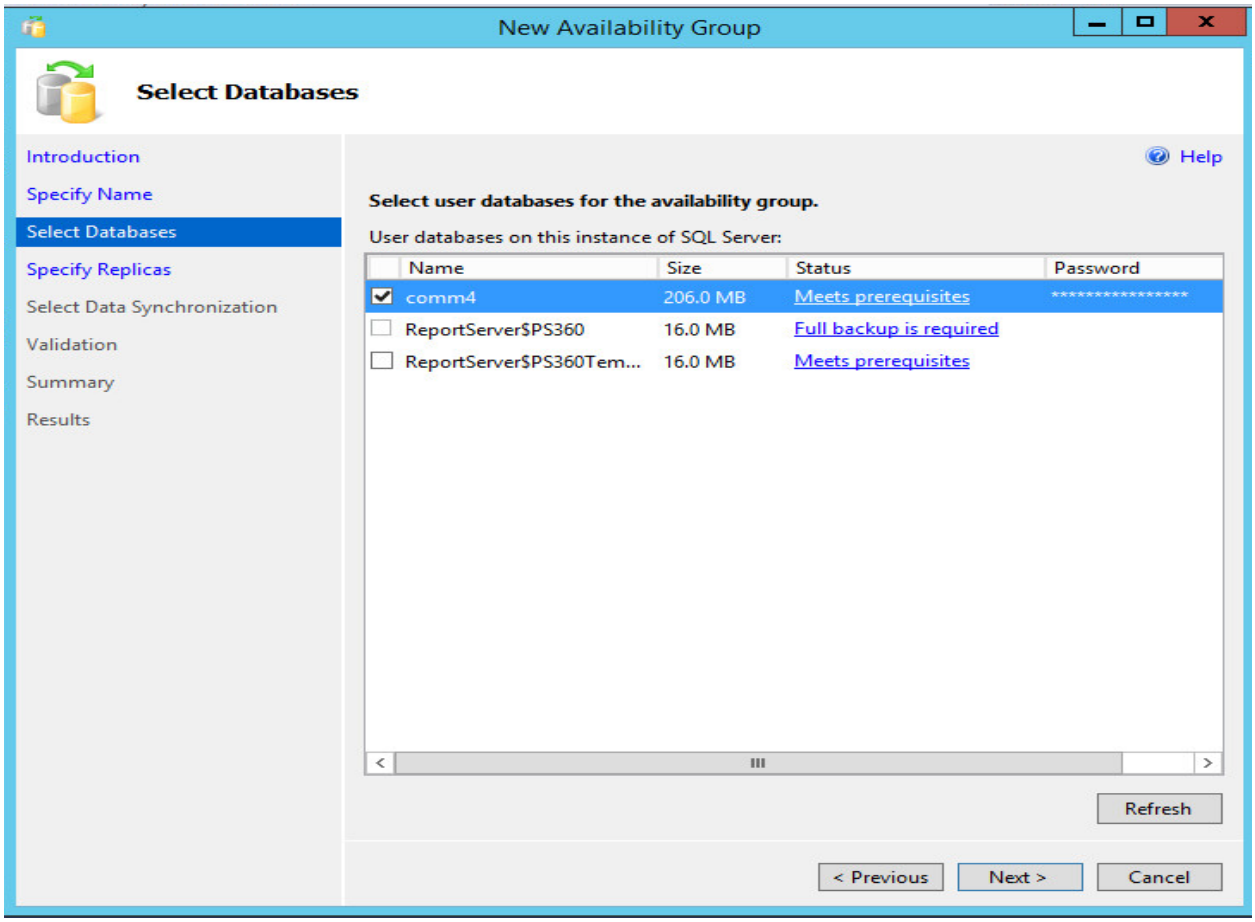
Note on our system it took a couple of clicks to get the window to allow the entering of the password and after the password was entered we had to click refresh before it was marked as Meets Prerequisites and when the Next button was active.



database master key password 67chUb=!3UdrebuD

The select Database select the Comm4 database if the database is not in a state that meets the prerequisites this must be addressed with before continuing

Note as long as the database you want to replicate states meets prerequisites you are good. If there are any other databases present that are not going to be replicated like in our case ReportServer and ReportServerTempDB they do not need to be dealt with.



Click next.

On the Specify Replicas Page you will need to add all the SQL Servers that you will be using as Replicas. Under the Replicas tab, click the Add Replicas button and connect to the other SQL Server instances that you joined as nodes in your Windows Server Failover Cluster.

Configure the following options Automatic Failover (Up to 2) :	Checked
Synchronous Commit (Up to 3) :	Un-Checked
Readable Secondary:	No

On the Endpoints tab, verify that the port number value is 5022.

On the Listener tab, select the Create an availability group listener option.

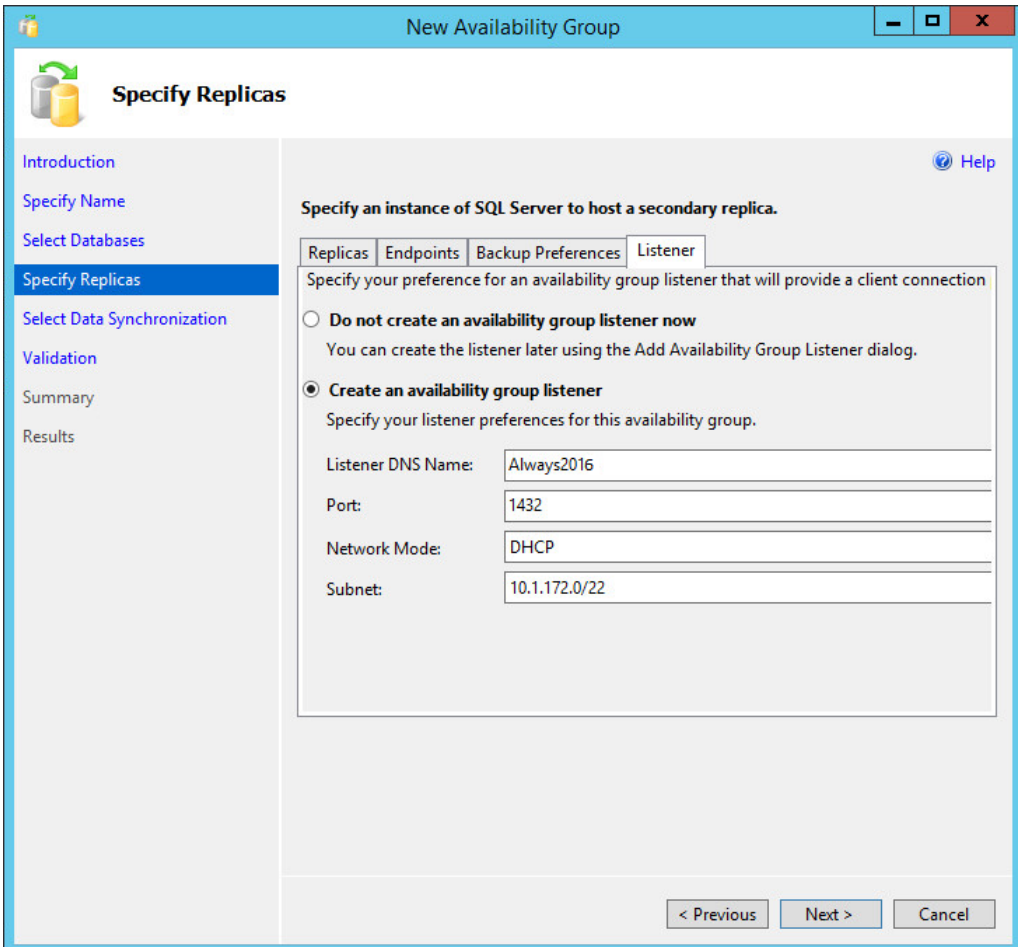
Under the Listener DNS Name fill in the name you want to call the Listener. This is the virtual name that you will use as the server name our Database connection string.

Select a Port number that is not being used

Under Network Mode you can select Static or DHCP. Note for our testing we used DHCP But setting it to a static IP address will also work.

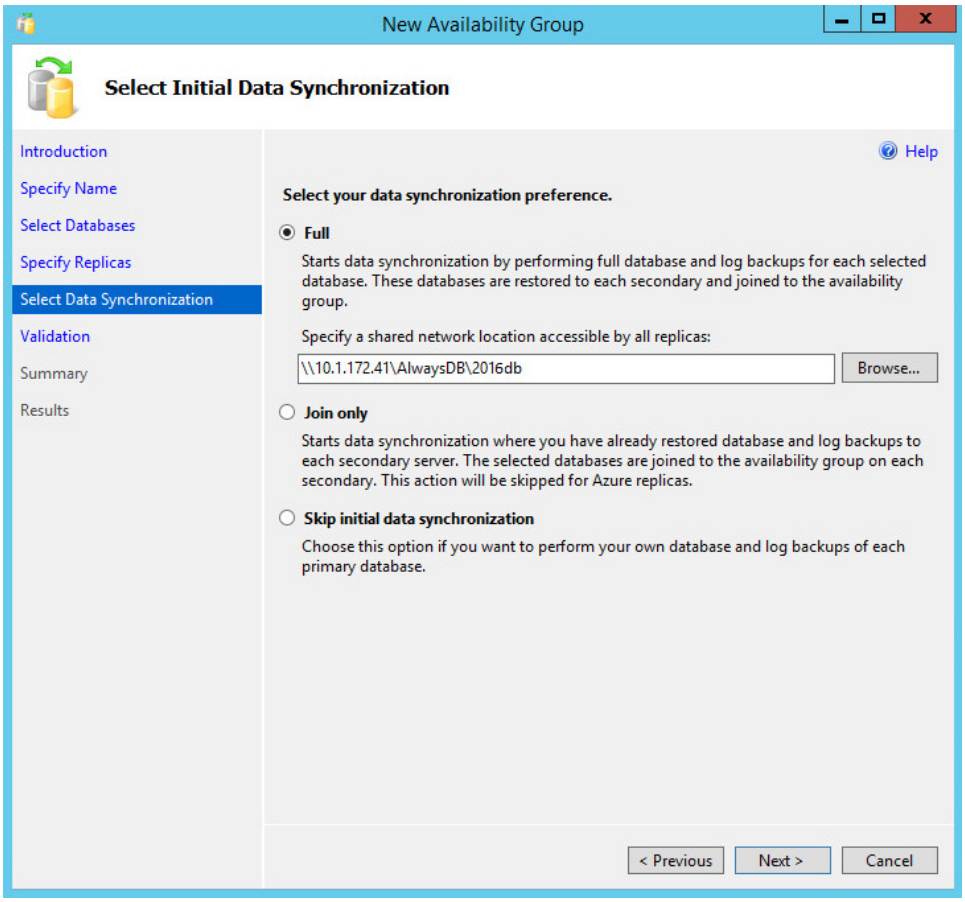
All this information will be used to create a DNS entry in the sites Active Directory.

Click Next



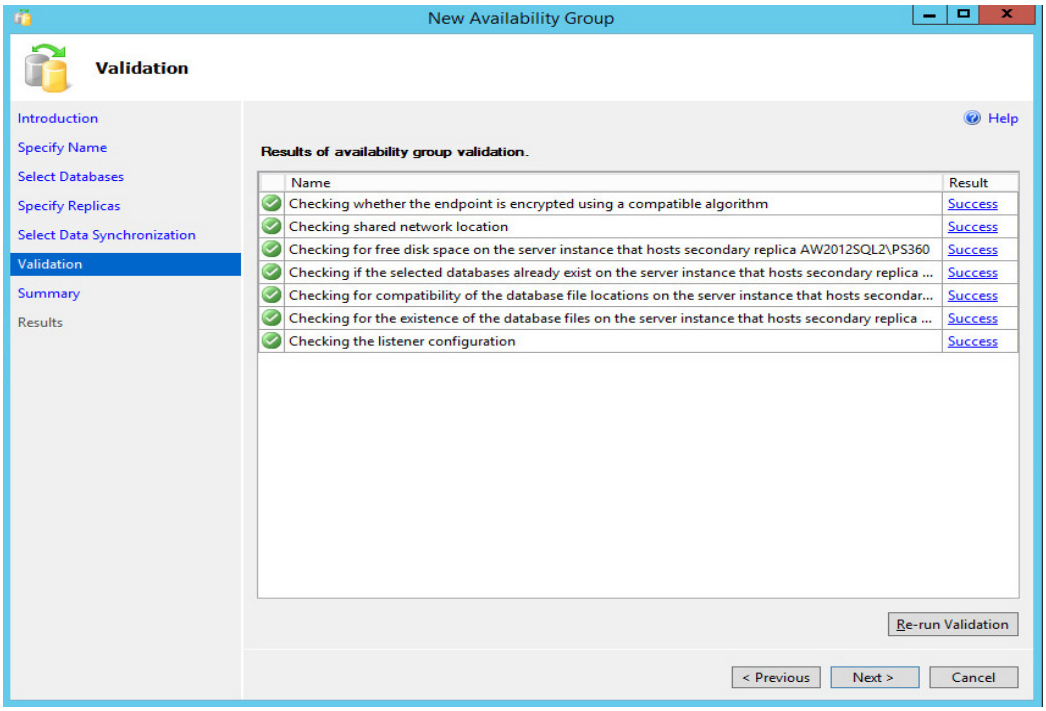
On the Select Data Synchronization page select Full option. Provide a shared folder that is accessible by the replicas and by the SQL Server service account that you used on both replicas has Write permissions to. This is just a temporary file share to store the database backups that will be used to initialize the databases in an Availability group. If you are dealing with large databases, it is recommended that you manually initialize the databases prior to configuring them as your network bandwidth may not be able to accommodate the size of the database backups.

Click Next.



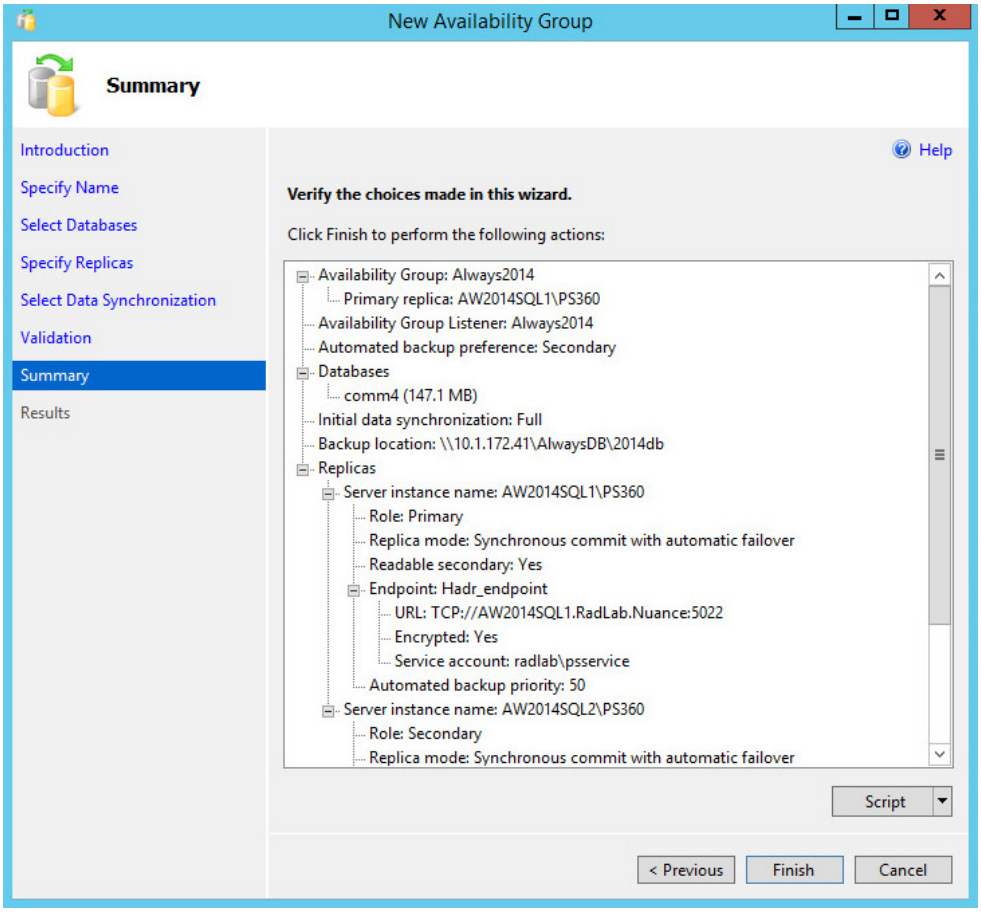
Under Validation review for any errors. As it runs you will see the green check box show up stating a success or a yellow box for a failure. Any failures must be fixed before continuing.

Click Next.



On the Summary page review your choices you have made.

Click Finish.



On the Results page review for any errors. As it runs you will see the green check box show up stating a success or a yellow box for a failure. This process will take a few minutes depending on the size of the Database. Any failures must be fixed before continuing.

If you receive “The wizard completed successfully” **Click Close**.

Verify that the Database is Synchronized expand the Databases folder and you should now see that the Comm4 databases name will have the word (Synchronized) after it on all nodes.

Verify that the Availability Group is installed expand the AlwaysOn High Availability folder

On the Primary server you should see the Availability Group you just created with the words (Primary)

On the Secondary server you should see the Availability Group you just created with the words (Secondary)

Configuring the PS360 User SID

1. On node 1 where everything is working fine, run the following query:

   ```
   select [name],SID from sys.server_principals
   where type_desc = 'SQL_LOGIN'
   ```

   This should include the ‘ps360user’ account that is used to access the database. Make note of the SID returned.

2. On node 2 that is failing, you need to drop and re-create the ‘ps360user’ login and assign it the same SID as above:

   ```
   drop login ps360user
   go
   create login ps360user
   with
       password = 'ps360userpassword',
       check_policy = off,
       sid = 0x14585E90117152449347750164BA00A7
   go
   ```

3. Replace the value for “sid” with the value returned from the query on node 1.
4. Then you need to make sure ps360user has appropriate access privileges to the Comm4 database.

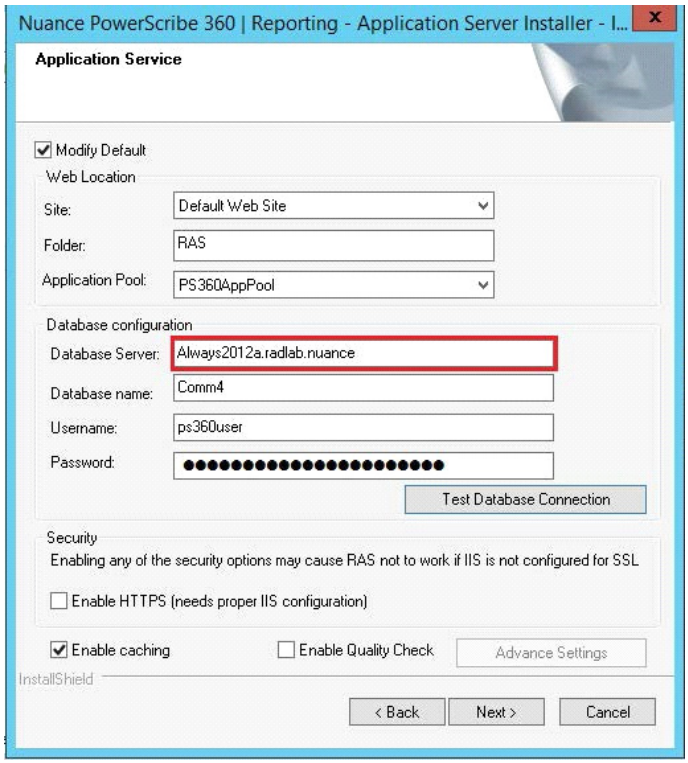
For details and more information, refer to:
http://dba.stackexchange.com/questions/30036/how-to-link-users-and-logins-in-an-availability-group

PowerScribe 360 Configuration

Configuring PS360 Running on AlwaysOn

The main difference in the installation is when setting up the SQL connection string, you must use the Availability Group Listeners name. You will need to use this name when installing or upgrading PS360.

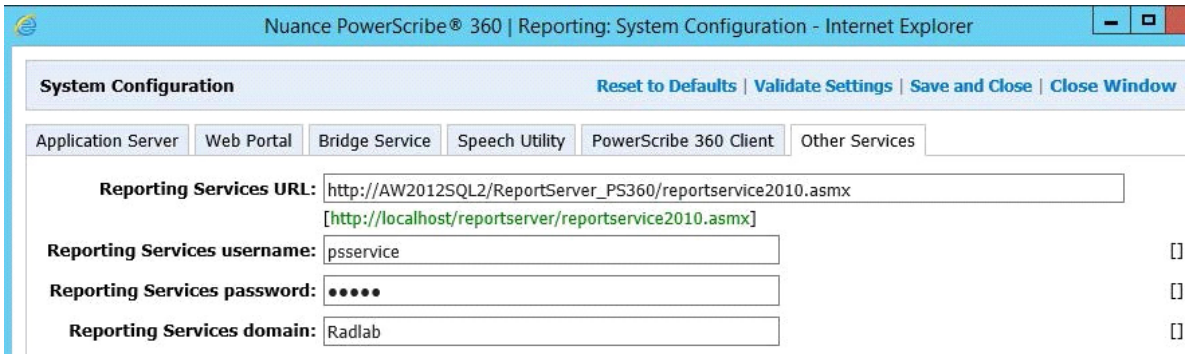
In this example, the Availability Group Listeners name is Always2012a. It was found that to access, it was necessary to use its fully qualified name. In this case, it was Always2012a.Radlab.Nuance.



Configuring Report Server to Run on the Secondary Node

When configuring SQL Reporting and PS360 Management Reports setup and configuration is the standard install. The only difference is when configuring reporting in the Admin modal point to the Secondary server. Still configure and test Reporting on both servers. This will give you the ability to fail over.

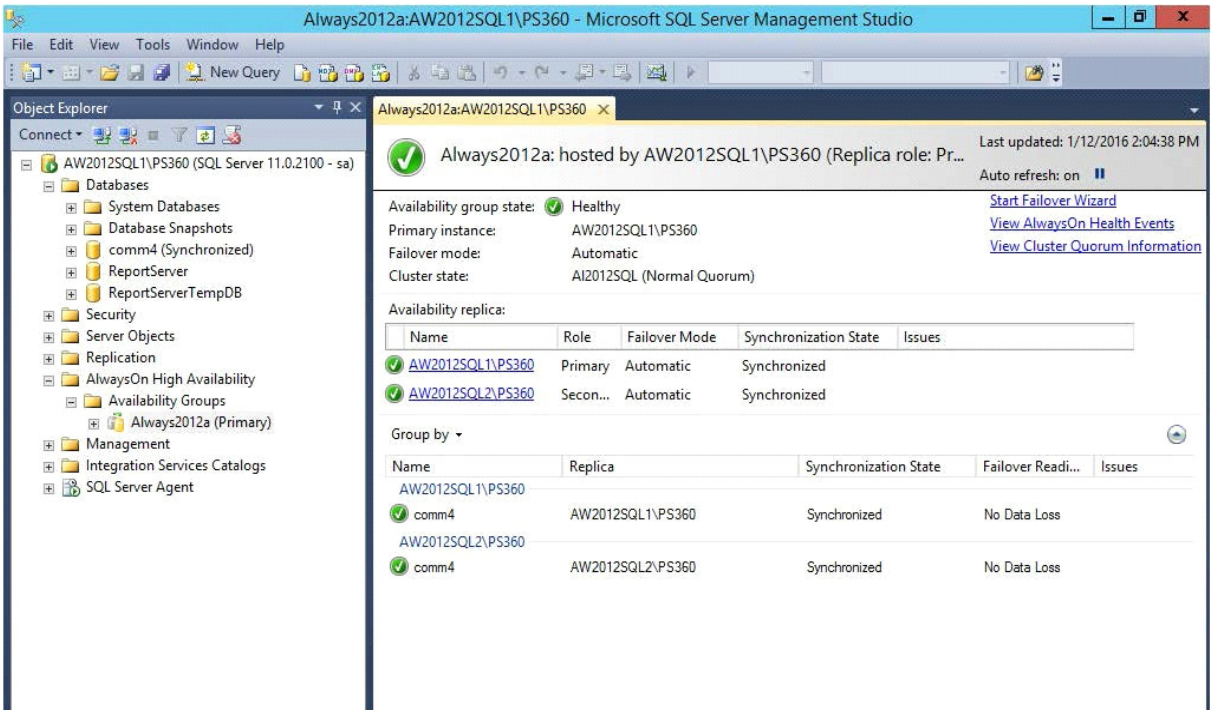
Using SQL AlwaysOn, one of the benefits, is that when you can set up the databases you set the secondary Databases to a Readable Secondary. This mode is a read-only mode. The benefit to this is it gives you the ability to take some of the load off of the Primary server when you run Reports. As long as the Admin modal is pointing at the secondary server, you will be able to take some of the load off the primary and have failover ability, if you have issues with the primary server. Only drawback is if you lose the secondary node. You will receive an error trying to load the reports. To correct this while the secondary Node is down, temporary re-point to the primary system in the Admin modal then refresh.



Tool to Monitor SQL AlwaysOn High Availability Group

SQL has a built in Dashboard to help you monitor the status of you availability groups.

1. To access the Dashboard, log in to SQL Enterprise Manager, scroll down and right-click on AlwaysOn High Availability, and then select **Show Dashboard**.



Some Strange Behaviors that Seen with SQL

Some strange behaviors that we have seen with SQL is that when you go to log in to SQL Enterprise Manager you need to check what server it is pointing at we have been seeing it jumping between the two Availability Replicas.

The other is that you need to hit the refresh on SQL Enterprise Manager after a failover.

Do not use the Failover Cluster Manager to manipulate availability groups, for example:

- Do not add or remove resources in the clustered service (resource group) for the availability group.
- Do not change any availability group properties, such as the possible owners and preferred owners. These properties are set automatically by the availability group.

Do not use the Failover Cluster Manager to move availability groups to different nodes or to fail over availability groups. The Failover Cluster Manager is not aware of the synchronization status of the availability replicas, and doing so can lead to extended downtime. You must use Transact-SQL or SQL Server Management Studio

Behavior of Client Connections on Failover

When an availability group failover occurs, existing persistent connections to the availability group are terminated and the client must establish a new connection in order to continue working with the same primary database or read-only secondary database. While a failover is occurring on the server side, connectivity to the availability group may fail, forcing the client application to retry connecting until the primary is brought fully back online.

If the availability group comes back online during a client application's connection attempt but before the connect timeout period, the client driver may successfully connect during one of its internal retry attempts and no error will be surfaced to the application in this case.

https://msdn.microsoft.com/en-us/library/hh213417.aspx#DbmConnectionString

https://msdn.microsoft.com/en-us/library/hh882437.aspx

File Server Data Replication

Copy the Hot Spare Files to the Application Servers

IMPORTANT

You must create the following folders on both the Production Server and the Hot Spare Application Servers.

Download the PS360_Hot_spare_3.5.zip.

Under the Nuance folder on the Production and Hot Spare Servers, create the "HotSpare" folders (e.g., X:\Nuance\HotSpare).

Production Server

Copy the contents of the "Production" folder from the Hot Spare Install to the **X:\Nuance\HotSpare folder** on the production server.

Hot Spare Server

Copy the contents of the "HotSpare" folder from the Hot Spare Install to the **X:\Nuance\HotSpare folder** on the server.

Folder Sharing/Permissions

You must make sure that the Administrators Group has Full Control permissions for both the folder security and folder sharing access for the following folders on both application servers:

- X:\Nuance\Wave
- X:\Nuance\DragonUsers
- X:\Nuance\BridgeLogs

Data Replication

The publication version numbers MUST be equal on both systems. If this is not set properly, the users will have issues switching to the hot spare or failback.

Modify the HotSpareConfig.bat

In the procedures in this section, you modify the files used by the Hot Spare Process.

1. Locate in the X:\Nuance\HotSpare\ folder on the hot spare server the file HotSpareConfig.bat:
2. Highlight the file, right click and choose **Edit**.
3. You must fill in the names of the servers, user names, passwords and drive letters in the REQURIED configuration section or the HotSpare scripts will not work. Review and enter values as needed in the OPTIONAL configuration section for your environment.

   EXAMPLE:
   The first REQUIRED value is the name of the application server. For this example, that name is **PS360-APP-01**. Looking at the file you will see the following:
   :: Name of the production App/SQL Server
   :: Example: PROD_APP=SERVERNAME
   set PROD_APP=
   Add the server name after the = in the set PROD_APP= line so it looks like this:
   set PROD_APP=**PS360-APP-01**
4. After you have edited the file entries, **save** the file and exit the application.
5. Place a copy of the HotSpareConfig.bat file on both the Production and HotSpare Application servers in the folder X:\Nuance\HotSpare (X is the data drive letter).

Create the Profile Data Move Task

Use the steps below to create the Data Move Task on the Hot Spare.

1. Select **Start/Programs/Administrative tools/Task Scheduler**.
2. Choose **Create Basic Task** in the right pane.

   The Create Basic Task wizard opens.
3. Name the task, “Profile Data Move”.
4. Enter a description.
5. Click **Next** to schedule the Task Trigger.

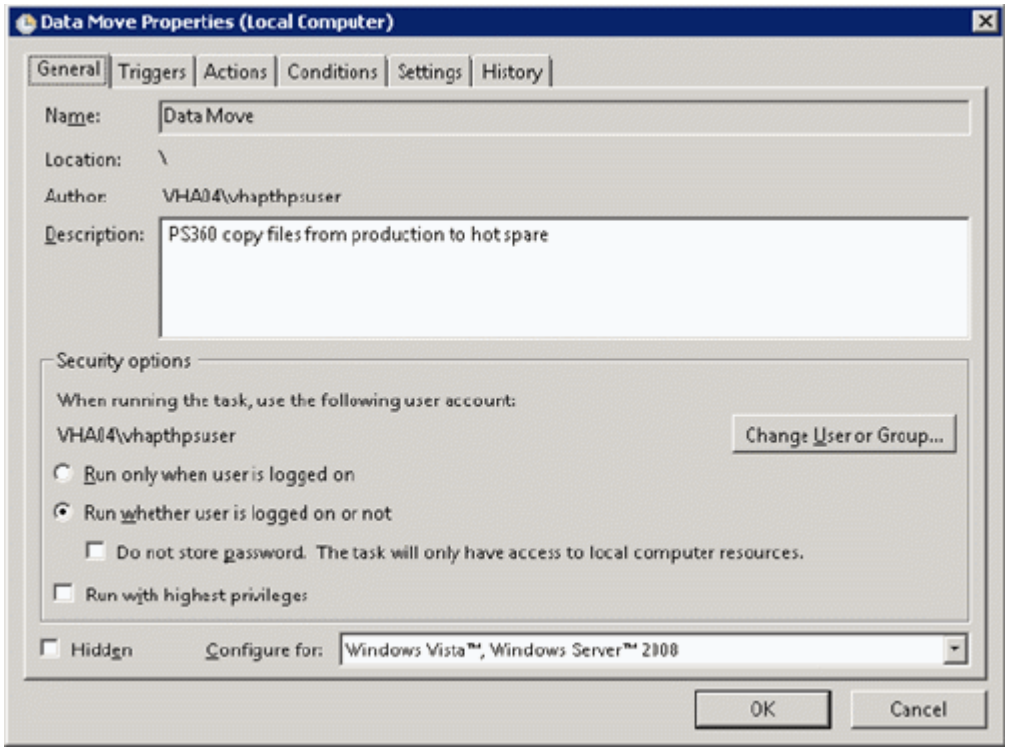
   The Task Trigger window displays.
6. Set the task to run **Daily**.

   You will further refine the Data Move schedule in the next procedure.
7. Click **Next** to set the time for the Daily Trigger.
8. Set a **Start** date and time for the Task to run and how many times for recurrence. Nuance recommends setting the **Recur** option to 1 so that the Task runs every day.
9. Click **Next** to set the Task Action.
10. Select the **Start a program** option.
11. Click **Next** to select the program to start.
12. Using the Browse button, browse to the program to the **Profile_Data_move.bat** file
13. Click **Next**.

    The Summary window displays.
14. Confirm that the options are correct in the Summary window for the particular task and click **Finish**.

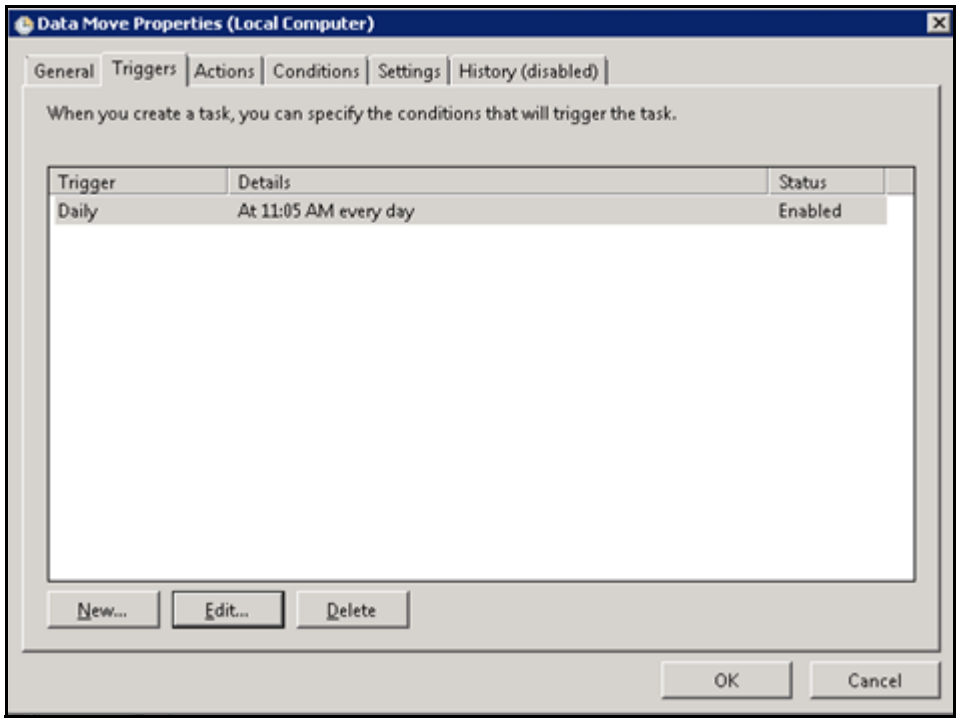
    You are returned to the Task Scheduler window.
15. Click the **Refresh** button for the window.
16. Browse the list of Tasks for the Profile Data Move Task, and double-click it to see the particulars for this Task in the lower center pane. From this location, you can further select to Run, End, Disable, Properties, etc., for the Task using the options in the lower half of the right pane.
17. Make sure that the Profile Data Move task is highlighted in the Scheduler window and select **Properties** in the lower right pane.

18. On the Profile Data Move Properties dialog, General tab, select Security option to **Run whether user is logged on or not**, and click **OK**.



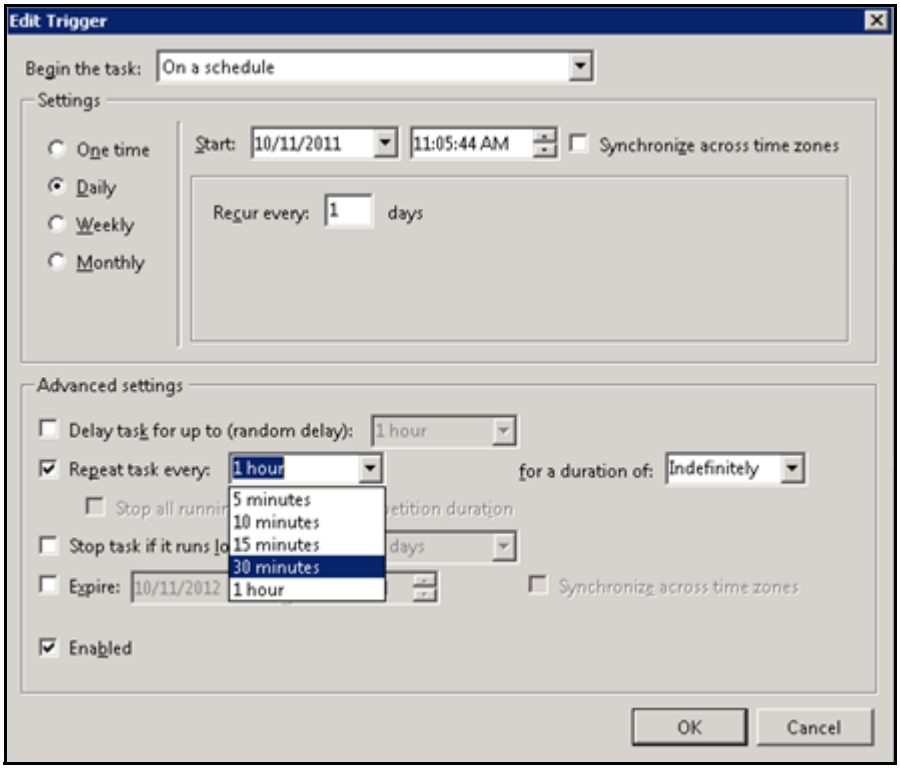
A prompt displays for the account to run, user domain account that has administrator rights to both servers.

19. On the Profile Data Move Properties dialog, click the **Triggers** tab.



20. Click **Edit**.

    The Edit Trigger dialog displays.



21. In the Advanced settings pane, check the **Repeat task every** option and then select the desired time in the drop-down list. Our example uses 30 minutes. The time depends on how long it takes to complete this task.
22. In the **for a duration of** list, select **Indefinitely**.
23. Check the **Enabled** option.
24. Click **OK** to close the Edit Trigger dialog.
25. Click **OK** to close the Properties dialog.
26. Execute the task and verify the data files are copied to the hot spare system.
27. Close the Task Scheduler application.

Create the Wave Data Move Task

Use the steps below to create the Data Move Task, on the Hot Spare.

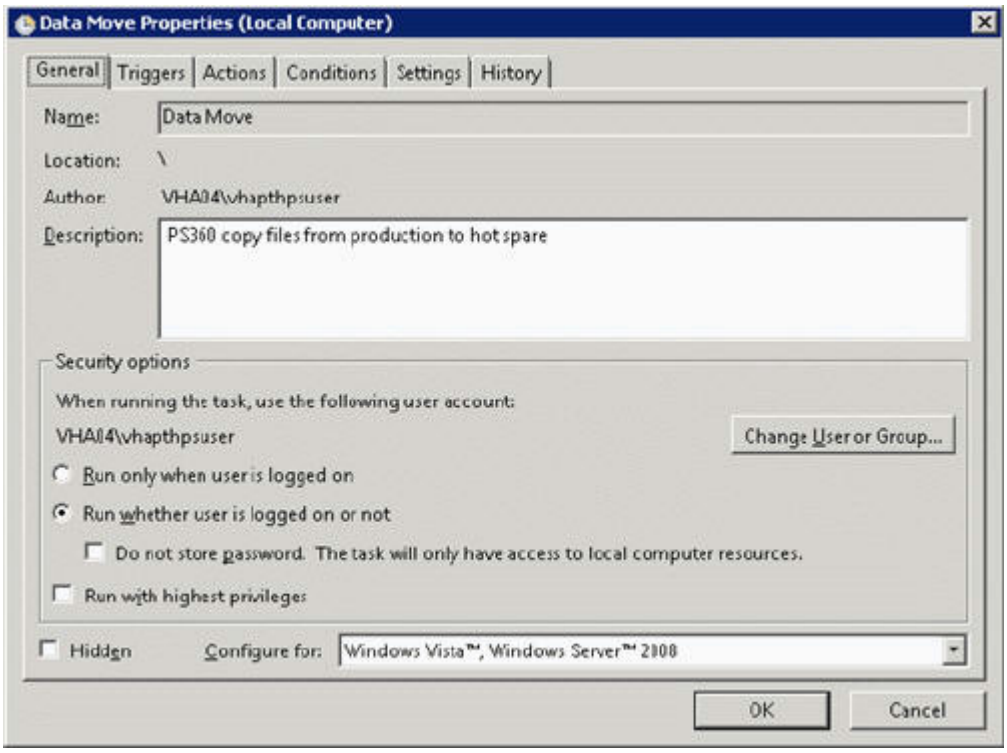
1. Select **Start/Programs/Administrative tools/Task Scheduler**.
2. Choose **Create Basic Task** in the right pane. The Create Basic Task wizard opens.
3. Name the task, “Wave Data Move”.
4. Enter a description.
5. Click **Next** to schedule the Task Trigger. The Task Trigger window displays.
6. Set the task to run **Daily**.

   You will further refine the Data Move schedule in the next procedure.
7. Click **Next** to set the time for the Daily Trigger.
8. Set a **Start** date and time for the Task to run and how many times for recurrence. Nuance recommends setting the **Recur** option to 1 so that the Task runs every day.
9. Click **Next** to set the Task Action.
10. Select the **Start a program** option.
11. Click **Next** to select the program to start.
12. Using the Browse button, browse to the program to the **Wave_Data_move.bat** file.
13. Click **Next**.

    The Summary window displays.
14. Confirm that the options are correct in the Summary window for the particular task and click **Finish**.

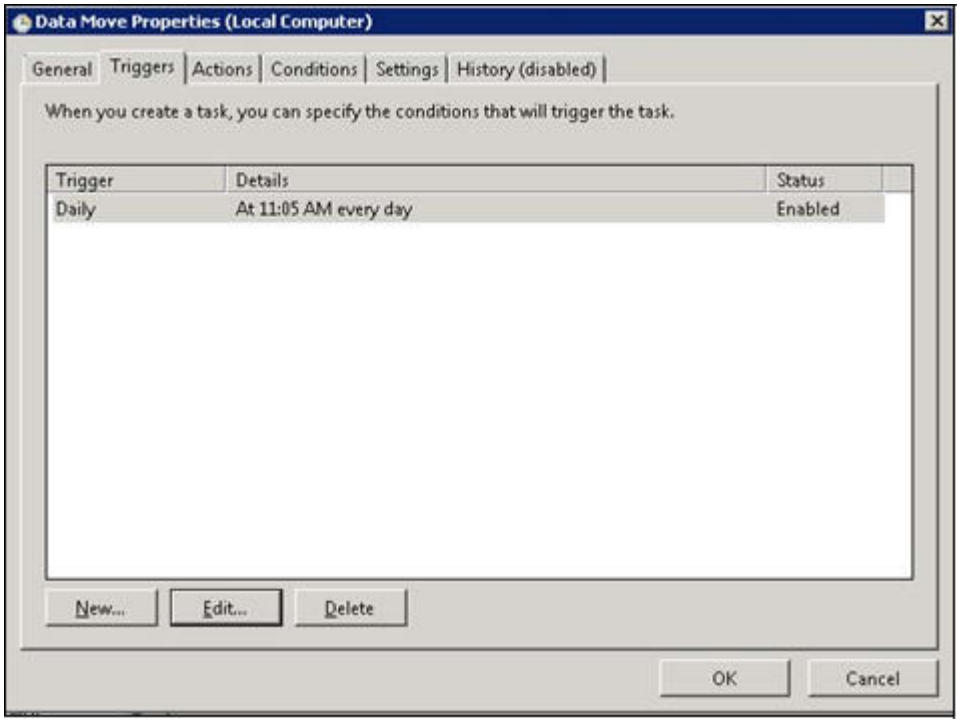
    You are returned to the Task Scheduler window.
15. Click the **Refresh** button for the window.
16. Browse the list of Tasks for the Wave Data Move Task, and double-click it to see the particulars for this Task in the lower center pane. From this location, you can further select to Run, End, Disable, Properties, etc., for the Task using the options in the lower half of the right pane.
17. Make sure that the Wave Data Move task is highlighted in the Scheduler window and select **Properties** in the lower right pane.

18. On the Profile Data Move Properties dialog General tab, select Security option to **Run whether user is logged on or not**, and click **OK**.



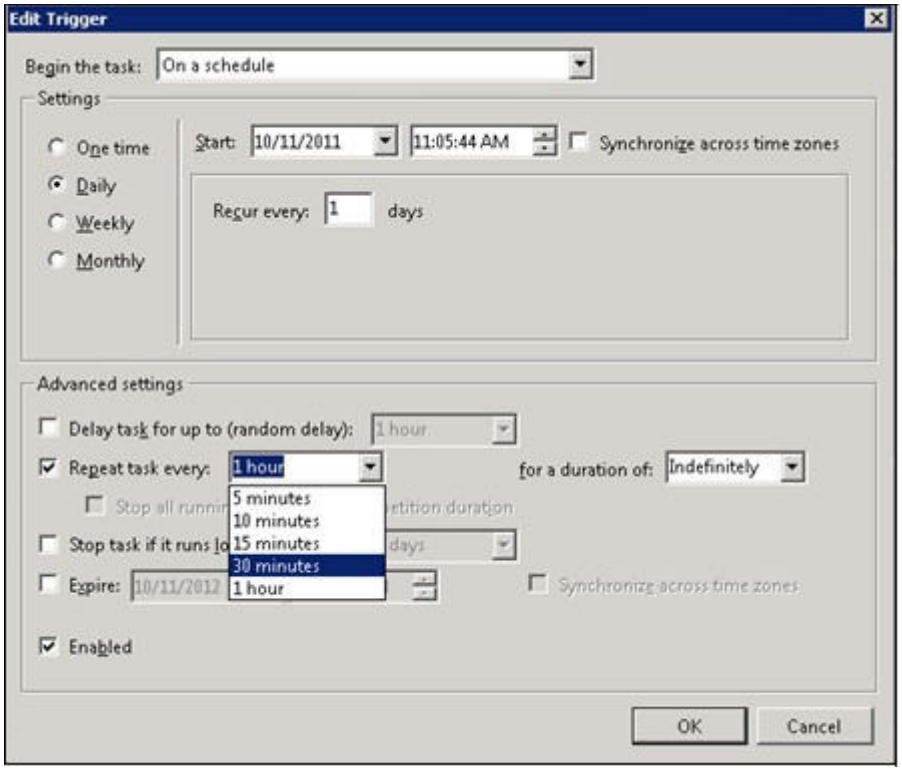
A prompt displays for the account to run, user domain account that has administrator rights to both servers.

19. On the Wave Data Move Properties dialog, click the **Triggers** tab.



20. Click **Edit**

    The Edit Trigger dialog displays.



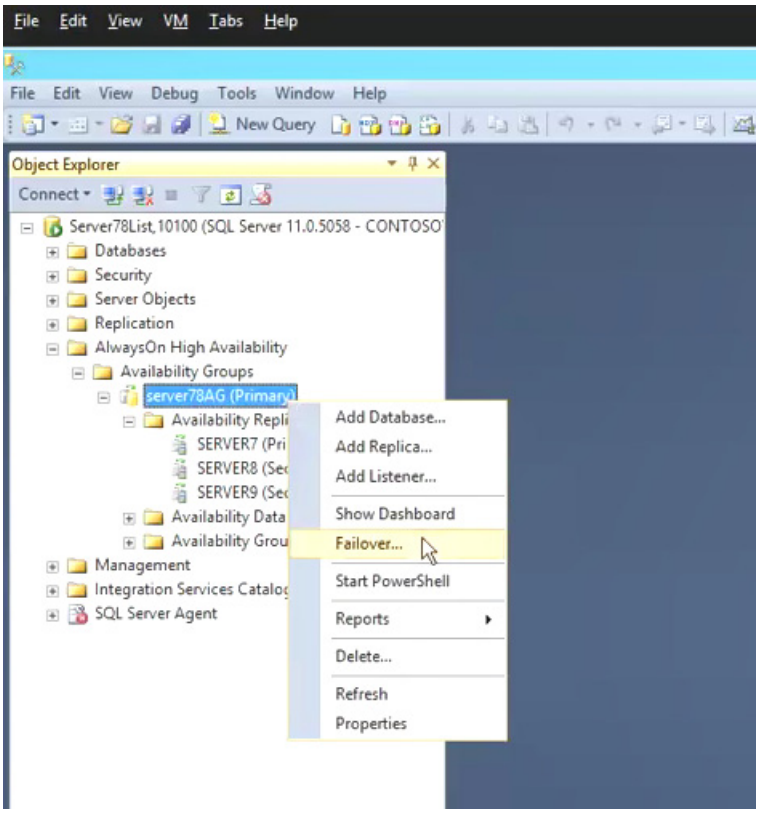
21. In the Advanced settings pane, check the **Repeat task every** option and then select **5 minutes** in the drop-down list.
22. In the **for a duration of list**, select **Indefinitely**.
23. Check the **Enabled** option.
24. Click **OK** to close the Edit Trigger dialog.
25. Click **OK** to close the Properties dialog.
26. Execute the task and verify the data files are copied to the hot spare system.
27. Close the Task Scheduler application.

Manually Failover the SQL Availability Group

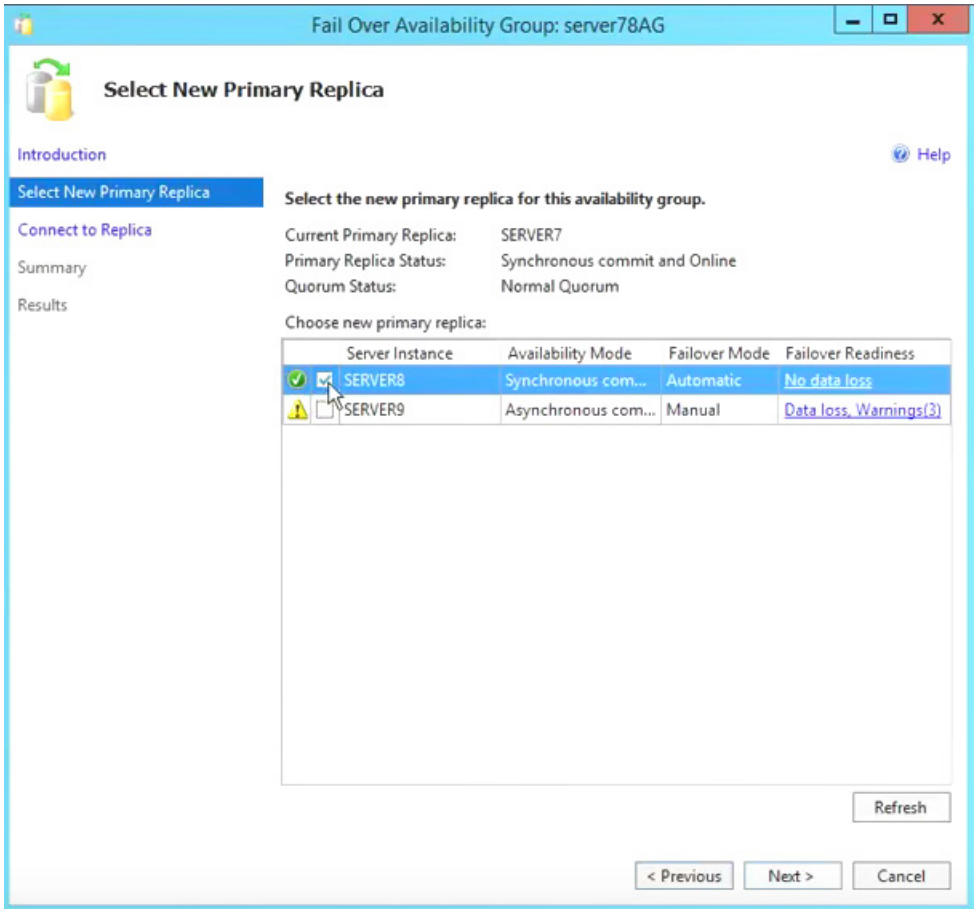
This should only be performed by the site's DBA (Database Administrator) or a qualified IT person.

To manually fail over an availability group:

1. In Object Explorer, connect to a server instance that hosts the availability group that needs to be failed over, and expand the server tree node.
2. Expand the AlwaysOn High Availability and the Availability Groups nodes.
3. In the Availability Group, right-click the server to failover, and then select **Failover**. The Failover Availability Group dialog displays.



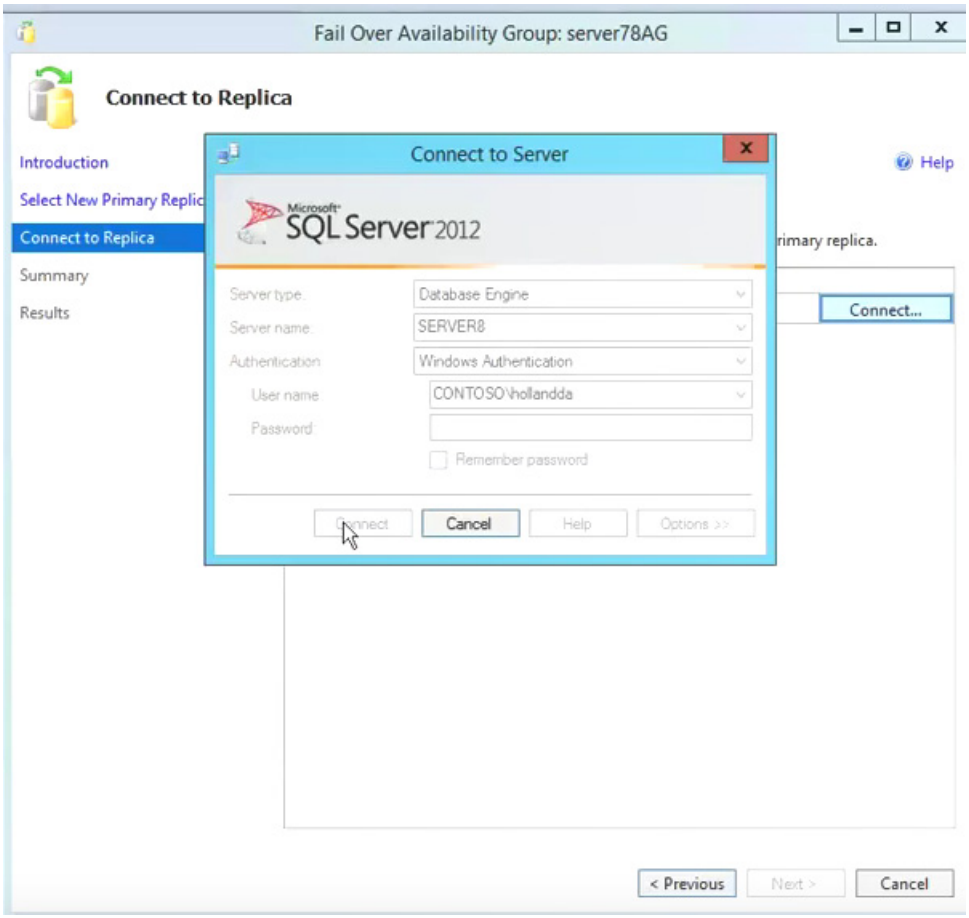
4. Check the server you want to be as the new primary server.



5. Click **Next**.

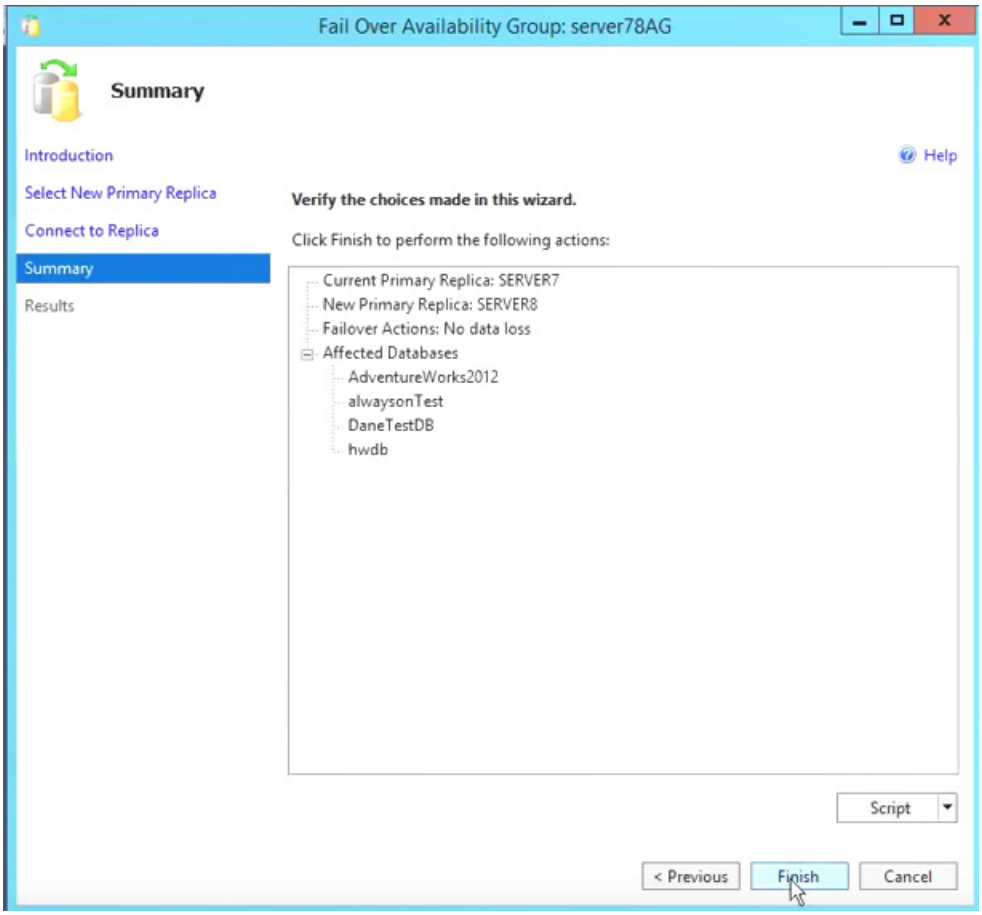
The Connect to Replica dialog displays.

6. On the Connect to Replica dialog, click **Connect**. The Connect to Server dialog displays.



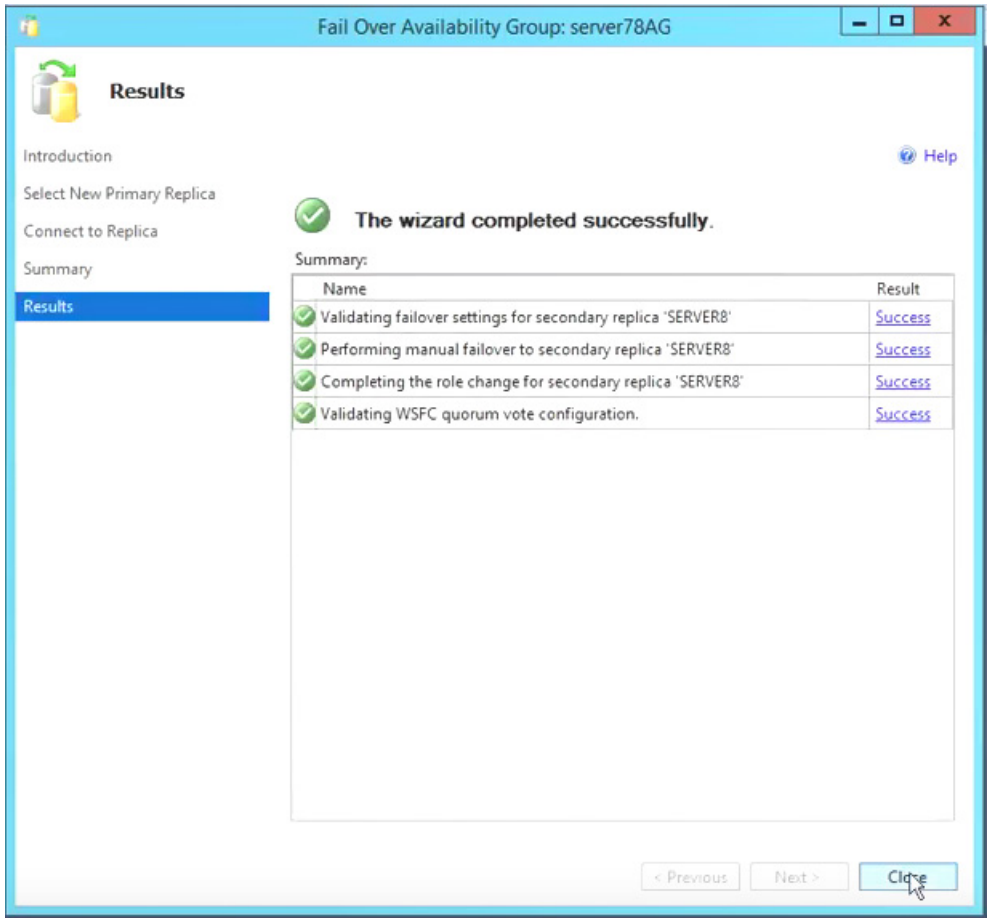
7. Enter the login credentials and click **Connect**, then click **Next**.

The Summary dialog displays.



8. Review the choices, and click **Finish**.

Once the fail over completes, the Results dialog displays.



9. Click **Close**.

Cutting Over to the Hot Spare

When the SQL AlwaysOn fails over, either automatically or manually, you will have to restart the RadBridge Service on the active system.

If your site performs a full cut over (Application and SQL), to the Hot Spare System, the following steps must be taken:

1. Have all users log out.
2. IT needs to update the Client FQDN DNS entry to point the client to the Hot Spare Application Server.
3. IT needs to execute a manual failover of the SQL AlwaysOn to the secondary DB server (Hot Spare).
4. IT needs to execute the Activate HotSpare.bat file on the Hot Spare Application Server. This will automatically stop and start the appropriate application server services on both systems.

Manual Revision History

Note: In this table the most recent changes are first by date.

Date	Sec	Page	Change (Paragraph, Sentence, Figure, Table, etc.)	Initials
10/12/18	1	All	Added Best Practices	BW