Oracle® DIVArchive

Cluster Manager Installation and Configuration Guide

Release 7.3

E63003-04

April 2016

ORACLE®

Oracle DIVArchive Cluster Manager Installation and Configuration Guide, Release 7.3

E63003-04

Primary Author: Lou Bonaventura

Contents

Preface

This document provides general guidelines for the installation of Microsoft Cluster Server (MSCS) software and Oracle Fail Safe software combined with Oracle's DIVArchive software, to achieve high availability for DIVArchive components by building a two node cluster.

This guide describes only MSCS and Oracle Fail Safe installation steps required for DIVArchive cluster installation.

The Active Directory installation and management is not documented, although it is mandatory for the two DIVArchive Cluster Node servers to be part of a Windows domain.

Audience

This document guides administrators through the Oracle DIVArchive Cluster Manager installation, configuration, and routine maintenance.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

For more information, see the following documents in the Oracle DIVArchive documentation set or the recommended Microsoft Oracle documentation set:

- *Oracle DIVArchive Installation and Configuration Guide*
- *Oracle DIVArchive Operations Guide*
- *Oracle Fail Safe Installation Guide*
- *Enable Support for Clustered Windows Servers using clustered RAID controllers*

  https://support.microsoft.com/en-us/kb/2839292

- *What's New in Failover Clustering in Windows Server 2012*

  http://technet.microsoft.com/en-us/library/hh831414.aspx
- *What's New in Failover Clustering in Windows Server 2012 R2*

  http://technet.microsoft.com/en-us/library/dn265972.aspx
- *Configure and Manage the Quorum in a Windows Server 2012 Failover Cluster*

  http://technet.microsoft.com/en-us/library/jj612870.aspx
- *NIC Teaming Overview*

  http://technet.microsoft.com/en-us/library/hh831648.aspx
- *Deploy a Guest Cluster using a Shared Virtual Disk*

  http://technet.microsoft.com/en-us/library/dn265980.aspx
- *Failover Clusters Cmdlets in Windows PowerShell*

  http://technet.microsoft.com/en-us/library/hh847239.aspx
- *Microsoft Best Practice for Configuring and Operating Server Clusters*

  http://technet.microsoft.com/en-us/library/cc785714%28v=ws.10%29.aspx
- *Microsoft Best Practice for Cluster-Aware Updating*

  http://technet.microsoft.com/library/jj134234#BKMK_FW
- *Microsoft Windows Firewall with Advanced Security*

  http://technet.microsoft.com/en-us/library/hh831365.aspx
- *Microsoft Cluster-Aware Updating*

  http://technet.microsoft.com/en-us/library/hh831694.aspx
- *Microsoft Cluster-Aware Updating Best Practice*

  http://technet.microsoft.com/library/jj134234#BKMK_FW

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1 Introduction

This chapter describes an overview of the Microsoft Cluster Server (MSCS), Oracle Fail Safe, Oracle DIVArchive integration, and tested releases.

Prerequisites

The prerequisites for installation must be met before the arrival of the Oracle Installation and Delivery Team at your location.

You are responsible for installing the Microsoft Cluster in your environment and providing a dedicated domain user with specific permissions. See "Domain Account Requirements (Performed by Customer)" for the required user permissions.

During installation you must make three shared partitions available so Oracle personnel can configure DIVArchive in your environment. The drive letters `E:`, `F:`, and `H:` must be used for the shared partitions.

When the Oracle team arrives they will install and configure the Oracle Fail Safe and Oracle DIVArchive software for you.

Oracle Fail Safe Integration with Windows

Oracle Fail Safe enables configuring and managing the Oracle Database and other Oracle and third-party applications for high availability on Windows clusters. An instance runs on only one node at a time.

A cluster is a group of independent computing systems that operate as a single virtual system. This type of configuration eliminates individual host systems as single points of failure. Oracle Fail Safe works with Microsoft Cluster Server to ensure that if a failure occurs on one cluster system, workloads running on that system fail over to a surviving system. Oracle Database combined with Oracle Fail Safe on a Windows cluster protects the system from both hardware and software failures.

When properly configured, Oracle Fail Safe ensures a surviving system becomes operational in less than one minute, even for heavily-used databases.

Oracle Real Application Clusters Integration with Windows

Oracle Real Application Clusters integrate with Microsoft Cluster Server clusters deployed on all Windows operating systems supporting clustering. This enhances high availability by offering:

- Optional automatic restarts of a failed instance or listener in a cluster.
- Detection and resolution of instance cluster hangs.

- Elimination of connect time failover TCP/IP timeout delays for new connection requests.
- Use of user written scripts after database state changes (from online to offline or vice versa).

Oracle DIVArchive Cluster Solution

DIVArchive Cluster uses Oracle Fail Safe. An external disk hosts the Oracle data file and backups. The disk serves the nodes through a Serial Attached SCSI (SAS) connection. Two Windows 2012 R2 Standard nodes connect to the disk and host Oracle Fail Safe and DIVArchive software.

All software components on each node must have the same release. Release discrepancies may cause cluster failure. For example, if Node-1 has DIVArchive 7.3 installed, Node-2 must also have DIVArchive 7.3 installed, not a different release.

The following software releases are currently supported:

Oracle DIVArchive
Release 7.2 or later

Oracle Fail Safe
Release 4.1 or later

Microsoft Cluster Server
Release 2012 R2 Standard

Tested and Supported Software Releases

The following Microsoft Cluster Server (release 11.2.0.4.7 - 64-bit) software patch levels have been tested and are currently supported with Windows 2012 R2 Standard, Oracle Fail Safe 4.1 (`failsafe_41_V38321-01.zip`), and DIVArchive 7.2 or later:

KB2843630	KB2913760	KB2962123	KB2989930
KB2862152	KB2914218	KB2962409	KB2990532
KB2868626	KB2916036	KB2964718	KB2992611
KB2876331	KB2917929	KB2965500	KB2993100
KB2883200	KB2917993	KB2966826	KB2993651
KB2884101	KB2918614	KB2966828	KB2993958
KB2884846	KB2919355	KB2966870	KB2994897
KB2887595	KB2919394	KB2967917	KB2995004
KB2888505	KB2920189	KB2968296	KB2995388
KB2892074	KB2922229	KB2971203	KB2996799
KB2893294	KB2923300	KB2971850	KB2998174
KB2894029	KB2923528	KB2972103	KB3000850
KB2894179	KB2923768	KB2972213	KB3002885
KB2894852	KB2925418	KB2972280	KB3003057
KB2894856	KB2926765	KB2973114	KB3003743
KB2896496	KB2928193	KB2973201	KB3004394

KB2898108	KB2928680	KB2973351	KB3005607
KB2898514	KB2929961	KB2973448	KB3006226
KB2898871	KB2930275	KB2975061	KB3008242
KB2900986	KB2931358	KB2975719	KB3008627
KB2901101	KB2931366	KB2976627	KB3008923
KB2901128	KB2938066	KB2976897	KB3008925
KB2902892	KB2939087	KB2977174	KB3010788
KB2903939	KB2950153	KB2977292	KB3011780
KB2904266	KB2954879	KB2977765	KB3012199
KB2906956	KB2955164	KB2978041	KB3013126
KB2908174	KB2956575	KB2978122	KB3013410
KB2909210	KB2957189	KB2978126	KB3013769
KB2911106	KB2958262	KB2978668	KB3013816
KB2911134	KB2959626	KB2979573	KB3014442
KB2911804	KB2959977	KB2979576	KB3025390
KB2912390	KB2961072	KB2979582	
KB2913152	KB2961851	KB2984006	
KB2913270	KB2961908	KB2988948	

2

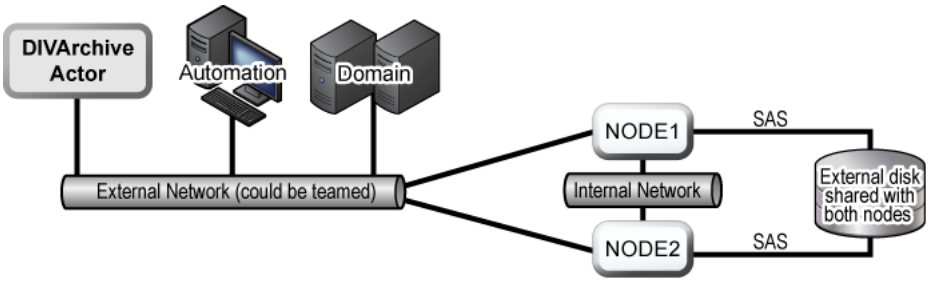
Installation Requirements

In this chapter, you will identify and confirm that your systems have the proper installation requirements, and set permissions for the domain user and cluster.

Hardware Requirements

- Server requirements for DIVArchive Clustered Managers (two identical servers):
  - Rack-mount chassis
  - One CPU Xeon E5-2420 (six cores - 1.9GHz) minimum
    * Embedded Oracle license is restricted to one CPU (processor card).
  - 16 GB RAM
  - Two 300GB Hard Disk Drive (HDD) 10,000 RPM (configured in RAID 1) system disks
    * If you use DIVArchive to archive complex objects (for example DPX), the best course of action is to request specific recommendations based on the estimated traffic (in terms of size and number of objects to be archived per day). In general, Oracle recommends using a minimum of two 900GB HDD with 10,000 RPM if complex objects need to be archived.
    * This recommendation is also valid for the backup Oracle DIVArchive Manager or an Oracle DIVArchive Actor if an Actor server is used for the backup Manager.
    * For more information and assistance on setting up your RAID refer to Microsoft's *Enable Support for Clustered Windows Servers using Clustered RAID Controllers*: https://support.microsoft.com/en-us/kb/2839292.
  - Redundant power supply and fans
  - Two on-board Gigabit Ethernet interfaces (copper RJ45 interfaces)
  - One SAS or Fiber Channel Host Bus Adapter (HBA) for the shared disk bay connection.
    * A shared disk bay with dual RAID controller (SAS or Fiber Channel interface) and seven 300 GB SAS disks connected to both servers for the Oracle database.
  - One Fiber Channel HBA for the tape library control. The Fiber Channel HBA is not required in the following cases:
    * With SONY Petasite libraries (controlled through the PCS software and a network API).

        * With StorageTek libraries if the ACSLS software with network ACSAPI interface is used in the configuration. *Important: If ACSLS virtual libraries are used, an HBA will be required (consult with Oracle for more information)*.
        * If the library control is based on SCSI LVD interface but some legacy libraries still use SCSI HVD interfaces which are no longer supported, contact Oracle in case the library control is based on a SCSI physical interface rather than Fiber Channel.
    - Windows 2008 R2 SP1, Enterprise Edition 64-bit server or Windows 2012 R2 Standard.
- Shared disk array requirements are:
    - One direct-attached shared disk array with dual controllers, dual power and dual fans.
    - Six 146 GB disk drives (6 Gb/sec 10,000) RAID 5 virtual disks.
    - Two spare physical disks.
- Two HBAs for direct attachment of servers to the shared storage.



Software Requirements

The following software is required for successful MSCS installation, configuration, and operation:

- Windows 2008 R2 SP1, Enterprise Edition 64-bit server or Windows 2012 R2 Standard.
- DIVArchive Database installation package
- Oracle Fail Safe 4.1 installation package
- Shared disk array drivers and management software
- All servers must be fully patched with important updates, recommended updates, and Microsoft updates - they must all be the same patch level.
    - All Microsoft patches as of January 7, 2015 have been tested and verified.

Network Requirements

The following connectivity and parameters are required for successful MSCS installation, configuration, and operation:

- For cluster management, one IP address and host name (`DIVA-CL-MSCS`) from the public network with corresponding Domain Name Service (DNS) and Active Directory entries on the DNS and domain controllers.

- For the Oracle Cluster Group, one IP address and host name (`DIVA-CL-ORC`) from the public network with corresponding DNS and Active directory entries on the DNS and domain controllers.
- For the cluster node's public network, two IP addresses - one per node (internal access only).
- For the cluster node's private network, two IP addresses - one per node.
  - The private network is reserved for cluster communications and is commonly referred to as the *heartbeat* network.
- When configuring the network interfaces:
  - Do not specify a default gateway or DNS servers.
  - On the **DNS Settings** tab, deselect the check box for the ***Register this connection's address in the DNS*** option.
  - On the **WINS Settings** tab, deselect the check box for the ***Enable LMHosts Lookup*** option.
  - On the **WINS Settings** tab, select the check box for the ***Disable NetBIOS over TCP/IP*** option.
  - Label the network interfaces as `Public` and `Private` respectively.
- The two server nodes must be members of a Windows domain.
- If NIC Teaming is in use, it must be configured before you create the cluster.

Example IP Addresses and Host Names

The following are examples of valid IP addresses and associated host name combinations:

- `172.20.128.129` `DIVA-CL-MSCS`
- `172.20.128.130` `DIVA-CL-ORC`

- `172.20.128.125` `RD-MC1` (Public)
- `10.10.10.125` `RD-MC1` (Private)

- `172.20.128.127` `RD-MC2` (Public)
- `10.10.10.127` `RD-MC2` (Private)

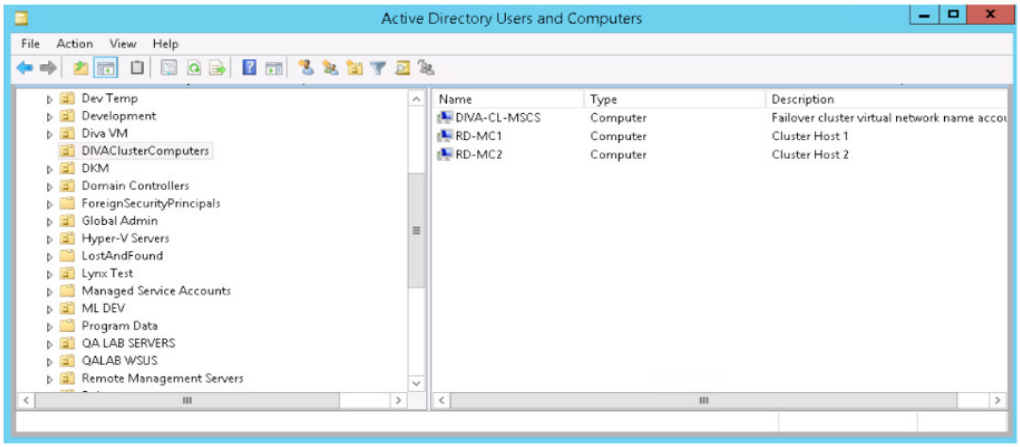
Domain Account Requirements (Performed by Customer)

You must have a dedicated domain account to install and manage the DIVArchive Cluster Manager. You must set the following local permissions on each domain account cluster node:

- Local Administrator
- Logon as batch job
  - Should be included with Local Administrator permissions.
- Logon as service mode
  - Should be included with Local Administrator permissions.

For example purposes this book uses a domain account named *DIVAClusterAdmin* that is a member of the *Domain Users* group.

For organizational purposes, Oracle recommends using a *DIVAClusterComputers* Active Directory Organizational Unit (OU). You use the Active Directory Users and Computers screen for managing the OU. Active Directory Users and Computers is an MMC snap-in that is a standard part of Microsoft Windows Server operating systems.



Granting Domain User Permissions to Create the Cluster

To successfully create a Cluster, you must ensure the Domain User has permission to ***Create Computer Objects*** in the Cluster Container and ***All Descendant Objects***. Alternately, the domain administrator can pre-create a computer object for each node and Cluster Name Objects.

If the domain administrator created an existing computer object, ensure that it is in a disabled state. You must also ensure that the user creating the Cluster has `Full Control` permission to that computer object using the Active Directory Users and Computers tool before creating the cluster. After you create the Cluster, repeat the steps below to give the Cluster Name Object the same `Full Control` permissions as the domain user.

To find out more about Cluster Permissions visit:

- https://technet.microsoft.com/en-us/library/cc731002(v=ws.10).aspx
- https://technet.microsoft.com/en-us/library/dn466519.aspx#BKMK_CreateVCOs

Use the following procedure to add `Full Control` permissions to the OU for the domain user:

1. Open the Active Directory Users and Computers snap-in from the Windows Server Management console.
2. Right-click the ***DIVAClusterComputers*** computer object and click **Properties** on the context menu to display the Properties dialog box.
3. Click the **Security** tab, and then select the Domain User (DIVAClusterAdmin in the examples) in the Group or user names area at the top of the screen.
4. Click the **Advanced** button on the bottom right side of the screen to open the Advanced Security Settings screen.
5. On the **Permissions** tab, locate the domain user and click the listing one time to highlight the domain user.

6. Click **Edit** just under the ***Permission*** entries area to open the Permission Entry screen.
7. On the top of the screen verify that the ***Type*** option is set to **Allow**, and the ***Applies to*** option is set to **This object and all descendent objects**.
8. Select all of the check boxes in the Permissions area.
9. Click **OK** on the bottom of the screen to apply the permissions.

3

Configuring the Microsoft Cluster (Performed by the Customer)

Configuring the Microsoft Cluster is the responsibility of the customer. The installation and configuration of the cluster must be completed before the Oracle Delivery and Installation Team arrives at your location.

The following subsections describe what you need to do to prepare for the Oracle team's arrival. Complete the steps in the following sections to configure the Microsoft Cluster for use with DIVArchive.

Configuring the External Disk

The following subsections are generic in nature. Due to differences in manufacturer disk and array management software, your installation process and configuration may differ slightly from the instructions presented here - however, the overall concept and configuration will be the same.

First you will install the disk management software.

Installing the Disk Management Software

Perform the following steps on *each cluster node server*:

1. Log on as a local administrator.
2. Insert the manufacturer's installation DVD. If the installer does not start automatically, locate and double-click the `setup.exe` file (or whichever file is used) to launch the installer.
3. Proceed through the storage software installation wizard; accept the license agreement and click **Next**.
4. If asked what features you want to install, select the *full feature set* and click **Next**. This is typically the recommended choice by manufacturers. Be sure to install the following if offered:
   - Management Consoles
   - Host Software
   - Volume Shadow-Copy Services
   - Virtual Disk Services
   - Event Monitoring Service (start automatically on one host only)

5. Select the installation location and click **Next**. Oracle recommends leaving the default installation path unless there is a compelling reason to change it.
6. When the installation process is complete, exit the installation program and restart the computer.
7. Log into the computer as a local administrator.
8. Open the Windows Management Console. and select the **Device Manager** menu item on the left side of the screen.
9. Confirm that the **Multipath I/O (MPIO)** driver was installed. This is required during the cluster building operation and should have been installed with the cluster feature.
10. Expand the **Disk Management** section of the Device Manager and confirm that multipath disk devices are present for each of your drives.

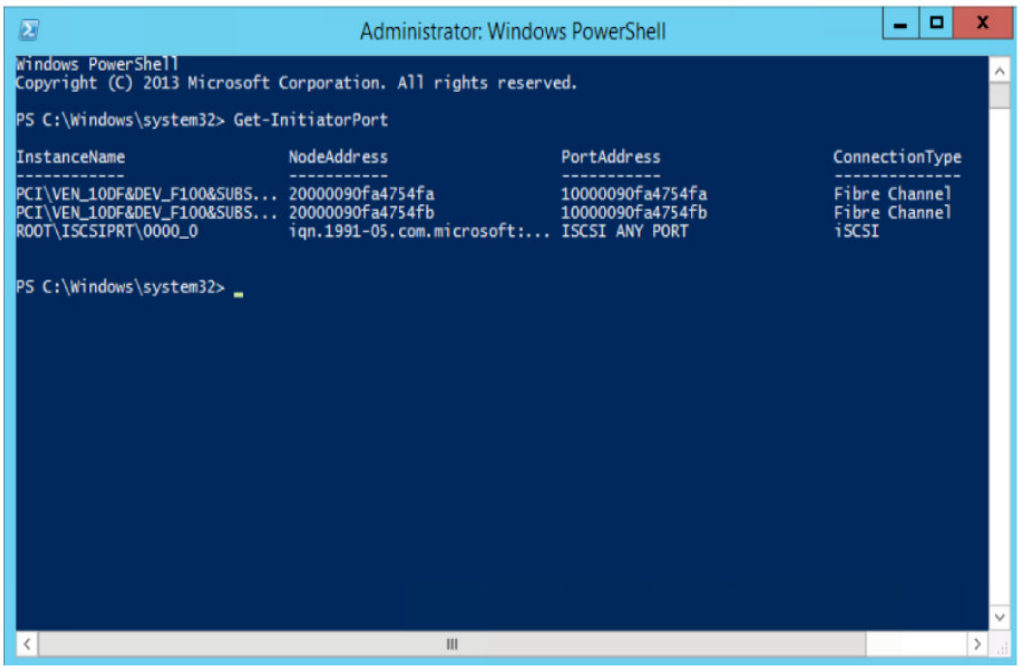
Next you will configure the storage you just added to the system.

Configuring Storage

Perform the following procedure on a *single cluster node server only*:

1. Log onto one of the node servers as a local administrator.
2. Launch the Disk Storage Manager that was installed with your storage software.
3. If the storage manager software has an option to automatically detect arrays, Oracle recommends using this method. Select the automatic detection method option (if available) and click **OK**.
   - If automatic detection is not available, or if the array is not detected, add the array manually.
   - You will need the ***IP address***, ***DNS Name***, or ***Network Name*** if the array is outside the local subnetwork.
4. Once the array is discovered (or manually added), right-click the array name and click **Manage Storage Array**.
5. Locate the ***Host Mappings*** configuration area in your storage manager software and click **Define Host**. This is where you will add Cluster Hosts and Host Groups.
6. Now you need to define the ***Cluster Hosts***. Most storage manager software will use a wizard style interface to perform this task.
   1. Enter the ***Host Name*** (in this case `rd-mc1`).
   2. Tell the wizard if you plan to use storage partitions on the array (you should answer **no** to this question).
   3. Click **Next**.
   4. Assign the ***Host Port Identifier*** by selecting (or creating) an identifier, giving it an alias (or user label), and then adding it to the list to be associated with the host (in this case `rd-mc1`).

      If you need to identify the ***HBA Port Address***, open a Windows PowerShell as an administrator and execute the command: `Get-InitiatorPort`



5. Click **Add** to complete the association and then click **Next**.

7. Now you identify the host's operating system (in this case ***Windows***).

8. Click **Next**.

9. This completes the configuration - click **Finish**.

   Some manager software will allow you to save the host definition as a script. Saving the definition as a script enables using the script as a template for adding additional hosts (if or when necessary).

10. If you are asked to add another host, click **Yes** and repeat the steps above to add the second ***Host Cluster*** (in this case `rd-mc2`).

When all ***Host Clusters*** are identified and configured, use the following procedure to add the ***Host Group***:

1. Locate the ***Host Mappings*** configuration area in your storage manager software and click **Define Host Group**. This is where you just defined the ***Cluster Hosts*** and now you will define the ***Host Groups***.

2. Enter the new ***Host Group Name*** (`DIVA`).

3. Add the ***Cluster Hosts*** to the new group.

4. Click **OK**.

Next you will add a ***Disk Group*** using the following procedure:

1. Locate the ***Storage Configuration*** area in your storage manager software.

2. Select the ***Total Unconfigured Capacity*** object from the **Computer Objects** list.

3. Select **Disk Group** and then click **Create**.

4. A dialog box will be displayed indicating the total unconfigured capacity - click **Next**.

5. Enter the ***Disk Group Name*** (`DIVA-CL-DISK-GRP`).

6. You must add the physical disks to the ***Disk Group***. Select the automatic detection method option (if available) and click **OK**.
   - Oracle recommends using the storage manager software's *automatically detect physical disks* option if available.
   - If automatic detection is not available, or if the disks are not detected, you must add the disks manually.
   - Automatic detection typically adds all available disk space to the group. If you do not need all of the storage space available for the Oracle Database, you can use the manual method to assign only the amount of space necessary.
7. Click **Next**.
8. Select ***RAID 5*** when presented with the RAID Level and Capacity screen.
9. Select the number of physical disks to be part of the ***Disk Group***.
   - Leave some unused space to be used as spare disks.
   - Typically four disks are selected for the group - this leaves two disks as spares.
10. Click **Finish**.

Next you will create virtual disks. In most disk management software once you complete Step 10, you will be asked to create a virtual disk.

1. If presented with the option to create a virtual disk, click **Yes.** If the option is not given to you, locate where to create a virtual disk in your particular management software and follow the steps below.
2. Assign 50 GB of the free capacity, name the virtual disk `U02`, and choose ***Host Group DIVA*** (under ***Map to Host***), then click **Next**.

   Five partitions are required for the Oracle Database, Logs, MetaDB (if used), Backup, and Cluster Quorum as follows:

   U02, 50 GB, `E:\`
   For the Oracle Database - 8 KB allocation size recommended.

   U03, 10 GB (20 GB maximum), `F:\`
   For the Oracle Archive Logs - 4 KB allocation size recommended.

   MetaDB, Calculated based on complex object size, `G:\`
   For the Metadata Database for Complex Objects. The size is based on the size of complex objects - this is typically larger than several terabytes.

   U04, greater than 130 GB, `H:\`
   For the Oracle Database backup location - 64 KB allocation size recommended.

   Quorum, 100 MB, `Q:\`
   For the Cluster Quorum Witness
3. If you are prompted with an option to create another virtual disk, click **Yes**. If the management software does not automatically ask this question, then repeat Step 1 and Step 2 until all required partitions are created (U02, U03, MetaDB, U04, and Quorum).
4. In your management software confirm that all partitions have been added to the ***Host Group*** and the database.

You will now configure Windows to use the Virtual disks you just created.

Configuring Windows for Virtual Disk Use

Now that you have created the virtual disks you must configure Windows to use them through the Windows Disk Management Console. You can also check for the virtual volumes you created using the Windows Computer Management utility. Use the following procedure to configure the disks for use in Windows:

1. Log into the host computer where you created the virtual disks as a local administrator (if not still logged in).
2. Click **Start** and enter `diskmgmt.msc` in the search area and press **Enter** to start the Disk Management Console.
3. Confirm that all five disks are present in the console. The physical disks will currently show being *Unknown* and *Offline*, but they should all be listed.
4. While leaving the Disk Management Console open, open the Windows Computer Management utility and check that the virtual volumes you created are listed.

   If they are not listed return to the previous section and review your creation of the virtual disks for errors and make any necessary corrections. Contact Oracle Support if you require additional assistance.
5. Once you confirm the presence of the virtual disks, close the Windows Computer Management utility and return to the Disk Management Console.
6. For each Cluster Disk listed in the Disk Management Console that displays an *Unknown* and *Offline* status, right-click in the disk name area (on the left side of the screen) and select **Online** from the resulting menu.

   This will bring the disk to an *Online* state. The disk will still show as *Unknown*, but it will now display *Not Initialized* instead of *Offline*.
7. Right-click one of the (now) *Online* disk names (on the left side of the screen) and click **Initialize Disk** from the resulting context menu.
8. Select each of the disks you just created from the list in the dialog box that is displayed.
9. Click the **MBR (Master Boot Record)** option for disks up to 2 TB. Click the **GPT** option if the disk is larger than 2 TB.
10. Click **OK** to initialize the selected disks.

Now that all disks are initialized, you must create volumes from the unallocated space.

1. Select the new U02 disk and right-click the striped area showing the partition size and *Unallocated*.
2. Select **New Simple Volume** from the resulting menu.
3. When the New Simple Volume Wizard opens, click **Next**.
4. On the second page of the wizard leave the default size and click **Next**.
5. On the third page assign an unused drive letter to the volume and click **Next**.
6. On the fourth page select the ***Format this volume with the following settings*** option.
   - Select **NTFS** for the ***File system***.
   - Use the (pre-filled) ***Recommended allocation unit size*** for MetaDB, U04, and Quorum partitions. For U02 and U03, you will need to change the allocation unit size to 64 K otherwise database performance may be impacted.
   - Enter the ***Volume label*** (for the first disk `U02`, the second disk `U03`, and so on).

- Select the **Perform a quick format** check box.

7. Click **Next** to format the partition with the selected settings.
8. Click **Finish** when the final page appears.
9. Repeat all of these steps for each partition using the appropriate volume label for each partition.

The disk partitions should now be mapped as follows:

Partition and Volume Label: U02, Drive Letter: `E:\`, Minimum Size: 50 GB
For the database file.

Partition and Volume Label: U03, Drive Letter: `F:\`, Minimum Size: 10 GB, Maximum Size 20 GB
For the archive log.

Partition and Volume Label: MetaDB, Drive Letter: `G:\`
For complex objects - the size is calculated based on the size of complex objects - this is typically several terabytes.

Partition and Volume Label: U04, Drive Letter: `H:\`, Minimum Size: 130 GB
For the database backups

Partition and Volume Label: Quorum, Drive Letter: `Q:\`, Minimum Size: 100 MB
For the Quorum Witness

Next you will configure the second node:

1. Log onto the second node as a local administrator.
2. Click **Start** and enter `diskmgmt.msc` in the search area, and then press **Enter** to start the Disk Management Console.
3. Check that the virtual disks are present as you did for the first node.
4. Check the drive letters of the disks and change them to match the first node's drive letters if necessary.
5. Open Windows Explorer and confirm that the drives have been created. Update the drive letters according to the previous partition mappings if necessary (on both nodes).

Next you will configure the operating system.

Configuring the Operating System

Now that all disks have been created and configured, you need to configure the operating system on both Cluster Node Servers. First, you will join both server nodes to a single, common domain.

Joining the Two Server Nodes to a Common Domain

The steps below must be completed on *both Cluster Node Servers*. Use the following procedure to join the two nodes on to a common domain:

1. Log on to the first node as a local administrator.
2. Click **Start**, enter `sysdm.cpl` in the search area, and press **Enter**. This opens the System Properties dialog box.
3. On the System Properties screen, click the **Computer Name** tab and click **Change**.

4. On the Computer Name/Domain Changes screen, check the ***Computer Name*** and correct if necessary.

   Tip: Oracle recommends using a permanent computer name that is less likely to require changing later. The computer names can be changed in the future if absolutely necessary, however it is not recommended and may adversely affect the database and cluster.

   Note: Do not use a server name starting with a dash, number, or any wildcard characters.

5. On the Computer Name/Domain Changes screen, click the **Domain** option and enter a valid domain name in the ***Domain*** field.
6. Click **OK**.
7. When prompted use a dedicated user for confirmation, click **OK** and restart the computer.
8. Repeat all of these steps for the second node.

Next you will add the DIVAClusterAdmin domain account to the local administrator's group.

Adding the DIVAClusterAdmin Domain Account to the Local Administrator's Group

The steps below must be completed on *both Cluster Node Servers*. Use the following procedure to add the DIVAClusterAdmin to the local administrator group:

1. Log onto the first node server as a local administrator.
2. Click **Start**, enter `lusrmgr.msc` in the search area, and press **Enter**. This opens the User Management Console.
3. Click **Groups** from the left navigation tree.
4. Select the ***Local Administrator*** group and open the Properties dialog box.
5. Near the bottom on the left side of the screen click **Add**.
6. Add the ***Cluster Domain*** (for example: `QALAB`) and the DIVAClusterAdmin account to the ***Local Administrator*** group in the form `cluster_domain\cluster_domain_account`.

For example: `QALAB\DIVAClusterAdmin`

7. Click **OK**.
8. Repeat all of these steps for the second node.

Now that the Cluster Administrator has been added to both nodes you must configure the MSCS Cluster.

Configuring the Microsoft Cluster Server Cluster

The following procedures for configuring the MSCS cluster must be completed on both node servers.

Installing the Windows 2012 R2 Standard Server Clustering Feature

Use the following procedure to install the clustering feature on each node:

1. Log on to the first node server as a dedicated cluster domain account user (*DIVAClusterAdmin*).
2. Open the Server Manager Console and using the menu on the top right side of the screen, navigate to **Manage**, and then **Add Roles and Feature Wizard**.
3. When the Add Roles and Features Wizard opens click **Next**.
4. Select the ***Role-based or feature-based installation*** option.
5. Click **Next**.
6. Click ***Select a server from the server pool*** option.
7. In the Server Pool listing area, select the server to use and click **Next** to connect to the local server.
8. Do not select anything on the Server Roles screen - just click **Next**.

   This screen is only for installing Server Roles.
9. On the Features screen select the ***Failover Cluster*** check box.
10. Click **Next**. A dialog box will open asking to add the required features for failover clustering.
11. In the dialog box, select the ***Include management tools (if applicable)*** check box if it's not already selected.
12. Click **Add Features**.
13. You will be returned to the Features screen. Click **Next**.
14. On the Confirmation screen check that the options you selected in the steps above are present.
15. Deselect the ***Restart the destination server automatically if required*** check box if it is selected.
16. Click **Install**.
17. When the installation is complete, click **Close**.
18. Repeat all of these steps for the second node.

Next you will enable the remote registry service on both node servers.

Enabling the Remote Registry Service

Use the following procedure to enable the remote registry service on each node:

1. Log onto the first node server as a dedicated cluster domain account user (*DIVAClusterAdmin*).
2. Click **Start**, enter `services.msc` in the search area, and press **Enter**. This opens the Windows Computer Management utility on the **Services** tab.
3. Double-click the ***Remote Registry Service*** to open the Properties dialog.
4. Select **Enable** to enable the service.
5. Select **Automatic** to start the service automatically in the future.
6. Click **Start** to start the service now.

7. Click **OK**.
8. Repeat all of these steps for the second node.

Next you will register the host names with the DNS Manager.

Registering the Required Host Names to the DNS Manager

You, or your DNS Administrator, must add the entries for the ***Cluster Hostname*** and the ***DIVA Group Name*** to the DNS as follows (respectively):

- `DIVA-CL-MSCS`
- `DIVA-CL-ORC`

Oracle recommends also adding each Cluster Host Server public IP address. Use the following procedure to register the host names and IP addresses in the DNS Manager:

1. Open the Server Manager.
2. Select **Tools**, then **DNS** from the menu on the top right side of the screen.
3. Right-click the ***DNS Zone*** and select **New Host** from the resulting menu.
4. Add the host name (`DIVA-CL-MSCS`) and IP address in the appropriate fields.
5. Select the ***Create associated pointer (PTR) record*** check box (if it is not already).
6. Click **Add Host**.
7. Right-click the ***DNS Zone*** again and select **New Host** from the resulting menu.
8. Add the ***DIVA Oracle Group Name*** (`DIVA-CL-ORC`) and IP address in the appropriate fields.
9. Select the ***Create associated pointer (PTR) record*** check box (if it is not already).
10. Click **Add Host**.

The following steps must be completed on each node server.

1. Log onto the first node server as a local administrator.
2. Open the Windows Network and Sharing Center.
3. Click **Change Adapter Settings** in the left menu.
4. Locate the Network Interface Card (NIC) for the *Private* network connection and right-click the icon.

   The private network is the cluster's heartbeat network only and should not be registered in the DNS.
5. Select **Properties** from the resulting menu.
6. Double-click **Internet Protocol Version 4 (TCP/IPv4)** in the protocols area.
7. In the displayed dialog box, click **Advanced** on the bottom right side of the screen.
8. Select the **DNS** tab on the Advanced TCP/IP dialog.
9. Deselect the ***Register this connection's addresses in DNS*** check box.

   The DIVArchive Prerequisites Package disables the DNS Client Service by default. To conform to Microsoft best practices, you must start the service and set it to automatically start in the future (after the DIVArchive Prerequisite Package is installed).

10. Click **Start**, enter `services.msc` in the search area, and press **Enter**. This opens the Windows Computer Management utility on the **Services** tab.
11. Double-click the **DNS Client** service to open the Properties dialog box.
12. Select **Enable** to enable the service.
13. Select **Automatic** to start the service automatically in the future.
14. Click **Start** to start the service now.
15. Click **OK**.
16. Repeat all of these steps for the second node.

Next you will create the Windows Server 2012 R2 Cluster.

Creating the Windows 2012 R2 Server Cluster

The following procedure should be completed on *one cluster node only*.

1. Log on to the first node server as a dedicated cluster domain account user (*DIVAClusterAdmin*).
2. Select **Start**, **Administrative Tools**, and then **Failover Cluster Management Console**.
3. In the Management area (in the middle of the screen), click **Create a Cluster**. This will start the Create a Cluster Wizard.
4. When the wizard opens click **Next**.
5. Enter the Fully Qualified Domain Name (FQDN) of the first Cluster Node Server in the ***Enter server name*** field and click **Add**.
6. Enter the Fully Qualified Domain Name (FQDN) of the second Cluster Node Server in the ***Enter server name*** field and click **Add**.
7. Click **Next**.
8. When the Validation Warning dialog box is displayed, leave the default (***Yes***) selected to run the validation tests and click **Next**.
9. When the first screen of the Validate Configuration Wizard is displayed click **Next**.

> **Note:** You must be a local administrator on each of the servers that you are validating.

10. On the Testing Options screen, select the ***Run all tests (recommended)*** option. This is the default selection.
11. Click **Next**.
12. On the Confirmation screen, click **Next**.
13. Monitor the validation tests and wait for them to complete. The Summary screen will be displayed when testing is done.
14. If warnings or exceptions are noted in the summary, click **View Report** to see the details.
15. Resolve any issues and rerun the Validate Configuration Wizard if you needed to make any configuration changes.

Note: Disable unused NICs to prevent minor warnings. Some NICs may have IP addresses on the same subnet. If they are not operational, this may not be an issue.

16. Continue rerunning the Validate Configuration Wizard and resolving any errors until the test all complete successfully.
17. When all tests complete successfully, select the ***Create the cluster now using the validated nodes*** check box and click **Finish** to create the Cluster.

    When the Validate Configuration Wizard closes, you will be returned to the Create Cluster Wizard to continue with the configuration.
18. Click **Next** to advance to the Access Point for Administering the Cluster screen.
19. Enter the cluster name (`DIVA-CL-MSCS`) in the ***Cluster Name*** field.
20. Enter the Cluster IP address in the ***Address*** field.
21. Click **Next**.
22. On the Confirmation screen verify that all entered information is correct.
23. Select the ***Add all eligible storage to the cluster*** check box.
24. Click **Next** to create the cluster.
25. When the cluster creation is complete, verify that all configurations were successful by clicking **View Report**.
26. When you have confirmed that the configuration was successful, click **Finish**.

    Next you must configure the Cluster Quorum Storage.
27. In the Failover Cluster Management Console, expand the navigation tree on the left side of the screen so you can see the cluster.
28. Expand the **Storage** menu item and select **Disks**.
29. In the middle of the screen you should be able to see drives `E:`, `F:`, `G:` and `H:`.
30. Select the main cluster item in the navigation tree on the left side of the screen.
31. On the right side of the screen (under Actions) click **More Actions**, and then **Configure Cluster Quorum Settings**. This will start the Cluster Quorum Wizard.
32. Select the ***Select quorum witness*** option.
33. Click **Next**.
34. In the displayed list of Cluster Disks, select the check box for the 100 MB dedicated Quorum Disk. You can identify the Quorum Disk either by the Location (it will show ***Available Storage***), or by expanding the entry using the plus sign and confirming that it is a 100 MB disk.
35. Click **Next**.
36. Verify that all selections are correct on the Confirmation screen and click **Next**.
37. When the configuration is complete, click **View Report** and verify that all configurations were successful.
38. When you have confirmed that the configuration was successful, click **Finish**.

Next you will validate the node configurations.

Validating the Nodes Configuration for MSCS Clustering

The following steps are to be completed on *one cluster node only*.

1. Log on to the first node server as a dedicated cluster domain account user (*DIVAClusterAdmin*).
2. Click **Start**, **Administrative Tools**, and then **Failover Cluster Management Console**.
3. Select the cluster name in the navigation tree on the left side of the screen.
4. Click **Validate Cluster** on the right side of the screen (under Actions).

   You run the Validate Configuration Wizard again to confirm that there are no errors in your configuration.
5. When the first screen of the Validate Configuration Wizard is displayed, click **Next**.
6. On the Testing Options screen, select the ***Run all tests (recommended)*** option. This is the default selection.
7. Click **Next**.
8. Click **Next** on the Confirmation screen.
9. Monitor the validation tests and wait for them to complete. The Summary screen will be displayed when testing is done.
10. If warnings or exceptions are noted in the summary, click **View Report** to see the details.
11. Resolve any errors and rerun the tests until all test complete successfully.
12. Click **Finish** to exit the wizard when all tests complete successfully.

Now that the cluster has been set up and configured you will test the configuration.

Testing the Configuration

Now that the installation and configuration is complete, you need to test everything to verify proper operation before going to live production. First you will do a manual failover test.

Performing a Manual Cluster Failover Test from the Failover Cluster Manager

Use the following procedure to test manual failover configuration and operation:

1. If the cluster that you want to configure is not displayed in the navigation tree on the left side of the Failover Cluster Manager, right-click Failover Cluster Manager, click **Manage a Cluster**, and then select or specify the desired cluster.
2. Expand the cluster in the navigation tree on the left side of the screen.
3. Expand **Roles** and click the role name to test for failover.
4. On the right side of the screen (under Actions) click **Move**, and then **Select Node**.

   The status is displayed under Results in the center of the screen as the service and application move.
5. You can repeat Step 4 to move the service or application to an additional node or back to the original node.

Next you will do a restart failover test on the active node.

Performing a Cluster Failover Test by Restarting the Active Cluster Node

Use the following procedure to perform a restart failover test on the active node:

1. Connect to the DIVArchive Control GUI using the virtual IP address (`DIVA-CL-ORC`) and confirm normal DIVArchive operation.
2. Disconnect the Public Network cable from the Active Cluster Node.
3. Confirm that the services move and start operation on the second Cluster Node.
4. Connect to the DIVArchive Control GUI using the virtual IP address (`DIVA-CL-ORC`) and confirm normal DIVArchive operation.
5. Reconnect the Public Network cable to the Active Cluster Node.

Next you will test moving a configured role to another Cluster Node.

Moving a Configured Role to Another Cluster Node

Use the following procedure to move a configured role to another Cluster Node:

1. Open the Failover Cluster Manager (if not already open).
2. Expand the cluster in the navigation tree on the left side of the screen.
3. Select **Roles**.
4. Right-click the role to failover in the Roles area in the center of the screen.
5. Click **Move**, and then **Select Node** from the resulting menu.
6. In the Move Cluster Role dialog box, select the Cluster Node where you want to move the role.
7. Click **OK**.

   The Role will now move to the selected Cluster Node.
8. Verify the *Owner Node* in the Roles area in the center of the screen - it should now be the selected node.

If all tests have completed successfully, you are ready to place the system into live production.

4

Configuring DIVArchive and Oracle Fail Safe (Performed by Oracle)

Configuring DIVArchive and Oracle Fail Safe is the responsibility of the Oracle Delivery and Installation Team. The customer should have successfully completed the installation and configuration of the cluster before the Oracle team arrives at their location. The following subsections describe what the services the Oracle team will perform when they arrive.

Configuring DIVArchive

The procedures in this section will install and configure DIVArchive and the Oracle Database. These steps must be completed on both Cluster Node Servers.

Installing DIVArchive Prerequisites

Install the DIVArchive Prerequisites on both Cluster Node Servers using the following procedure:

1. Log onto the first node server as a dedicated cluster domain account user (*DIVAClusterAdmin*).
2. Open the User Account Control Settings from the Windows Control Panel.
3. Set the notifications to ***Never notify***. This will reduce the amount of administrator approval request messages during installation.
4. Open a Windows command prompt as an administrator (use ***Run as Administrator***).

   WARNING: In Step 5, confirm that there are no spaces in the directory path. If there are spaces in the directory path, the Cygwin installation will fail after restarting the computer.

5. If not already completed, copy the prerequisite directory, including all subdirectories and files, from the installation DIVArchive DVD to a temporary directory path (with no spaces).

   The directory typically used is `C:\temp\Prerequisites_x.x.x` where x.x.x is the DIVArchive release number.
6. Change to the temporary directory containing the DIVArchive prerequisites installation files.
7. Enter the command `StartSetup.bat` and press **Enter**.

8. When the name and password of the account to run the tasks are requested, enter the *DIVAClusterAdmin* account name and password and press **Enter**. The account name must be in the format *Domain\User* (for example, *QALAB\ClusterAdmin*).
9. Confirm that the prerequisites installation completes successfully. If any errors were identified, resolve the errors and repeat the previous steps again until the installation is successful.
10. Repeat all of these steps for the second node.

Next you will install the Oracle Database.

Installing Oracle Database

There are specific tasks that must be completed on one, or both Cluster Node Servers. Which tasks need to be completed on which (or both) servers are identified within the procedure steps. Install the Oracle Database on *both Cluster Node Servers* using the following procedures:

1. Log on to both node servers as a dedicated cluster domain account user (*DIVAClusterAdmin*).
2. Open a Windows command prompt as an administrator on both node servers (use ***Run as Administrator***).
3. Mount the Oracle ISO file on each node server.
4. Enter `InstallEngine.cmd` at the command prompt and press **Enter**. This will install the Oracle binary files in `C:\app`.

The following steps must be completed on *Node 1 (active node) only*:

1. Enter `InstallDatabase-huge.cmd` at the command prompt and press **Enter**.

> **Note:** Oracle Fail Safe will be used to configure Oracle services on Node 2 later in the procedures.

2. Navigate to `C:\app\oracle\product\11.2.0\dbhome_1\NETWORK\ADMIN\` and edit the `listener.ora` file.
3. Replace `HOST` with the Oracle Cluster Group IP address. This IP address is required during Oracle Fail Safe installation. In our examples `172.20.128.130` (`DIVA-CL_ORC`) are used.

The following steps must be completed on *Node 2 (standby or rebuilding node) only*:

1. Copy the `C:\app\oracle\product\11.2.0\dbhome_1\database\initLIB5.ora` file from Node 1 to Node 2.
2. Navigate to `C:\app\oracle\product\11.2.0\dbhome_1\NETWORK\ADMIN\` and edit the `listener.ora` file.
3. Replace `HOST` with the Oracle Cluster Group IP address. This IP address is required during Oracle Fail Safe installation. In our examples `172.20.128.130` (`DIVA-CL_ORC`) are used.
4. Open the Computer Properties window.
5. Select **Advanced system settings** in the menu on the left side of the screen.
6. Select the **Advanced** tab.
7. Click **Environment Variables** on the bottom right side of the screen.

8. Click **New** under the System Variables area.
9. Repeat steps 4 through 8 (inclusive) to set each of the following environment variables:

   DIVA_ORACLE_HOME
   `C:\app\oracle\product\11.2.0\dbhome_1`

   ORACLE _BASE
   `C:\app\oracle`

   PATH
   `%SystemRoot%\system32;%SystemRoot%;%SystemRoot%\System32\Wbem;%SYSTEMROOT%\System32\WindowsPowerShell\v1.0\;C:\app\oracle\product\11.2.0\client32\bin;C:\app\oracle\product\11.2.0\dbhome_1\bin;C:\Oracle\Ofs41_1\FailSafe\Server`

   You also must include the full path to your disk manufacturer's Disk Management Console software binaries and shared files. For example (assuming this is the basic path used for the manufacture's software installation):

   `C:\Program Files\DISK_MFG\bin`

   `C:\Program Files\DISK_MFG\shared\bin`

   Where DISK_MFG is the disk manufacture's name.

The following procedure must be completed on *both node servers*:

1. Open the Computer Properties window.
2. Select **Advanced system settings** in the menu on the left side of the screen.
3. Select the **Advanced** tab.
4. Click **Environment Variables** on the bottom right side of the screen.
5. Click **New** under the System Variables area.
6. On the New System Variable dialog box, enter `ORACLE_SID` in the ***Variable name*** field, and `LIB5` (must be all uppercase) in the ***Variable value*** field.

The following procedure must be completed on *Node 2 only*:

1. Open the Computer Properties window.
2. Select **Advanced system settings** in the menu on the left side of the screen.
3. Select the **Advanced** tab.
4. Click **Environment Variables** on the bottom right side of the screen.
5. Click **New** under the System Variables area.
6. On the New System Variable dialog box, enter `ORACLE_BASE` in the ***Variable name*** field, and `C:\app\oracle` in the ***Variable value*** field.
7. Repeat steps 4 and 5.
8. On the New System Variable dialog box, enter `DIVA_ORACLE_HOME` in the ***Variable name*** field.
9. On the New System Variable dialog box, enter `C:\app\oracle\product\11.2.0\dbhome_1` in the ***Variable value*** field.
10. Repeat steps 4 and 5.

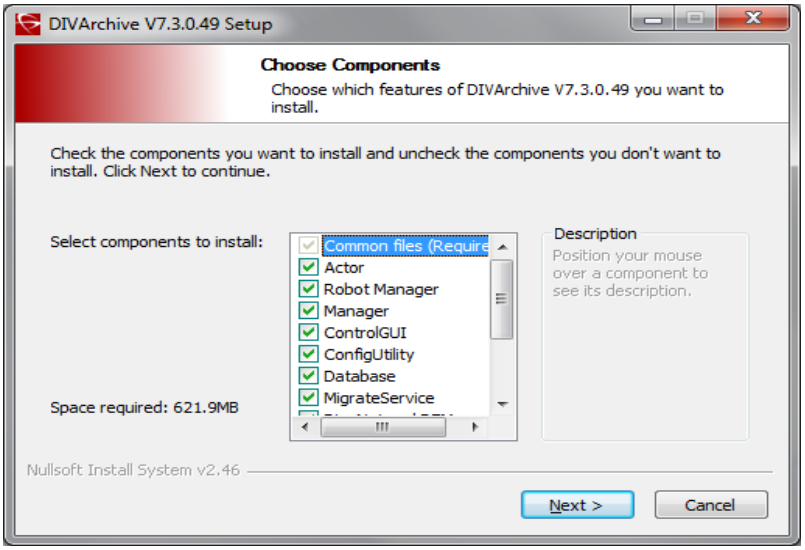
11. On the New System Variable dialog box, enter `PATH` in the ***Variable name*** field, and in the ***Variable value*** field enter the same path you entered for Node 1 (they must match).

Next you will install DIVArchive.

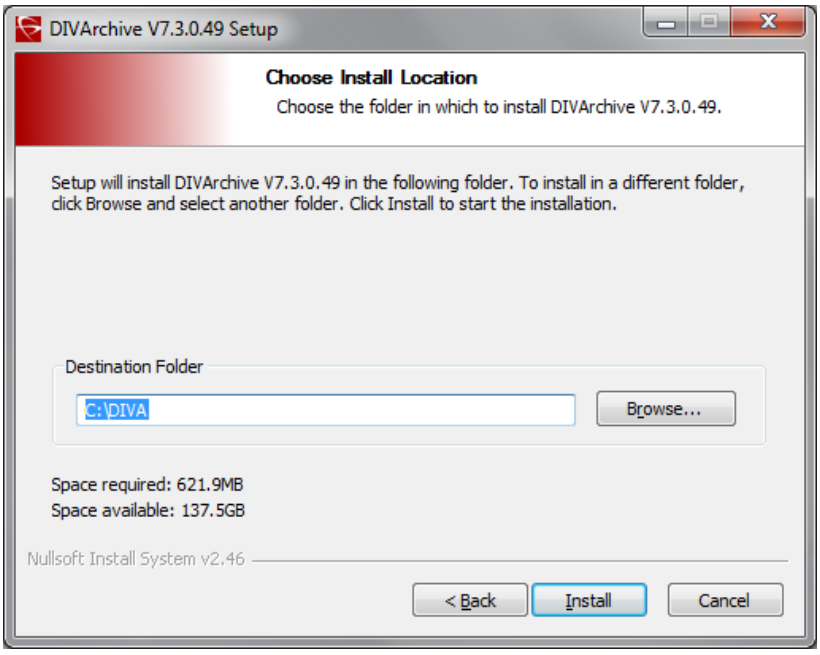
Installing DIVArchive

DIVArchive must be installed on *both Cluster Node Servers*. Use the following procedure to install DIVArchive:

1. Log on to both node servers as a dedicated cluster domain account user (*DIVAClusterAdmin*).
2. Install DIVArchive using the installation program. Refer to the *Oracle DIVArchive Installation and Configuration Guide* and the *Oracle DIVArchive Operations Guide* for additional details if necessary.
3. Start the DIVArchive installation program.
4. When the Choose Components dialog box is displayed, confirm that all check boxes for all components are selected.



5. Click **Next**.
6. Choose the installation location - Oracle recommends the default location (`C:\DIVA`).



7. Click **Install**.
8. When installation is complete, click **Close**.

DIVArchive Guidelines

- The DIVArchive Schema must be created on a shared disk (`E:` and `F:`) from only one node.
- DIVArchive backup must be configured on a shared disk (`H:`).
- The DIVArchive license must be configured with the `172.20.128.130` (`DIVA-CL-ORC`) cluster IP address and applied to one node only.
- In the `manager.conf` file, the `DIVAMANAGER_DBHOST` parameter must be set to the DIVA Cluster Group's IP address (`172.20.128.130` - `DIVA-CL-ORC`).
- The Oracle DIVArchive Actor service must use the domain user account (`qalab\DIVAClusterAdmin`).
- Your desired Manager Services must be installed now.
- All DIVArchive services must be installed with the same exact name and configuration on both cluster nodes.
- Install Oracle Secure Backup services.
- The `SPMservice` uses the Oracle client.
- The file `tnsname.ora` located in the `C:\app\oracle\product\11.1.0\client32\network\admin` directory must be updated to run the `SPMservice` on both nodes.

  The `HOST` parameter should be changed to the IP address of the cluster (`DIVA-CL-ORC`). For example, `HOST = 172.20.138.130`.
- The Node 2 environment variables previously configured are required, otherwise an Oracle DIVArchive Storage Plan Manager (SPM) installation error will occur.

Next you will install and configure Oracle Fail Safe.

Configuring Oracle Fail Safe

The procedures in this section will install and configure Oracle Fail Safe. When the installation is complete, you will verify that it was installed properly.

Installing Oracle Fail Safe

The steps in this section must be completed on *both Cluster Node Servers*.

Fail Safe requires Microsoft's .NET 3.5 SP1 to be installed on the computer before installing Fail Safe. The Fail Safe installation program will notify you if it cannot find .NET 3.5 SP1 on the computer.

Fail Safe also requires that the Cluster Object (`DIVA-CL-MSCS`) must have full control permissions on the Cluster OU before installation proceeds so the cluster can create a Cluster Group Object.

Oracle Fail Safe 4.1 References:

Oracle Fail Safe 4.1 Installation Guide
https://docs.oracle.com/cd/E27731_01/doc.41/e24700.pdf

Oracle 4.1 Fail Safe Tutorial
https://docs.oracle.com/cd/E27731_01/doc.41/e24702.pdf

Oracle Fail Safe 4.1 Concepts and Administrator Guide
https://docs.oracle.com/cd/E27731_01/doc.41/e24699.pdf

1. Log on to both node servers as a dedicated cluster domain account user (*DIVAClusterAdmin*).
2. Install Microsoft .NET 3.5 SP1 on the computer if not already installed. You can install .NET from the Server Manager Console.
3. Use the following procedure to grant full control to the Cluster Object:
    1. Open the Active Directory Users and Computers snap-in from the Windows Server Management console.
    2. Right-click the **DIVAClusterComputers** computer object and select **Properties** to display the Properties dialog box.
    3. Select the **Security** tab, and then select the ***Cluster Object*** (`DIVA-CL-MSCS` in the examples) in the Group or user names area at the top of the screen.
    4. Click the **Advanced** button on the bottom right side of the screen to open the Advanced Security Settings screen.
    5. On the **Permissions** tab, locate the domain user and click the listing one time to highlight the domain user.
    6. Click **Edit** just under the Permission entries area to open the Permission Entry screen.
    7. On the top of the screen, verify that the ***Type*** option is set to **Allow**, and the ***Applies to*** option is set to **This object and all descendent objects**.
    8. Select all of the check boxes in the Permissions area.
    9. Click **OK** on the bottom of the screen to apply the permissions.
4. Extract the Oracle Fail Safe 4.1.0 installation package into a temporary directory.

Oracle Fail Safe 4.1.0 has a known display issue with Windows 2012. Use the following example and website listed below to resolve the issue. MMC is still not 100% stable upon closing the program.

A reference to this issue can be found here: http://www.oracle.com/technetwork/database/windows/sw-comp-41-1946549.html

1. Create a plain text file named `mmc.exe.config` in the `C:\Windows\SysWOW64` folder.
2. Edit the file with a plain text editor (for example, Notepad) and enter the following text:

```
<?xml version="1.0" encoding="utf-8" ?>
 <configuration>
  <appSettings>
    <add key="UseSetWindowPosForTopmostWindows" value="True" />
  </appSettings>
 </configuration>
```

3. Save and close the file.

5. Execute the `temp_folder\install\setup.exe` file to begin installation.
6. On the first screen click **Next**.
7. Select the ***Typical (178MB)*** installation.
8. Click **Next**.
9. Leave the ***Path*** as the pre-filled default and click **Next**.

> **Note:** The installation path must be the same on both nodes.

10. Enter the Domain Username (`qalab\DIVAClusterAdmin`) in the ***Username*** field.
11. Click **Next**.
12. Enter the Domain User's password in the ***Enter Password*** field, and then enter it again to confirm it in the ***Confirm Password*** field.
13. Click **Next**.
14. Review the Summary. If everything is correct click **Install**; otherwise click **Back** and resolve any issues.
15. When installation is complete, click **Exit**.
16. Restart the node.
17. Repeat all of these steps for the second node.

Next you will verify the Fail Safe installation.

Verifying the Oracle Fail Safe Installation

The steps in this section must be completed on *one Cluster Node Server only*. Use the following procedure to verify the Fail Safe installation:

1. Log onto the node server as a dedicated cluster domain account user (*DIVAClusterAdmin*).
2. Launch the Oracle Fail Safe Manager.

3. Connect to the new cluster using the cluster alias (`DIVA-CL-MSCS`) as follows:
    1. Select the cluster alias in the navigation tree on the left side of the screen.

    Note: If the cluster is not shown in the navigation tree you must add it before proceeding - select **Action**, and then **Add Cluster** from the menu.

    2. Select **Connect** from the **Actions** menu on the right side of the screen. This should automatically connect to the cluster.
4. Select the cluster alias in the navigation tree on the left side of the screen.
5. Click **Validate** from the **Actions** menu on the right side of the screen. The cluster validation will begin.
6. You must resolve any warnings or errors before proceeding.
7. When issues are resolved run the validation again.
8. Repeat Step 4 through Step 7 until the validation completes successfully.

Next you will create a Cluster Group and Role dedicated to DIVArchive.

Creating a DIVArchive Dedicated Cluster Group and Role

The procedures in this section must be completed on *one Cluster Node Server only*. In the previous version of Oracle Fail Safe, this process was completed in the Fail Safe Manager. However, with Fail Safe version 4.1, this configuration is accomplished in the Windows Failover Cluster Manager. Use the following procedure to create the DIVArchive dedicated group and role:

1. Log on to the node server as a dedicated cluster domain account user (*DIVAClusterAdmin*).
2. Click **Start**, **Administrative Tools**, and then **Failover Cluster Management**.
3. Expand the cluster in the navigation tree on the left side of the screen, and then click **Roles**.
4. Click **Configure Role** under Roles on the right side of the screen.
5. On the first screen, click **Next**.
6. On the Select Role screen, select ***Generic Service*** in the list located in the middle of the screen, and then click **Next**.
7. On the Select Service screen, select ***DIVArchive Manager*** in the list in the middle of the screen, and then click **Next**.
8. On the Client Access Point screen, enter the Oracle Cluster Group Name (`DIVA-CL-ORC`) in the ***Name*** field.
9. Enter the Oracle Cluster IP address in the ***Address*** field, and then click **Next**.
10. On the Select Storage screen, select the check boxes next to each of the cluster storage disks so all cluster disks are selected, and then click **Next**.
11. On the Replicate Registry Settings screen, click **Next**.
12. Verify the configuration options you selected on the Confirmation screen, and then click **Next**.
13. When the configuration process is complete, click **Finish**.

Once the Cluster Role and Group have been created you may need to add other DIVArchive services (for example, DIVArchive Backup) and other disks that need to be part of the cluster. Use the following procedure to add additional resources to the cluster. For the purpose of this example the DIVArchive Backup Service will be added.

1. In the Failover Cluster Manager expand the cluster (`DIVA-CL-ORC`), and click **Roles** in the navigation tree on the left side of the screen.
2. The Cluster Name (`DIVA-CL-ORC`) will be visible on the right side of the screen with a menu underneath it.
3. Under the Cluster Name, click **Add Resource** and then **Generic Service**.

   Note: If you are adding more storage, you will click **Add Storage** rather than **Add Resource**.

4. Select the **DIVArchive Backup** service (or storage device) from the list in the displayed dialog box, and then click **Next**.
5. Verify that the selected options are correct on the Confirmation screen, and then click **Next**.
6. Click **Finish** when the configuration is complete.

Next you will configure Oracle Fail Safe.

Configuring Oracle Fail Safe Parameters

The procedure in this section must be completed on *one Cluster Node Server only.* Oracle Fail Safe will automatically configure some parameters and others you must manually configure. Use the following procedure to manually configure the necessary parameters:

1. Open the Oracle Fail Safe Manager. The resources will be displayed including the LIB5 Database.
2. Expand the Cluster Object (`DIVA-CL-MSCS`) in the navigation tree on the left side of the screen.
3. Click the **Oracle Resources** menu item.
4. On the right side of the screen, click **Group Actions**, then **Add Resources** to open the Add Resource To Group wizard.
5. On the Group screen, select the group to add the resource to from the list, and then click **Next**.
6. On the Nodes screen, select the nodes from the list, and then click **Next**.
7. On the Virtual Host screen, select the host from the list, and then click **Next**.
8. On the Parameters screen, you will point to the `initLIB5.ora` file for automatic configuration of the Oracle System Parameters (`C:\app\oracle\product\11.2.0\dbhome_1\database\initLIB5.ora`).
9. Click **Next**.
10. Follow through the remaining wizard screens using the default parameters until finished.

    When finished with the wizard your configuration in the Oracle Fail Safe Manager should show all of the resources you added and configured. All other cluster

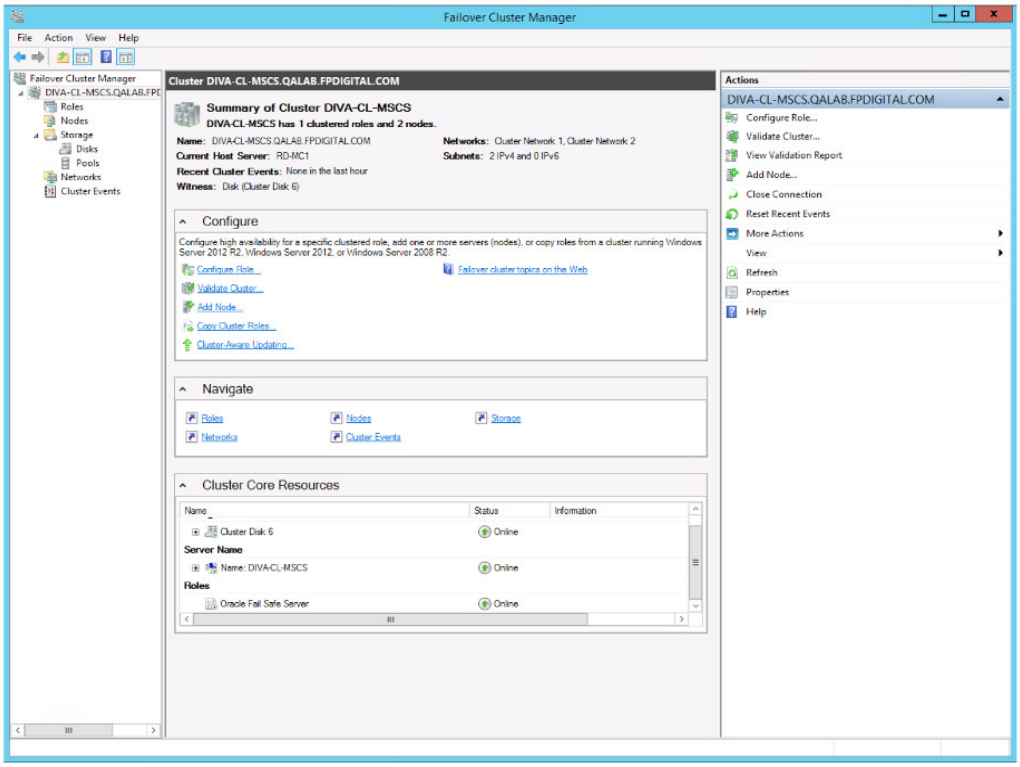
configuration is completed within the Failover Cluster Manager. The Oracle Fail Safe Manager and the Failover Cluster Manager should both show the same resources.

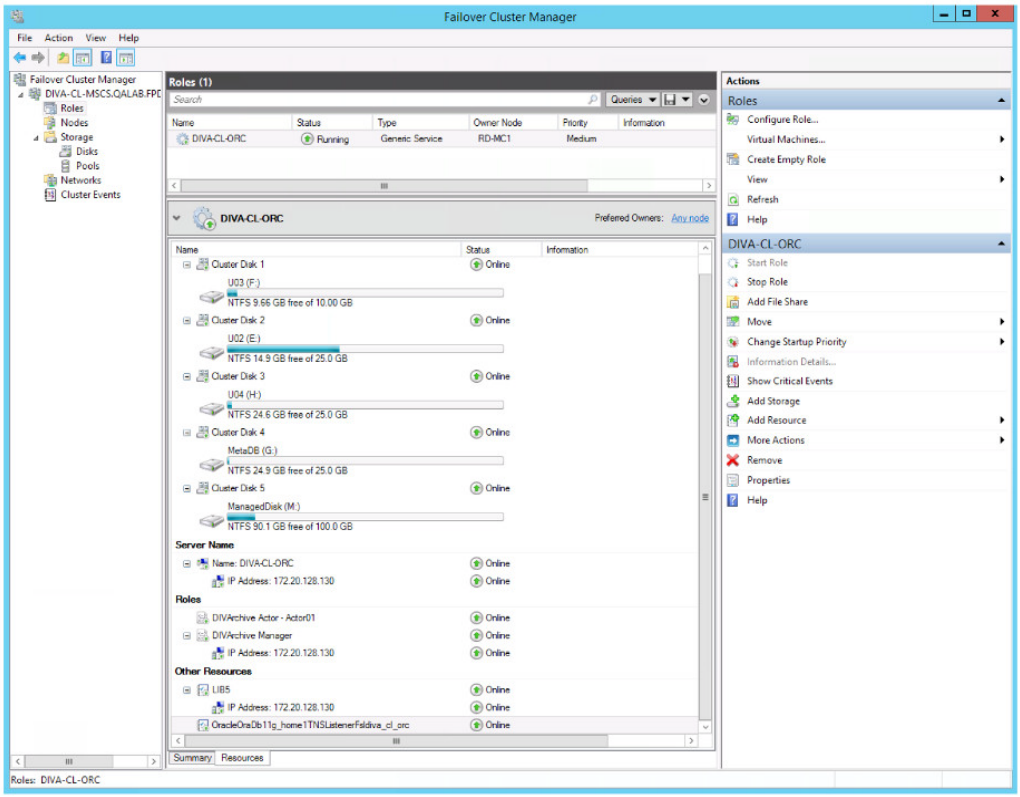
Perform the following procedure in the Failover Cluster Manager:

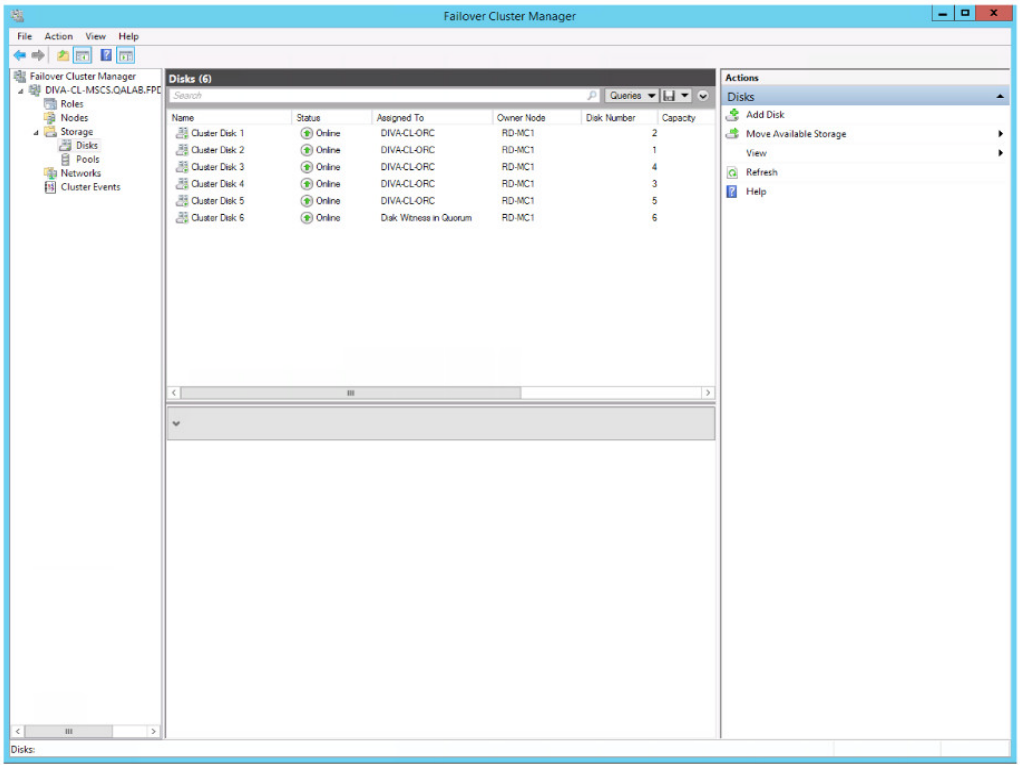
1. In the middle of the Failover Cluster Manager, locate the entry for the ***DIVArchive Manager*** and click it one time to highlight the entry.
2. On the right side of the screen, click **Properties** to open the Properties dialog box for the Oracle DIVArchive Manager.
3. Click the **Dependencies** tab.
4. The last entry in the list displays ***Click here to add a dependency***. Select the field, and then click **Insert**.
5. Select **AND** from the list.
6. Add the following resources to the dependencies:
   - IP address (`172.20.128.130` in our examples)
   - `DIVA-CL-ORC`
   - LIB5
   - Oracle Database TNS Listening Service
   - All Cluster Storage Disks
7. Click **OK**.
8. Repeat Step 14 through Step 20 to add the following dependencies to the *LIB5* service:
   - IP address (`172.20.128.130` in our examples)
   - All Cluster Storage Disks
9. Repeat Step 14 through Step 20 to add the `DIVA-CL-ORC` to the dependencies for the *OracleIORaDB11g Listener* service.

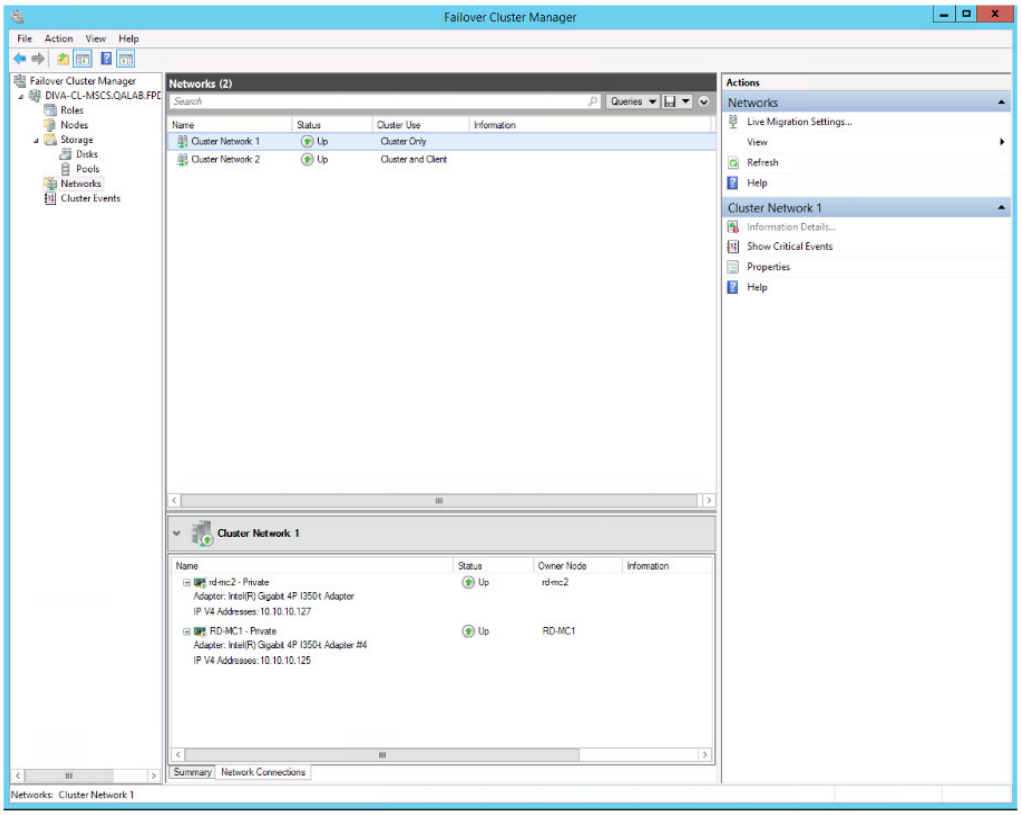
Cluster Configuration Examples

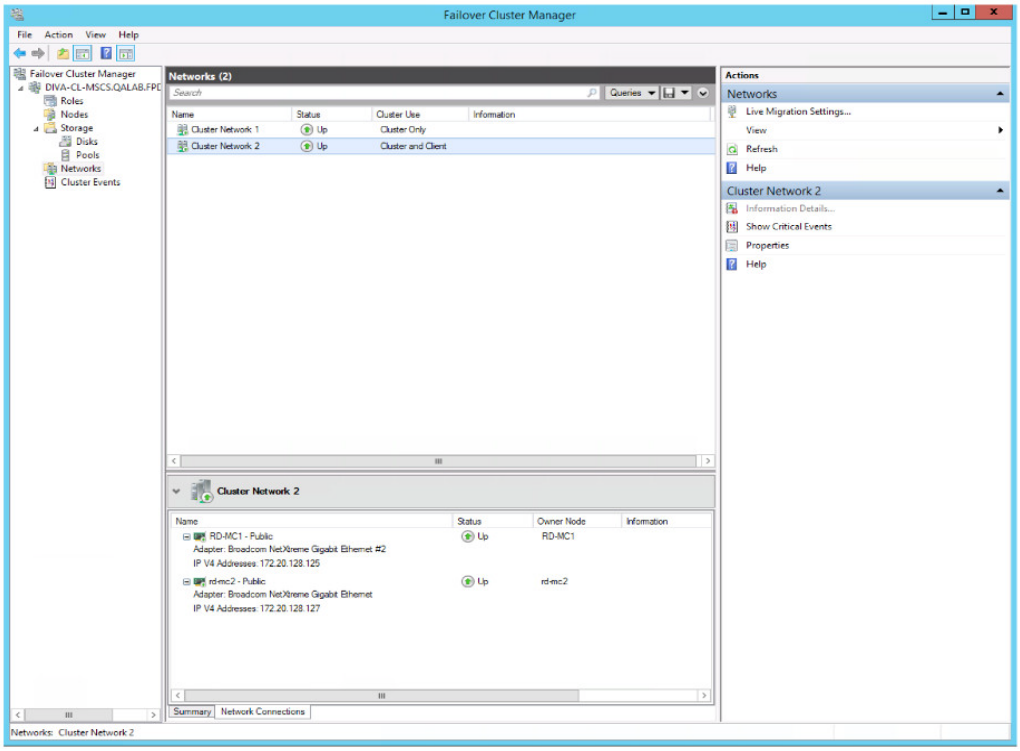
This section only includes sample screen shots of successful cluster configuration and no instructional content.


Failover Cluster Manager
File Action View Help
Failover Cluster Manager
DIVA-CL-MSCS.QALAB.FPDIGITAL.COM
Roles
Nodes
Storage
Disks
Pools
Networks
Cluster Events
Cluster DIVA-CL-MSCS.QALAB.FPDIGITAL.COM
Summary of Cluster DIVA-CL-MSCS
DIVA-CL-MSCS has 1 clustered roles and 2 nodes.
Name: DIVA-CL-MSCS.QALAB.FPDIGITAL.COM
Current Host Server: RD-MC1
Recent Cluster Events: None in the last hour
Witness: Disk (Cluster Disk 6)
Networks: Cluster Network 1, Cluster Network 2
Subnets: 2 IPv4 and 0 IPv6
Configure
Configure high availability for a specific clustered role, add one or more servers (nodes), or copy roles from a cluster running Windows Server 2012 R2, Windows Server 2012, or Windows Server 2008 R2.
Configure Role...
Validate Cluster...
Add Node...
Copy Cluster Roles...
Cluster-Aware Updating...
Failover cluster topics on the Web
Navigate
Roles
Nodes
Storage
Networks
Cluster Events
Cluster Core Resources
Name
Status
Information
Cluster Disk 6
Online
Server Name
Name: DIVA-CL-MSCS
Online
Roles
Oracle Fail Safe Server
Online
Actions
DIVA-CL-MSCS.QALAB.FPDIGITAL.COM
Configure Role...
Validate Cluster...
View Validation Report
Add Node...
Close Connection
Reset Recent Events
More Actions
View
Refresh
Properties
Help


Failover Cluster Manager
File Action View Help
Failover Cluster Manager
DIVA-CL-MSCS.QALAB.FPDIGITAL.COM
Roles
Nodes
Storage
Disks
Pools
Networks
Cluster Events
Roles (1)
Search
Queries
Name
Status
Type
Owner Node
Priority
Information
DIVA-CL-ORC
Running
Generic Service
RD-MC1
Medium
DIVA-CL-ORC
Preferred Owners: Any node
Cluster Disk 1
Online
U03 (F:)
NTFS 9.66 GB free of 10.00 GB
Cluster Disk 2
Online
U02 (E:)
NTFS 14.9 GB free of 25.0 GB
Cluster Disk 3
Online
U04 (H:)
NTFS 24.6 GB free of 25.0 GB
Cluster Disk 4
Online
MetaDB (G:)
NTFS 24.9 GB free of 25.0 GB
Cluster Disk 5
Online
ManagedDisk (M:)
NTFS 90.1 GB free of 100.0 GB
Server Name
Name: DIVA-CL-ORC
Online
IP Address: 172.20.128.130
Online
Roles
DIVArchive Actor - Actor01
Online
DIVArchive Manager
Online
IP Address: 172.20.128.130
Online
Other Resources
UB5
Online
IP Address: 172.20.128.130
Online
OracleOraDb11g_home1TNSListenerFsldiva_cl_orc
Online
Summary
Resources
Roles: DIVA-CL-ORC
Actions
Roles
Configure Role...
Virtual Machines...
Create Empty Role
View
Refresh
Help
DIVA-CL-ORC
Start Role
Stop Role
Add File Share
Move
Change Startup Priority
Information Details...
Show Critical Events
Add Storage
Add Resource
More Actions
Remove
Properties
Help


Failover Cluster Manager
File Action View Help
Failover Cluster Manager
DIVA-CL-MSCS.QALAB.FPD
Roles
Nodes
Storage
Disks
Pools
Networks
Cluster Events
Disks (6)
Search
Queries
Name Status Assigned To Owner Node Disk Number Capacity
Cluster Disk 1 Online DIVA-CL-ORC RD-MC1 2
Cluster Disk 2 Online DIVA-CL-ORC RD-MC1 1
Cluster Disk 3 Online DIVA-CL-ORC RD-MC1 4
Cluster Disk 4 Online DIVA-CL-ORC RD-MC1 3
Cluster Disk 5 Online DIVA-CL-ORC RD-MC1 5
Cluster Disk 6 Online Disk Witness in Quorum RD-MC1 6
Actions
Disks
Add Disk
Move Available Storage
View
Refresh
Help
Disks:


Failover Cluster Manager
File Action View Help
Failover Cluster Manager
DIVA-CL-MSCS.QALAB.FPD
Roles
Nodes
Storage
Disks
Pools
Networks
Cluster Events
Networks (2)
Search
Queries
Name Status Cluster Use Information
Cluster Network 1 Up Cluster Only
Cluster Network 2 Up Cluster and Client
Actions
Networks
Live Migration Settings...
View
Refresh
Help
Cluster Network 1
Information Details...
Show Critical Events
Properties
Help
Cluster Network 1
Name Status Owner Node Information
rd-mc2 - Private Up rd-mc2
Adapter: Intel(R) Gigabit 4P I350t Adapter
IP V4 Addresses: 10.10.10.127
RD-MC1 - Private Up RD-MC1
Adapter: Intel(R) Gigabit 4P I350t Adapter #4
IP V4 Addresses: 10.10.10.125
Summary
Network Connections
Networks: Cluster Network 1


Failover Cluster Manager
File Action View Help
Failover Cluster Manager
DIVA-CL-MSCS.QALAB.FPD
Roles
Nodes
Storage
Disks
Pools
Networks
Cluster Events
Networks (2)
Search
Queries
Name Status Cluster Use Information
Cluster Network 1 Up Cluster Only
Cluster Network 2 Up Cluster and Client
Cluster Network 2
Name Status Owner Node Information
RD-MC1 - Public Up RD-MC1
Adapter: Broadcom NetXtreme Gigabit Ethernet #2
IP V4 Addresses: 172.20.128.125
rd-mc2 - Public Up rd-mc2
Adapter: Broadcom NetXtreme Gigabit Ethernet
IP V4 Addresses: 172.20.128.127
Summary Network Connections
Networks: Cluster Network 2
Actions
Networks
Live Migration Settings...
View
Refresh
Help
Cluster Network 2
Information Details...
Show Critical Events
Properties
Help

5 Maintenance

This chapter describes routine maintenance and procedures necessary during normal operations. If you have an issue not covered here, refer to the appropriate "Related Documents" at the beginning of the book or contact Oracle Support.

Manually Placing a Service Offline

When a service is experiencing issues, Microsoft Cluster detects that it is offline and restarts the service on the active node. You can take the service offline for maintenance to avoid the service restart using the following procedures:

1. Open the Failover Cluster Manager.
2. Expand the Cluster Object (`DIVA-CL-ORC`) in the navigation tree on the left side of the screen.
3. Select **Roles** in the expanded tree on the left side of the screen.
4. Select the failing service in the Roles area in the middle of the screen.
5. Right-click the selected service, and then click **Take Offline** from the resulting menu.
6. The status of the selected service should now show *Offline* in the Roles area in the middle of the screen.

Adding a Network for Client Access

You can configure additional client access using the Failover Cluster Manager. This is useful when another subnet is configured for automation. Each node must have one static IP address on the same subnet as listed in the "Network Requirements". Use the following procedure to configure additional clients:

1. Configure the new interfaces and subnetwork on each node.
2. Click **Start**, **Administrative Tools**, and then **Failover Cluster Management Console**.
3. Expand the Cluster Object (`DIVA-CL-ORC`) in the navigation tree on the left side of the screen.
4. Select **Networks** in the expanded tree on the left side of the screen.
5. Select the new network to use for automation from the ***Networks*** list in the middle of the screen.
6. Click **Properties** under the listed network on the right side of the screen.

7. Enter a new name for the network used for automation in the ***Name*** field.

   Using the name *Automation* for the network makes it easily identifiable.

8. Select the ***Allow clients to connect through this network*** check box.
9. Click **Apply**, and then click **OK**.
10. Right-click **Roles** in the navigation tree on the left side of the screen.
11. Click **Add Resource** from the resulting menu, and then click **Client Access Point** to open the Client Access Point Wizard.
12. On the Client Access Point screen enter an access point name (for example, `DIVA-CL-AUTO`) in the ***Name*** field.
13. Use the check box to select the proper network and associated IP address in the ***Networks*** list.

    You must add the FQDN to the DNS. Refer to the procedures in "Registering the Required Host Names to the DNS Manager" and "Creating the Windows 2012 R2 Server Cluster" if necessary.

14. Click **Next**.
15. Verify the selected configuration on the Confirmation screen, and then click **Next**.
16. When the configuration is complete, verify that all configurations were successful by clicking **View Report**.
17. Click **Finish** after you have confirmed that the configuration was successful.

Rebuilding the Cluster after a Node Hardware Failure

Use this procedure when one node fails. The procedure requires downtime during Fail Safe configuration. To rebuild the cluster, complete the steps in the following sections (in order):

- "Evicting a Failed node"
- "Preparing New Hardware"
- "Joining a New Node Server to a Cluster"
- "Installing DIVArchive"
- "Installing and Configuring Oracle Fail safe"

Evicting a Failed node

Do not perform this procedure as the primary troubleshooting method. Eviction should only be used when:

- Replacing a node with different hardware.
- Reinstalling the operating system.
- Permanently removing a node from a cluster.
- Renaming a node in a cluster.

Use the following procedure to evict a node:

1. Log in to the Active Node server as a dedicated cluster domain account user (*DIVAClusterAdmin*).

2. Click **Start**, **Administrative Tools**, and then **Failover Cluster Management Console**.
3. Expand the Cluster Object (`DIVA-CL-ORC`) in the navigation tree on the left side of the screen.
4. Right-click the failed node in the ***Nodes*** list in the middle of the screen.
5. Click **More Actions f**rom the resulting menu, and then click **Evict**.
6. A confirmation dialog box asks if you are sure you want to evict the node from the cluster - click **Yes** to evict the node (or **No** to leave the node in the cluster).

Preparing New Hardware

When the new hardware is ready, install Windows Server 2012 R2 Standard and all patches to match the Active Node.

> **Note:** Both nodes must be at the same patch level.

Refer to the following procedures (in order):

1. "Configuring the Operating System"
2. "Installing the Windows 2012 R2 Standard Server Clustering Feature"
3. "Enabling the Remote Registry Service"

Joining a New Node Server to a Cluster

Use the following procedure to add a new server to the cluster:

1. Follow the procedure in "Validating the Nodes Configuration for MSCS Clustering."
2. Before connecting the external disk, ensure there are no local partitions using the `E:`, `F:`, or `H:` drives.

   Use the Windows Server Manager to view the disks and assigned drive letters.
3. Follow the procedure in "Replacing a Host Bus Adapter (HBA)."
4. Add the node to the cluster as follows:
   1. Log in to the Active Node server as a dedicated cluster domain account user (*DIVAClusterAdmin*).
   2. Click **Start**, **Administrative Tools**, and then **Failover Cluster Management Console**.
   3. Expand the Cluster Object (`DIVA-CL-ORC`) in the navigation tree on the left side of the screen.
   4. Right-click **Nodes** in the expanded tree on the left side of the screen.
   5. Click **Add Node** in the resulting menu to open the Add Node Wizard.
   6. Click **Next** on the first wizard screen.
   7. Proceed through the wizard to add the new node to the cluster.

Installing DIVArchive

Refer to "Configuring DIVArchive" to complete DIVArchive installation and configuration. Since the DIVArchive Database schema is already in place, do not reinstall the schema on the Active node.

Installing and Configuring Oracle Fail safe

Use the following procedure to install and configure Oracle Fail Safe:

1. To install Oracle Fail Safe, refer to "Installing Oracle Fail Safe."
2. Complete the Oracle Fail Safe configuration as follows:
    1. Confirm the Fail Safe service was created during the installation.
    2. Confirm the LIB5 service instance was created during the installation.

    Note: The `initLIB5.ora` file must be replicated on both nodes.

    3. Confirm the Oracle TNS Listener service was created during installation.
    4. Restart the new node and run the tests described in "Testing the Configuration."

Replacing a Host Bus Adapter (HBA)

The SAS HBA interfaces external disks dedicated for the database and quorum partitions. Use the following procedure if a SAS HBA fails, or if a node fails and you must rebuild the node using new hardware:

1. Replace the failed SAS HBA in the server following the manufacture's installation and configuration instructions and recommendations.
2. Launch the Storage Manager software on the Active Node.
3. Locate the Host Mapping area of your Storage Manager.
4. Expand the **DIVA Host Group** and select the host that contains the new HBA.
5. Right-click the host and click **Manage Host Port Identifiers** (your menu item listing may be different) from the resulting menu.
6. Select the failed port in the list, and then click **Replace**.
7. On the following screen, click the **Replace by creating a new host port identifier** option under ***Choose a method for replacing the host port identifier***.
8. Enter the new host port identifier in the ***New host port identifier (16 characters required)*** field, and then click **Replace**.
9. When the replacement process completes, you should see the Cluster Volumes from the Active Node.

Configuring Windows Firewall with Advanced Security

Microsoft Best Practices recommend enabling the Windows Firewall, however it is not mandatory for DIVArchive. To use the Windows Firewall, use the `DIVACloud_Firewall_Exceptions_2012.ps1` PowerShell script to enable DIVArchive exceptions through the firewall. Use the following procedure to create and run the Firewall Exceptions script in PowerShell:

1. Open Notepad to create a text file.
2. Copy the following script content and paste it into the file you just created.

> **Note:** You may (or may not) need to make adjustments to the line breaks, and so on due to formatting.

```
### Oracle DIVACloud Firewall Exception list. This will enable the Windows
Firewall for all profiles and exclude common DIVA ports. ###
### WINDOWS 2012 Only BELOW ###
Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled True
New-NetFirewallRule -DisplayName "DIVACloud SSH" -Description "Oracle DIVACloud
(SSH Remote Access)" -Direction Inbound -LocalPort 22 -Protocol TCP -Action
Allow
New-NetFirewallRule -DisplayName "DIVACloud DIVADirector HTTP" -Description
"Oracle DIVACloud (DIVADirector HTTP)" -Direction Inbound -LocalPort 80
-Protocol TCP -Action Allow
New-NetFirewallRule -DisplayName "DIVACloud Remote Administration" -Description
"Oracle DIVACloud (Remote Administration)" -Direction Inbound -LocalPort 135
-Protocol TCP -Action Allow
New-NetFirewallRule -DisplayName "DIVACloud DIVADirector HTTPS" -Description
"Oracle DIVACloud (DIVADirector HTTPS)" -Direction Inbound -LocalPort 443
-Protocol TCP -Action Allow
New-NetFirewallRule -DisplayName "DIVACloud CIFS" -Description "Oracle
DIVACloud (Req. Collection Script)" -Direction Inbound -LocalPort 445
-Protocol TCP -Action Allow
New-NetFirewallRule -DisplayName "DIVACloud RSYNC" -Description "Oracle
DIVACloud (RSYNC)" -Direction Inbound -LocalPort 873 -Protocol TCP -Action
Allow
New-NetFirewallRule -DisplayName "DIVACloud Oracle TNS Listener" -Description
"Oracle DIVACloud (Oracle Database - Transparent Network Substrate)"
-Direction Inbound -LocalPort 1521 -Protocol TCP -Action Allow
New-NetFirewallRule -DisplayName "DIVACloud VACP" -Description "Oracle
DIVACloud (Automation (Harris) Control)" -Direction Inbound -LocalPort 5010
-Protocol TCP -Action Allow
New-NetFirewallRule -DisplayName "DIVACloud DataExpedition" -Description
"Oracle DIVACloud (ExpeDat - Accelerated File Transfer)" -Direction Inbound
-LocalPort 8080 -Protocol UDP -Action Allow
New-NetFirewallRule -DisplayName "DIVACloud DIVArchive Robot Manager"
-Description "Oracle DIVACloud (DIVArchive Robot Manager)" -Direction Inbound
-LocalPort 8500 -Protocol TCP -Action Allow
New-NetFirewallRule -DisplayName "DIVACloud DIVArchive Manager" -Description
"Oracle DIVACloud (DIVA API Listener / Systems Monitoring)" -Direction Inbound
-LocalPort 9000 -Protocol TCP -Action Allow
New-NetFirewallRule -DisplayName "DIVACloud DIVArchive Webservices"
-Description "Oracle DIVACloud (DIVA Systems Monitoring)" -Direction Inbound
-LocalPort 9443,9763 -Protocol TCP -Action Allow
New-NetFirewallRule -DisplayName "DIVACloud DIVArchive AccessGateway"
-Description "Oracle DIVACloud (DIVA Communications)" -Direction Inbound
-LocalPort 9500 -Protocol TCP -Action Allow
New-NetFirewallRule -DisplayName "DIVACloud DIVArchive Actor" -Description
"Oracle DIVACloud (DIVActor)" -Direction Inbound -LocalPort 9900 -Protocol TCP
-Action Allow
New-NetFirewallRule -DisplayName "DIVACloud SNMP" -Description "Oracle
DIVACloud (Systems Monitoring)" -Direction Inbound -LocalPort 161 -Protocol
UDP -Action Allow
New-NetFirewallRule -DisplayName "DIVACloud RDP" -Description "Oracle DIVACloud
(Remote Desktop Protocol)" -Direction Inbound -LocalPort 3389 -Protocol TCP
-Action Allow
```

```
New-NetFirewallRule -DisplayName "DIVACloud NRPE" -Description "Oracle
DIVACloud (Icinga Systems Monitoring - Nagios NRPE)" -Direction Inbound
-LocalPort 5666 -Protocol TCP -Action Allow
New-NetFirewallRule -DisplayName "DIVACloud NSClient++" -Description "Oracle
DIVACloud (NSClient++ Monitoring w/Icinga)" -Direction Inbound -LocalPort
12489 -Protocol TCP -Action Allow
New-NetFirewallRule -DisplayName "DIVACloud ICMP" -Description "Oracle
DIVACloud (Packet Internet Groper ICMPv4)" -Protocol ICMPv4 -IcmpType 8
-Enabled True -Profile Any -Action Allow
### OPTIONAL LOGRHYTHM ONLY### New-NetFirewallRule -DisplayName "DIVACloud
LogRhythm TCP" -Description "Oracle DIVACloud (LogRhythm Log Collection TCP)"
-Direction Inbound -LocalPort 135, 137, 138, 139, 445, 49153 -Protocol TCP
-Action Allow
### OPTIONAL LOGRHYTHM ONLY### New-NetFirewallRule -DisplayName "DIVACloud
LogRhythm UDP" -Description "Oracle DIVACloud (LogRhythm Log Collection UDP)"
-Direction Inbound -LocalPort 514 -Protocol UDP -Action Allow
### OPTIONAL NEVERFAIL ONLY### New-NetFirewallRule -Program "C:\Program
Files\Neverfail\R2\bin\nfgui.exe" -Action Allow -Profile Domain, Private,
Public -DisplayName "DIVACloud Neverfail" -Description "Oracle DIVACloud
(Neverfail)" -Direction Inbound
New-NetFirewallRule -Program "%SystemDrive%\Oracle\Ofs41_
1\FailSafe\Server\FsSurrogate.exe" -Action Allow -Profile Domain, Private,
Public -DisplayName "DIVACloud Oracle Fail Safe" -Description "Oracle DIVACloud
(Fail Safe)" -Direction Inbound
### WINDOWS 2012 Only ABOVE ###
```

3. Save the file with the file name `DIVACloud_Firewall_Exceptions_2012.ps1`.
4. Open a Windows PowerShell command prompt. You may have to open the PowerShell as a Windows Administrator to successfully execute the script.
5. Navigate to the folder where the script is located.
6. Execute the script by entering `DIVACloud_Firewall_Exceptions_2012.ps1` at the command prompt.
7. All necessary exceptions required for DIVArchive operations should now be included in the Windows Firewall configuration.

If you require additional information or assistance refer to the Microsoft TechNet document named *Windows Firewall with Advanced Security* located at http://technet.microsoft.com/en-us/library/hh831365.aspx.

Cluster-Aware Updating

Cluster-Aware updating automates the Microsoft software updating process on clustered servers while maintaining availability. It is a Microsoft best practice to perform regular Windows updates, however it is not mandatory for DIVArchive. Refer to the following Microsoft TechNet documentation for details on Cluster-Aware updating:

- *Microsoft Cluster-Aware Updating*

  http://technet.microsoft.com/en-us/library/hh831694.aspx

- *Microsoft Cluster-Aware Updating Best Practice*

  http://technet.microsoft.com/library/jj134234#BKMK_FW

Glossary

Domain Name Service (DNS)

A system for naming computers and network services that is organized into a hierarchy of domains. DNS services resolve IP addresses to host names for proper network routing.

Fully Qualified Domain Name (FQDN)

The complete domain name for a specific computer, or host, on the internet. The FQDN consists of two parts: the host name and the domain name. For example, `rd-mc1-qalab.oracle.com`.

Multipath I/O (MPIO)

Microsoft Multipath I/O (MPIO) is a Microsoft-provided framework that allows storage providers to develop multipath solutions that contain the hardware-specific information needed to optimize connectivity with their storage arrays.

Network Interface Card (NIC) Teaming

The process of combining multiple network cards together for performance and redundancy reasons. Microsoft refers to this as *NIC Teaming*, however other vendors may refer to this as bonding, balancing, or aggregation. The process is the same regardless of which solution is used or what it is called.

Organizational Unit (OU)

An organizational unit (OU) is a subdivision within an Active Directory into which you can place users, groups, computers, and other organizational units. You can create organizational units to mirror your organization's functional or business structure. Each domain can implement its own organizational unit hierarchy. If your organization contains several domains, you can create organizational unit structures in each domain that are independent of the structures in the other domains.

Serial Attached SCSI (SAS)

A point-to-point serial protocol that moves data to and from computer storage devices such as hard drives and tape drives.