

# Enterprise Manager Cloud Control 12c: Configuring Microsoft Windows Server Failover Clustering

ORACLE WHITE PAPER | DECEMBER 2015





## Table of Contents

Introduction	1
Enterprise Manager Cloud Control Architecture Overview	1
Pre-requisites	2
Building a Highly Available deployment	3
Enable Failover Clustering Feature	3
Create Failover Cluster and Role	5
Install Oracle Enterprise Manager Cloud Control	10
Oracle Apache Target Reconfiguration	10
Verification of Windows Service	12
Configure standby Windows node	12
Step1- Windows Registry Configuration	12
Step2- Windows Service Registration	13
OMS service	13
Agent Service	13
Configure Enterprise Manager Services for Failover	14
Failover Generic Script	15
Defining policies and dependencies	15
Failover Generic Script	15
OMS Generic Service	17
Agent Generic Service	18
Verify Switchover	20
Deploy Physical Agents to monitor Windows node	21
Fetching Agent image from software library	21
Local physical agent deployment	22
Verify Failover	23
Troubleshooting	24
Conclusion	24
Appendix	24
Failover Script	24



## Introduction

Oracle Enterprise Manager is Oracle's integrated enterprise IT management product line, which provides the industry's first complete cloud lifecycle management solution. With Enterprise Manager Cloud Control, Oracle offers a unique approach to systems management, enabling organizations to deploy a single tool with a tightly integrated set of features to manage all tiers in the datacenter as well as the entire lifecycle of applications. Through the use of Enterprise Manager Cloud Control, organizations are able to lower the cost of managing applications while at the same time dramatically improving quality of service.

With Oracle Enterprise Manager's integrated application-to-disk management, organizations get intuitive and robust system health monitoring and management of all hardware and software components in their infrastructure. Hence Enterprise Manager Cloud Control is regarded as key systems management tool and is a crucial application in any data center. Ensuring continuous operation of this mission-critical application is very vital for overall data center monitoring and management. As such, High Availability has become a key requirement for Enterprise Manager Cloud Control deployments. High Availability solution of Enterprise Manager Cloud Control aims to guard against failure at each component of the system, thus avoiding any service disruptions. High Availability solution of Enterprise Manager Cloud Control aims to provide reliability, recoverability, timely failure detection and continuous operations.

This white paper details how to install Enterprise Manager Cloud Control in a highly available Cold Failover Cluster (Active/Passive) solution on Microsoft Windows Server Failover Clustering platform so that the planned / unplanned downtime can be minimized. The configuration details outlined in this whitepaper can be used by customers deploying Enterprise Manager Cloud Control on Windows platform. The solution is characterized by key benefits of automatic failure detection and fast recoverability.

## Enterprise Manager Cloud Control Architecture Overview

Enterprise Manager Cloud Control provides a central point for monitoring and administration in the data center. To achieve this, it collects information from a variety of distributed components and consolidates it in a centralized repository. The key Enterprise Manager components must all work in concert for the system to operate correctly. The components involved in collecting, processing and presenting this information to users are as follows:



**Targets** - A Target, or more specifically, a Target instance, can be defined as any entity that can be monitored within an enterprise. This entity can be an application running on a server, the server itself, the network, or any of its constituent parts.

**Oracle Management Agent (Agent)** – The Oracle Management Agent is a software component that is installed on every monitored host in the enterprise. Agents collect information from the Targets running on the host and send this information to the Oracle Management Service (OMS). Agents also perform operations against the Targets on behalf of Enterprise Manager users. There are many different types of Targets that Enterprise Manager can manage. Examples include Host, VM Guest, Database, Listener, ASM, WebLogic Server, Service Bus and Fusion Applications components

**Oracle Management Service (OMS)** – The Oracle Management Service is the central component in Enterprise Manager with which all other components interact. The OMS is deployed on a WebLogic Server and must be available in order for the Agents to upload data and for administrators to access the Enterprise Manager cloud control console.

**Oracle Management Repository (Repository)** – The Oracle Management Repository is used as a persistent data store. Examples of the information stored in the repository include user information, job definitions, monitoring and alerting settings and all configuration and monitoring data related to Targets. The OMS cannot run if the repository is unavailable.

**Software Library** – The Software Library is a filesystem repository that stores software entities such as software patches, virtual appliance images, reference gold images, application software, and their associated directive scripts. The Software Library is accessed by the OMS and is used extensively by the Enterprise Manager framework for features such as self-update and Agent deployment.

**Console** – The Console is a browser-based web application that is the main user interface for Enterprise Manager. This console allows the administrator to monitor, manage and report on the Enterprise Manager Targets that have been setup.

**Enterprise Manager Command Line Interface (EM CLI)**–EM CLI allows users to access Cloud Control functionality either interactively from a command line, or as part of a script. This allows Cloud Control operations to be integrated with complex business processes without user interaction.

## Pre-requisites

The highly available Cold Failover Cluster (Active/Passive) solution outlined in this whitepaper assumes that the customer already has an investment in Windows infrastructure required for Microsoft Windows Server Failover Clustering deployment.

### Platform Requirements

Platform	Supported Version
Microsoft Windows	Windows Server 2012 R2

### Supported Software Versions

Oracle Enterprise Manager Repository Database	Oracle Enterprise Edition 11.2.0.4
---	------------------------------------

Microsoft Windows Server Failover Clustering configuration for Enterprise Manager Cloud Control requires a minimum of 2 Windows 2012 R2 cluster nodes and a single shared storage cluster disk that is shared between the nodes. Designation of quorum disk is not a pre-requisite for cluster configuration.

Ensure that the Windows domain administrative account is used for logging into the cluster nodes since configuration of Failover Clustering feature, creation of cluster and cluster resource /roles must be done using the Windows domain administrative account.

## Building a Highly Available deployment

The high level steps for building the configuration are as follows

- ➔ **Enable Failover Clustering Feature**
- ➔ **Create Failover Cluster and Role**
- ➔ **Install Oracle Enterprise Manager Cloud Control**
- ➔ **Configure standby Windows node**
- ➔ **Configure Enterprise Manager Services for Failover**
- ➔ **Verify Switchover**
- ➔ **Deploy Physical Agents to monitor Windows node**
- ➔ **Verify Failover**
- ➔ **Troubleshooting**

### Enable Failover Clustering Feature

If the Failover Clustering had not been enabled prior on the Windows cluster nodes, follow this section to enable the feature using Server Manager Windows application. Enable the Failover Clustering feature on both the Windows cluster nodes.

In the Server Manager, select Local Server and scroll down to the ROLES AND FEATURES section. From the TASKS drop-down list, select Add Roles and Features (Figure1) which will start the configuration wizard.

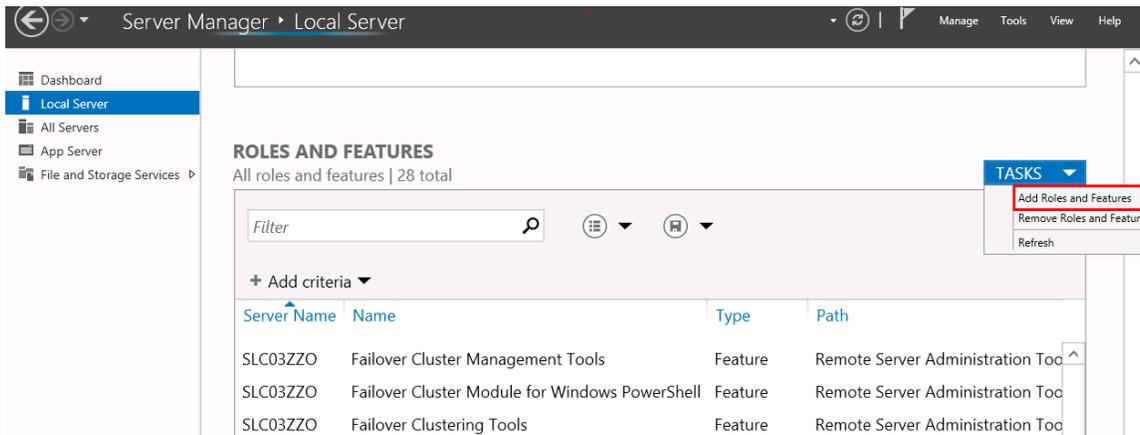


Figure 1. Add Roles and Features option in Server Manager

On Select installation type page select the Role-based or feature-based installation option and click next. On the Select destination server page, select the server on which the Failover Clustering feature needs to be installed. On the Select features page, scroll and select Failover Clustering. After the installation completes, the wizard will end and Failover Clustering will be displayed in the ROLES AND FEATURES section of Server Manager. This process must be completed on both nodes.

Validate the failover clustering configuration using the Validate a Configuration wizard in Failover Cluster Manager. This wizard checks the hardware and software configuration of all the cluster nodes and reports on any issues that might prevent the cluster from being created. If the validation tests succeed (Figure 2), proceed to the next step of creating the cluster.

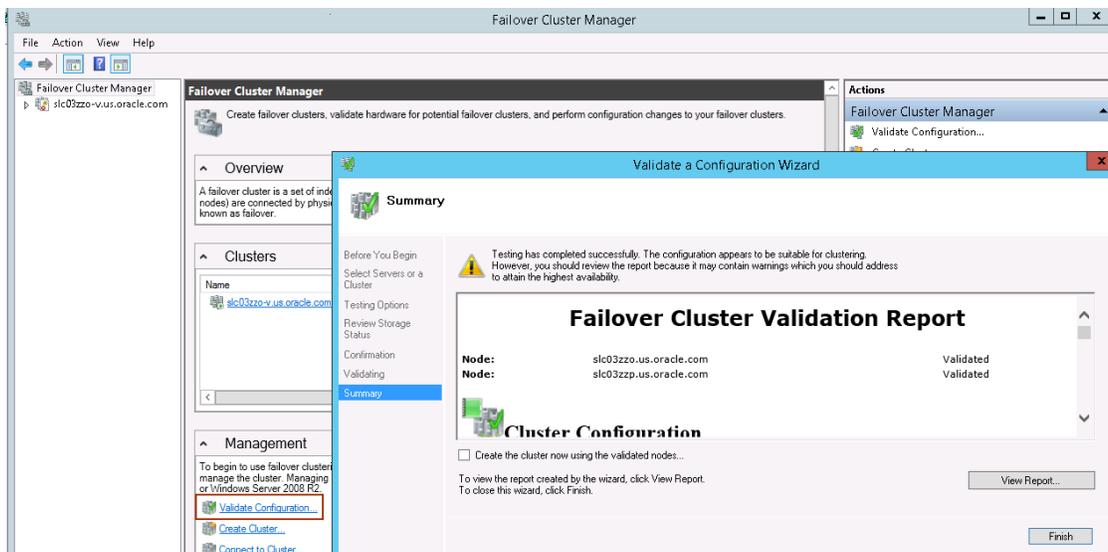


Figure 2. Failover Cluster Validation report

## Create Failover Cluster and Role

The Microsoft Windows Server Failover Clustering configuration for Enterprise Manager Cloud control requires configuration of two virtual IPs which is used for cluster management and access point management.

Configure two VIPs and register their names in DNS server with valid IP address. The IPs must be in the same subnet and available for use.

- Cluster VIP
- Cluster resource / role VIP

Create the cluster from the Actions menu in the Failover Cluster Manager pane.

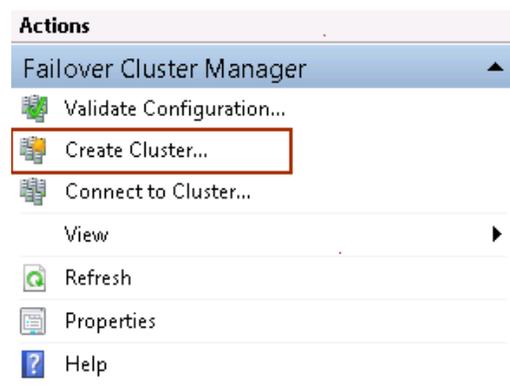


Figure 3. Failover Cluster Manager Action Menu

In the Create Cluster wizard - Access Point for Administering the Cluster page, enter the cluster VIP name. During cluster creation, this name is registered as the cluster object in Active Directory. Then enter the IP address that needs to be assigned to the cluster. The cluster name and IP address will be the virtual name registered in DNS and will be used to connect and manage the cluster itself. This information is usually different than the name and IP address that will be used by clients to connect to clustered applications.

Select the cluster and click on Configure Role in Actions menu. The Enterprise Manager will be configured to use this role during installation. Select the "Other Server" role type and configure the Client Access Point by giving the Cluster resource VIP and its corresponding IP address.

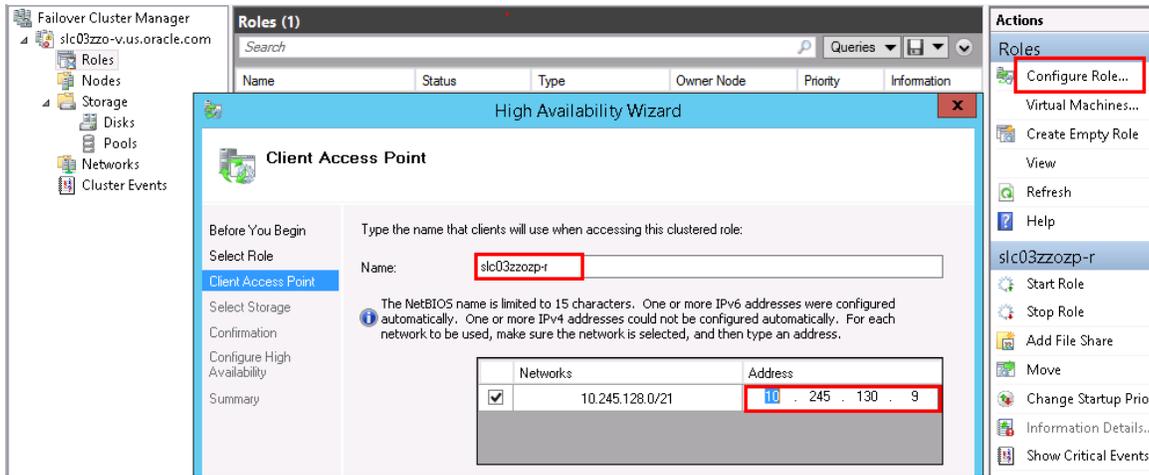


Figure 4. Cluster role configuration wizard

Also, in the cluster role configuration wizard, associate a shared storage to be a cluster disk .If one does not see the shared storage, ensure storage is allocated to the nodes by running diskpart (Figure 5).

```
C:\>diskpart

Microsoft DiskPart version 6.3.9600

Copyright (C) 1999-2013 Microsoft Corporation.
On computer: SLC03ZZO

DISKPART> list disk

   Disk ###  Status              Size               Free               Dyn  Gpt
   -----  -
   Disk 0    Online              230 GB              9 MB
   Disk 1    Reserved            200 GB              0 B

DISKPART> _
```

Figure 5. Diskpart Utility

To enable the cluster resource /role to become online, in the Active Directory check the security tab and give the cluster name full control to the resource Active Directory object.

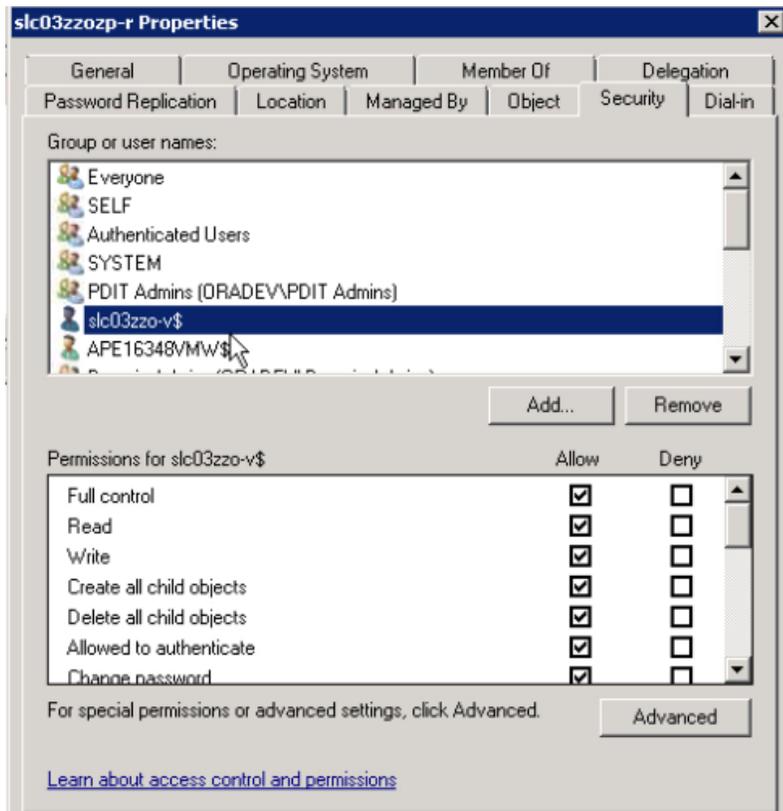


Figure 6. Active Directory security Configuration

If the cluster resource /role is still not Online /Running, select the role, go to properties > Failover tab > Changed the value of "Maximum failures in the specified period:" from 1 to 2( Figure 7).

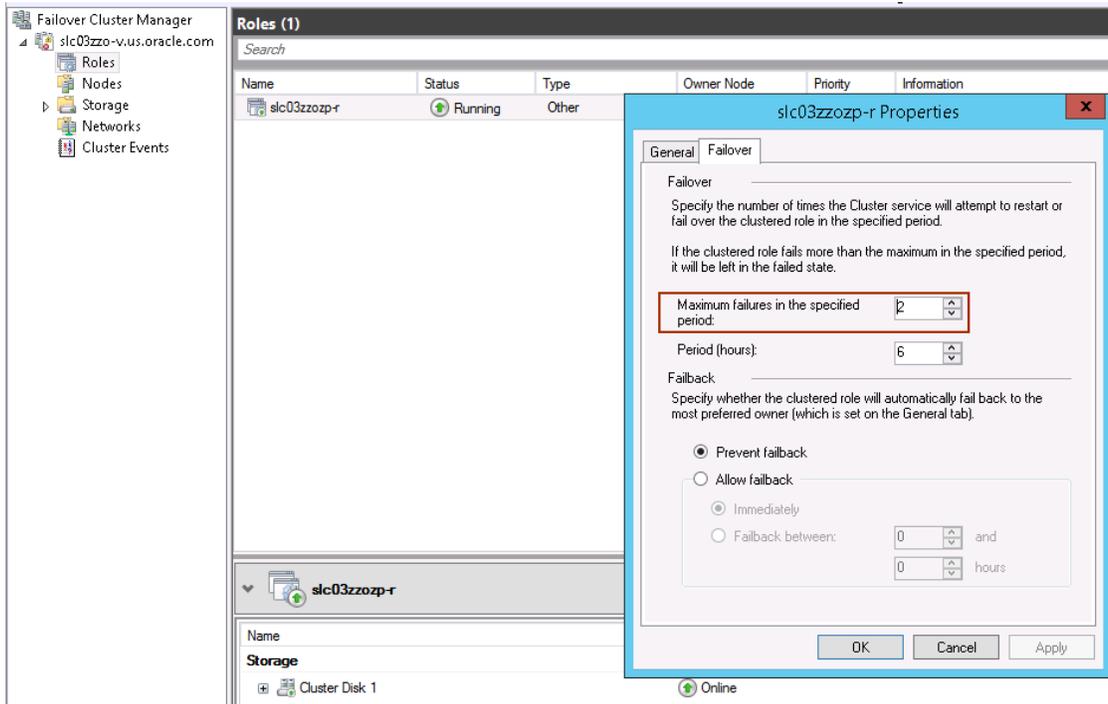


Figure 7. Failover configuration Cluster Resource Role properties

Make sure that the IPv6 is enabled in Network Connections even if not using IPv6 .In the NIC properties uncheck "register this connection with dns"(Figure 8). This should stop all the ipv6 errors.

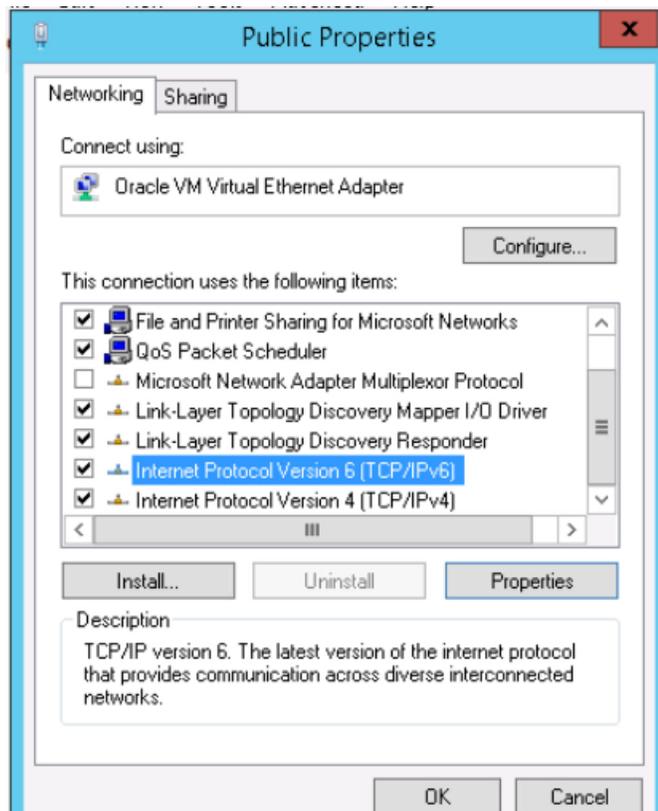


Figure 8. Network Configurations

At the end of the configuration, expect to see the below set of cluster components (Figure 9).

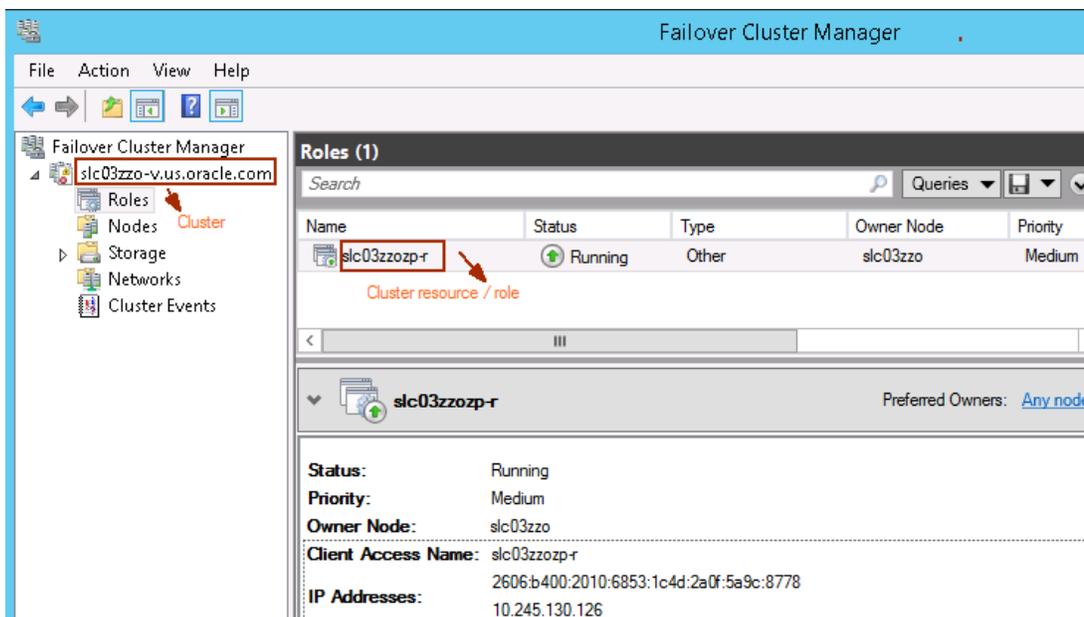


Figure 9. Cluster components in Failover Cluster Manager

## Install Oracle Enterprise Manager Cloud Control

Install the Enterprise Manager Repository on local drive in one of the Windows cluster node. The recommended best practice to configure the Enterprise Manager Repository for failover on Windows platform is to use Fail Safe. Fail Safe is the Oracle recommended solution for configuring high availability of Oracle databases on Microsoft Windows Failover cluster platform. The Enterprise Manager Repository configuration using Fail Safe is beyond the scope of this whitepaper. Refer to Oracle Fail Safe documentation library for configuration details.

Install the Oracle Enterprise Manager on the shared storage cluster disk using the alias host name on one of the Windows cluster nodes. Alias hostname is the cluster resource/role name. Invoke the Enterprise Manager installer either by using the `ORACLE_HOSTNAME=<ALIAS_HOST_NAME>` parameter or by specifying the alias host name in the Host Name field in the OUI installation. For example, include the following parameter on the `setup.exe` command line:

**`ORACLE_HOSTNAME=slc03zzzp-r.us.oracle.com`**

Once the installation is complete, verify in the logs that all host information references the alias host name and no entries to the actual physical host name reside in the installation log.

Login to the Enterprise Manager Cloud Control Console and verify that all targets except Oracle Apache target are successfully monitored by the alias hostname agent and the host is referred to by alias hostname. Oracle Apache target's host references the physical hostname rather than alias hostname though the installation happened by passing alias hostname as the `ORACLE_HOSTNAME` parameter. Follow the below section "**Oracle Apache Target Reconfiguration**" to change the referenced host name from physical hostname to alias hostname.

### Oracle Apache Target Reconfiguration

The Oracle Apache target, aka OHS1, is configured using a different setting than the environment variables. Note that the Host, Virtual Hosts and Host name in the target home page (Figure 10) uses the physical host/node and not the alias hostname (cluster resource name).

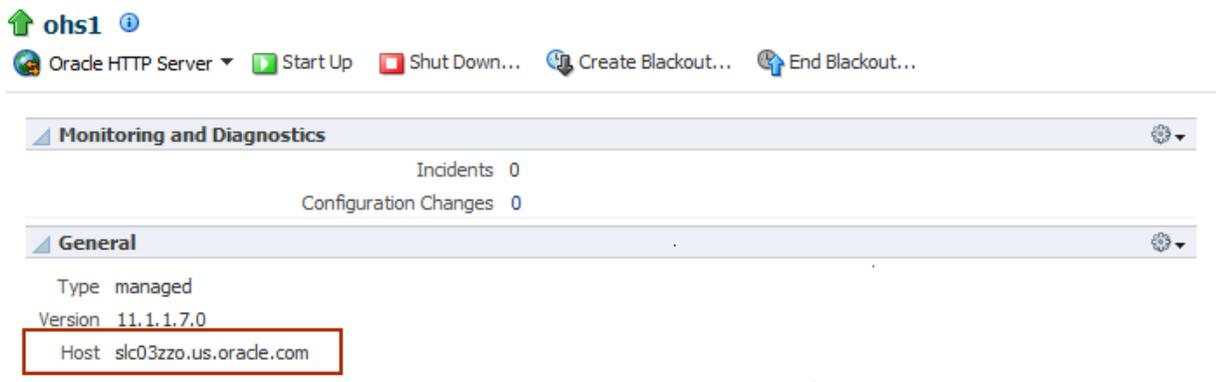


Figure 10. Oracle Apache target with physical hostname reference

Make sure to configure the host parameter to reference alias hostname, otherwise the target status shows DOWN following the failover of the current installation node to the standby Windows node.

To reconfigure, stop the OMS Windows service running on the node. Make a backup copy of the `$OMS_HOME\user_projects\domains\GCDDomain\opmn\topology.xml`. Edit the `topology.xml` file and replace the

physical hostname reference with alias hostname in host parameter. Save the file with the new changes. Start the OMS Windows service.

Follow the steps to re-add the Oracle Apache target. Login the Enterprise Manager Cloud Control console and go to OHS target home page. Remove the target following the option: **Oracle HTTP Server - Target Setup - Remove Target**. Navigate to the Oracle WebLogic Domain Target's home page and click the option- Refresh WebLogic Domain. The job will locate missing targets within the domain and re-add them, including the Oracle Apache target (ie OHS1) with the new host name(Figure 11).

**GCDomain** slc03zzozp-r.us.oracle.

WebLogic Domain Start Up Shut Down... Page Refreshed Jul 27, 2015 12:43:54 AM MDT

**Refresh WebLogic Domain: Assign Agents** Add Targets Cancel

New Targets Found 1  
 Modified Targets Found 5  
 Targets Assigned To Local Agent 12

**Targets And Agents Assignments**

Target Name	Target Type	Host	Configured Agent
EMGC_GCDomain	Oracle Fusion Middleware Farm	slc03zzozp-r.us.oracle.com	slc03zzozp-r.us.oracle.c
GCDomain	Oracle WebLogic Domain	slc03zzozp-r.us.oracle.com	slc03zzozp-r.us.oracle.c
EMGC_ADMINSERVER	Oracle WebLogic Server	slc03zzozp-r.us.oracle.com	slc03zzozp-r.us.oracle.c
FMW Welcome Page Application(11.1.0.0.0)	Application Deployment	slc03zzozp-r.us.oracle.com	slc03zzozp-r.us.oracle.c
EMGC_OMS1	Oracle WebLogic Server	slc03zzozp-r.us.oracle.com	slc03zzozp-r.us.oracle.c
emgc	Application Deployment	slc03zzozp-r.us.oracle.com	[Inherited From Parent]
empbs	Application Deployment	slc03zzozp-r.us.oracle.com	slc03zzozp-r.us.oracle.c
OCMRepeater	Application Deployment	slc03zzozp-r.us.oracle.com	slc03zzozp-r.us.oracle.c
oracle.security.apm(11.1.1.3.0)	Oracle Authorization Policy Manager	slc03zzozp-r.us.oracle.com	[Inherited From Parent]
mds-owsm	Metadata Repository	slc03zzozp-r.us.oracle.com	slc03zzozp-r.us.oracle.c
mds-sysman_mds	Metadata Repository	slc03zzozp-r.us.oracle.com	slc03zzozp-r.us.oracle.c
ohs1	Oracle HTTP Server	slc03zzozp-r.us.oracle.com	slc03zzozp-r.us.oracle.c

Figure 11. Apache OHS target with alias hostname referred

Navigate to the Oracle Apache target home page and confirm the presence of alias hostname(Figure 12).

Oracle HTTP Server Start Up Shut Down... Create Blackout...

**Monitoring and Diagnostics**

Incidents 0  
 Configuration Changes 0

**General**

Type managed  
 Version 11.1.1.7.0  
 Host slc03zzozp-r.us.oracle.com

Figure 12. Oracle Apache target with alias hostname reference

## Verification of Windows Service

After the Enterprise Manager installation is done on a single Windows node, verify that all the required Windows services are in the Running status (Figure 13)

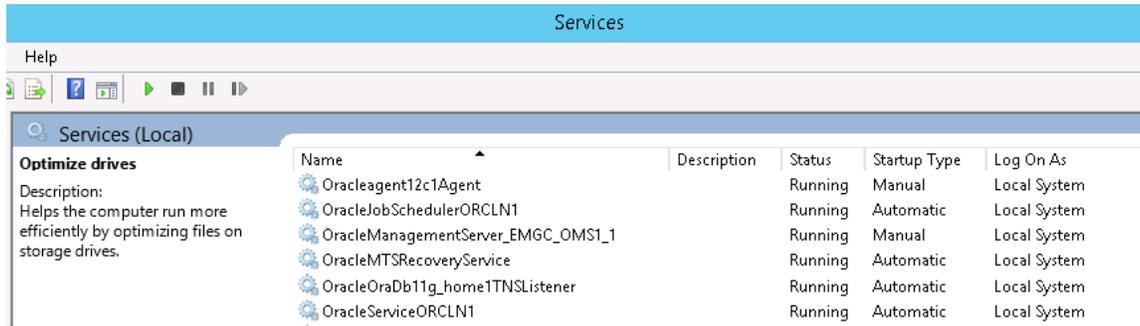


Figure 13. Windows Service with Enterprise Manager installation

## Configure standby Windows node

Configure the services on the second standby Windows node so that the services can start up on this node after failover. The high level flow of standby Windows node configuration involves

1. Configuring the Windows Registry
2. Registering the Windows services
  - a. OMS Service
  - b. Agent Service

### Step1- Windows Registry Configuration

Export and Import the Registry key from the first Windows node where the Enterprise Manager Cloud Control was installed to the standby Windows node.

Click on Start, Run. Type in Regedit and click OK.

In the registry, navigate to the following folder: Computer - HKEY\_LOCAL\_MACHINE - Software - oracle - SYSMAN. Click on Export and choose to save the registry file(.reg) in a location that can be located easily.

Transfer the .reg file to the standby Windows node via FTP or another secure file transfer method.

Log onto each of the standby Windows node and double click on the registry (.reg) file. Windows will prompt for confirmation to import the registry key (Figure 14). Click on YES and import.

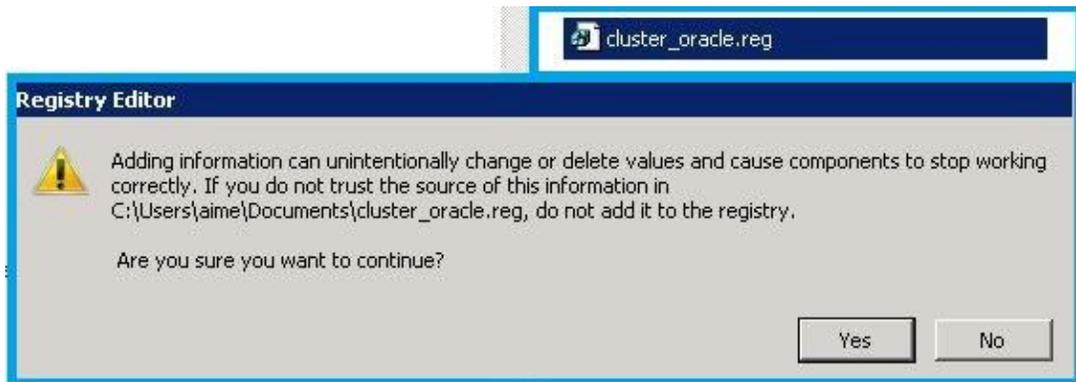


Figure 14. Windows Prompt for Registry Import Confirmation

This will import the Oracle registry key in and overwrite any existing Oracle registry key on the standby Windows node.

### Step2- Windows Service Registration

Windows services need to exist on the standby Windows node to support the applications in event of failure on primary Windows node where installation had happened. Follow the steps to configure the OMS and Agent Windows services on standby Windows node.

#### OMS service

- Creation of OMS Windows service at standby node does not require the existence of corresponding registry entries that was created in prior step. Hence open the registry in standby host and rename the OMS Key ( HKEY\_LOCAL\_MACHINE -> SOFTWARE -> oracle -> SYSMAN -> OracleManagementService\_EMGC\_OMS ) to "%\_old".
- Transfer the shared installation storage of Enterprise Manager to the standby host by using Failover Cluster Management UI and clicking "Move the service or application to another node". At this point, only the shared cluster disk moves to the standby node.
- Access the Enterprise Manager Installation folder from standby node and navigate to \$OMS\_HOME\bin folder and execute the command "**emctl create service -oms\_svc\_name <service\_name>**" where <service\_name> is the exact OMS Service name as shown in the primary Windows node service registry.
- Ensure that the above step creates the registry entries for the OMS service.

#### Agent Service

- Open the registry in standby Windows node and rename the Agent Key(HKEY\_LOCAL\_MACHINE->SOFTWARE->oracle->SYSMAN->Oracleagent12c2Agent) to "%\_old".
- Navigate to the agent home and execute the command "**\$ORACLE\_HOME\bin\nmesrvops create <servicename> \$ORACLE\_HOME/bin/nmesrv.exe auto**" where <servicename> is the exact Agent Service name as shown in the primary Windows node service registry(Figure 15).

```
H:\app\oracle\oem\agent\core\12.1.0.4.0\bin>nmesrvops create Oracleagent12c2Agent
t H:/app/oracle/oem/agent/core/12.1.0.4.0/bin/nmesrv.exe auto
Service "Oracleagent12c2Agent" create SUCCESS
```

Figure 15. Agent Service Creation

- Regedit entries are not created by default for Agent Service. Hence undo the renaming done in prior step and check to ensure they have the same values as present in primary Windows node (Figure 16).

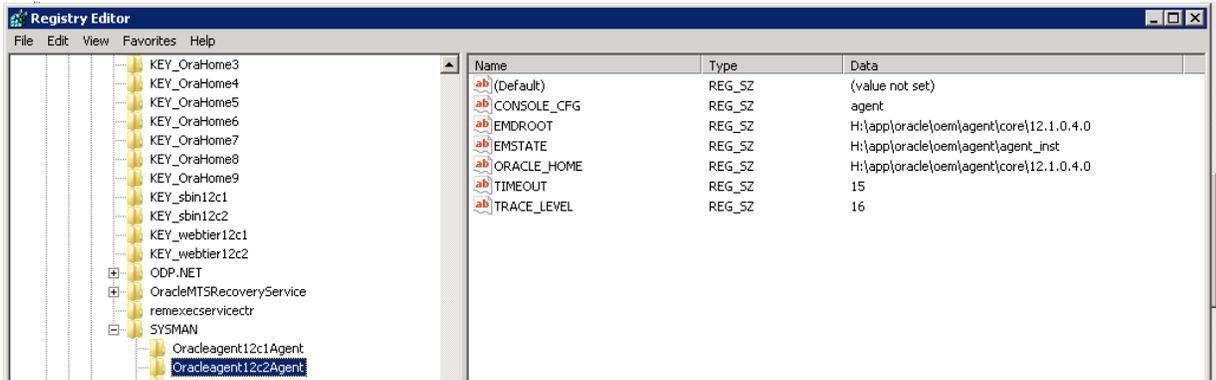


Figure 16. Agent Registry Entry Values

## Configure Enterprise Manager Services for Failover

In the Windows 2012 R2 server, OS level clustering offers management options for Failover cluster creating software connect that provides information to Oracle Services to failover and run on a standby Windows node. This is achieved by grouping the services as resources within the Cluster resource/role as shown in Figure 17.

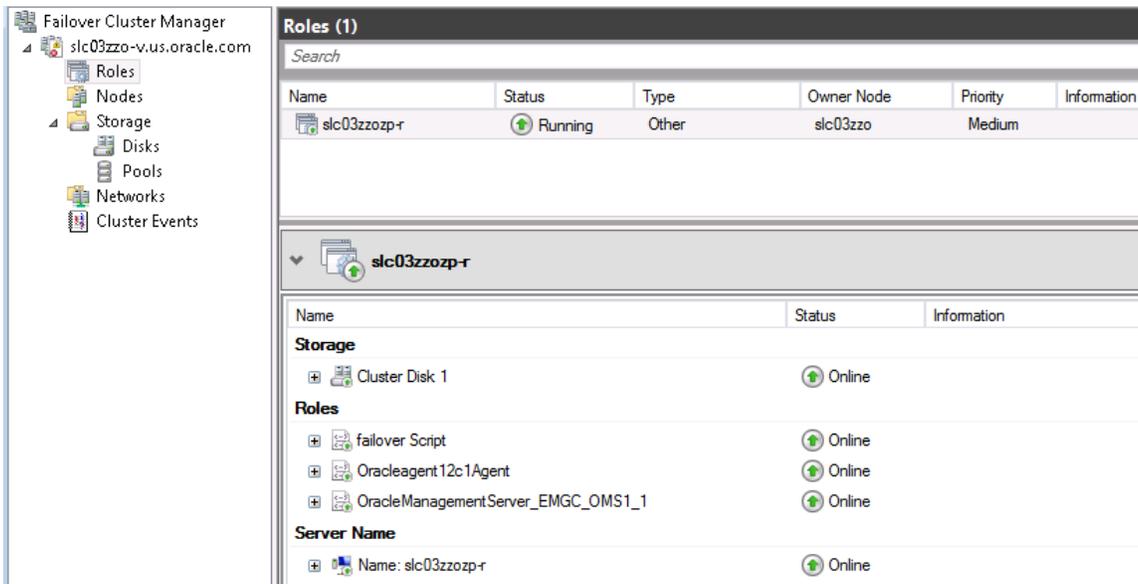


Figure 17. Grouping of Services with cluster resource /role

Open Failover Cluster Management UI, navigate to the cluster resource (eg slc03z0p-r here ) and add the following resources for failover

- Failover Generic Script
- OMS Windows service as generic service(OracleManagementServer\_EMGC\_OMS1\_1)

- c) Agent Windows service as generic service(Oracleagent12c1Agent)

The details of Failover Generic Script resource configuration are outlined below

### Failover Generic Script

This generic script ensures that all OMS processes are shutdown when cluster resource goes offline in a specific node. This script also has a generic placeholder function called CleanProcess() where administrators can embed custom code to clean all the OMS processes and any other java process prior to starting a cluster resource online in a specific node by providing a unique search pattern identifying the processes to be cleaned. The sample code shipped cleans the OMS processes in 12.1.0.4 version only and the administrator should diligently make sure the search pattern provided in the sample confirms to the intended OMS processes in their environment.

This script ensure that no redundant process are left behind in the specific node when cluster resource goes offline in a planned switchover and hence future failback works with no issues. It also ensures that the cluster resource starts /becomes online on a clean Windows node following abrupt un-planned failovers.

Important points to note:

- a) During the script deployment, ensure the emctl executable path is changed within the script in the variable # EmctlCmdPath to point to the installation folder.
- b) Ensure the call to CleanProcess() function within Online( ) is uncommented if the script is intended to be used for handling abrupt failover scenarios also. Find out the OMS processes in the environment and ensure that search pattern in the code retrieves these OMS processes only. If there are any custom processes retrieved in the search pattern used, narrow down the search filter appropriately to accommodate only the intended processes to be cleaned.

The script code is given in Appendix.

### Defining policies and dependencies

After adding the three cluster resources, define the policies and dependency setting for each of the resource. Dependency settings for resources let the cluster know the order of services to be started or stopped. This is essential to ensure that the cluster fails over correctly in a specific sequential order on any Windows node.

Sequential Starting Order: Failover Generic script -> OMS Service -> Agent Service

Sequential Stopping Order: Agent Service -> OMS Service -> Failover Generic script

Right-click the resource and go to Properties and set the following for each resource

### Failover Generic Script

Click on the Dependencies Tab and add the **IP Address** and **Cluster Disk** as the dependency. This will require the drives to be online and the IP Address to be reachable before the script attempts to run. The drives are part of the Failover service group, so they will now start before the failover generic script attempts to run ensuring that binaries are available to run the emctl command.

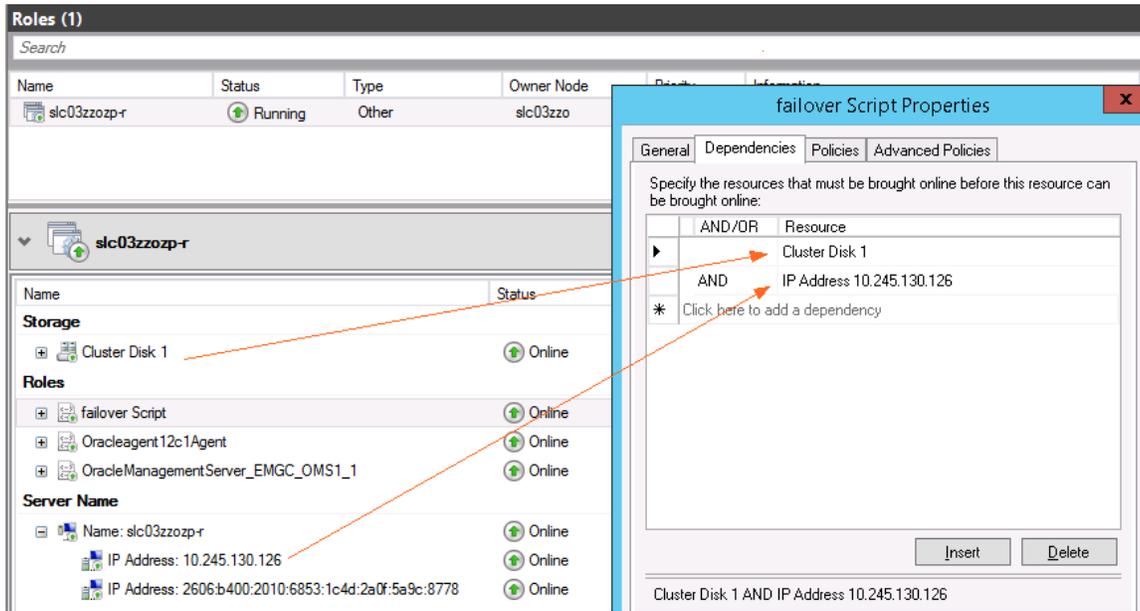


Figure 18. Dependencies for Failover Generic Script

Set the policies as below:

- If resource fails, do not restart.
- Increase Pending Timeout to 20.

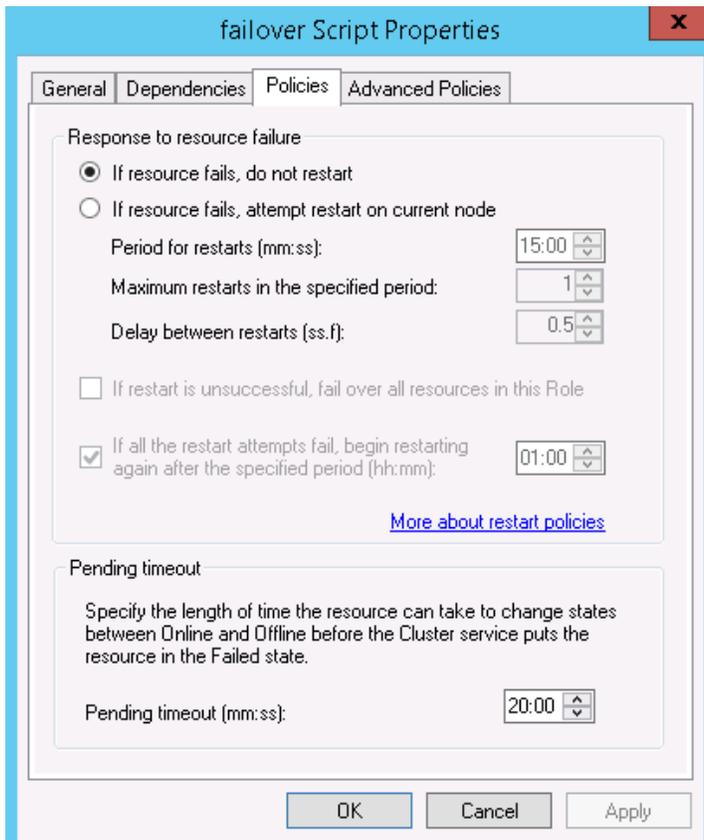


Figure 19. Failover Script Properties

### OMS Generic Service

Click on the Dependencies Tab and add the **IP Address** ,**Cluster Disk** and **Failover Generic Script** as the dependency. This will require the drives to be online, the IP Address to be reachable and the Failover Generic Script to be run before the OMS service starts up.

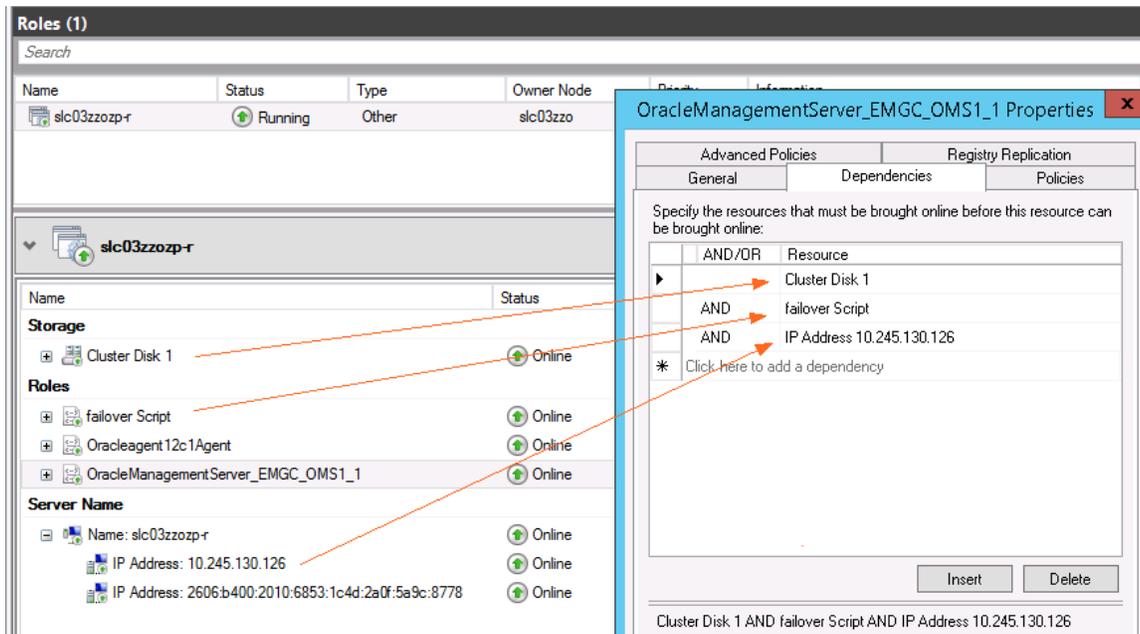


Figure 20. Dependencies for OMS Service

Set the policies as below:

- If resource fails, do not restart.
- Increase Pending Timeout to 20.

### Agent Generic Service

Click on the Dependencies Tab and add **the IP Address ,Cluster Disk ,Failover Generic Script and OMS service** as the dependency. This will require the drives to be online , the IP Address to be reachable , Failover Generic Script to be run and OMS service to be run before the Agent Service starts up.

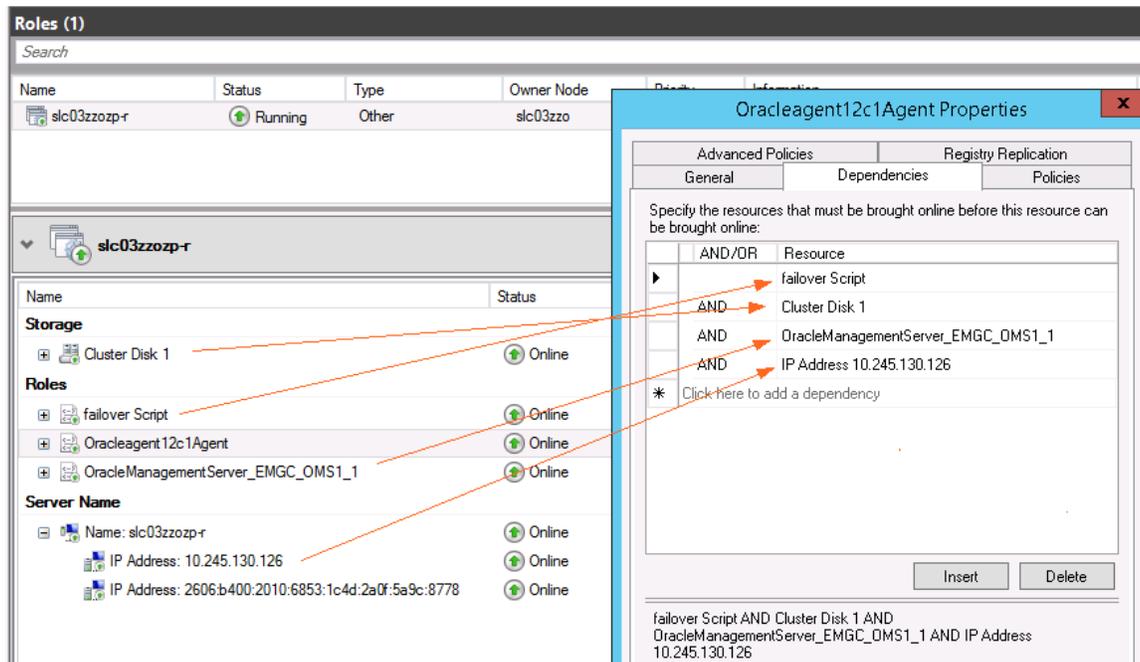


Figure 21. Dependencies for Agent Service

Set the policies as below:

- If resource fails, do not restart.
- Increase Pending Timeout to 3.

## Verify Switchover

After the cluster resource configurations are done following the prior steps, verify the functionality by switching over from primary Windows node to standby Windows node following the below steps.

Open the Failover Cluster Manager UI and navigate to the cluster resource (eg.sl c030zop-r ) and perform switchover by moving the cluster resource to the available standby Windows node.

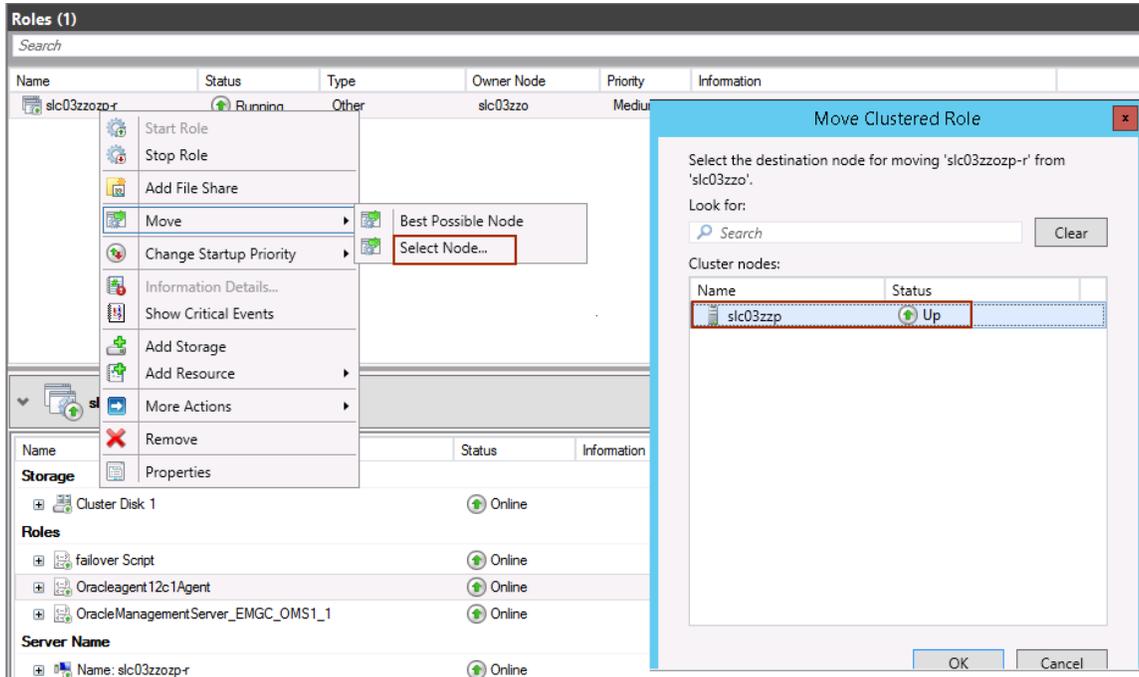


Figure 22. Switchover the Cluster Resource from one node to another

The resources becomes offline in one node based on dependency order, the storage disk fails over to other node and all the resources become online in other node based on dependency order(Figure 23).

Roles (1)				
Search				
Name	Status	Type	Owner Node	Priority
 slc03zzozp-r	 Pending	Other	slc03zzo	Medium

slc03zzozp-r		
Name	Status	Information
<b>Storage</b>		
 Cluster Disk 1	 Online	
<b>Roles</b>		
 failover Script	 Online	
 Oracleagent12c1Agent	 Offline	
 OracleManagementServer_EMGC_OMS1_1	 Offline Pendi_	
<b>Server Name</b>		
 Name: slc03zzozp-r	 Offline	

Figure 23. Services going offline –online with switchover sequence

Stop Order Sequence: Agent -> OMS -> Script -> Disk offline

Note: In offline function, script calls **emctl stop oms -all** to shut down all OMS process.

Start Order Sequence: Disk online ->Script -> OMS -> Agent

Note: In online function, script has a placeholder function to clean the OMS process/ java process prior to starting.

Observe the process as the OMS and agent process starts and stops on either of nodes.

## Deploy Physical Agents to monitor Windows node

It is essential to deploy physical agents on primary and standby windows nodes to monitor the health of these nodes. Physical agents are installed on the local drive.

Local physical agents are deployed using the agent silent deployment using the agent image from software library. Refer to **Section 6.4.2 Installing a Management Agent Using the agentDeploy Script** in Enterprise Manager Advanced Installation and Configuration Guide for configuration details.

Fetching Agent image from software library

Login to emcli and query the repository to check what agents are in the repository using “emcli get\_supported\_platforms”

Download the specific agent image using "emcli get\_agentimage". Download the agent zip on shared directory and then copy over to both Windows nodes on a local directory. Installation folder to be provided local directory on each Windows node.

### Local physical agent deployment

Prepare agent.rsp response file entries as below

- OMS\_HOST= slc03zozp-r.us.oracle.com < Cluster Resource Name >
- EM\_UPLOAD\_PORT=1159 < Repository Upload port of OMS >
- AGENT\_REGISTRATION\_PASSWORD=<changeme>
- AGENT\_INSTANCE\_HOME=C:\local\_agent\agent\_inst <Local path>
- AGENT\_PORT=1830 <Port to be different from that of central shared agent>
- b\_startAgent=true
- ORACLE\_HOSTNAME= <physical hostname of the node>
- s\_agentHomeName=\_agent167
- s\_agentSvcName="localAgent"

Deploy the agent using the command(Figure 24):

```
c:\local_agent\agent_inst\bin>agentDeploy.bat AGENT_BASE_DIR=C:\local_agent RESP
ONSE_FILE=C:\local_agent\agent.rsp
```

Figure 24 . Agent Deploy Command

Start the local agent and observe the process( Figure 25) to confirm that two agent process ( one on shared storage and one on local disk) are started on the primary active Windows node.

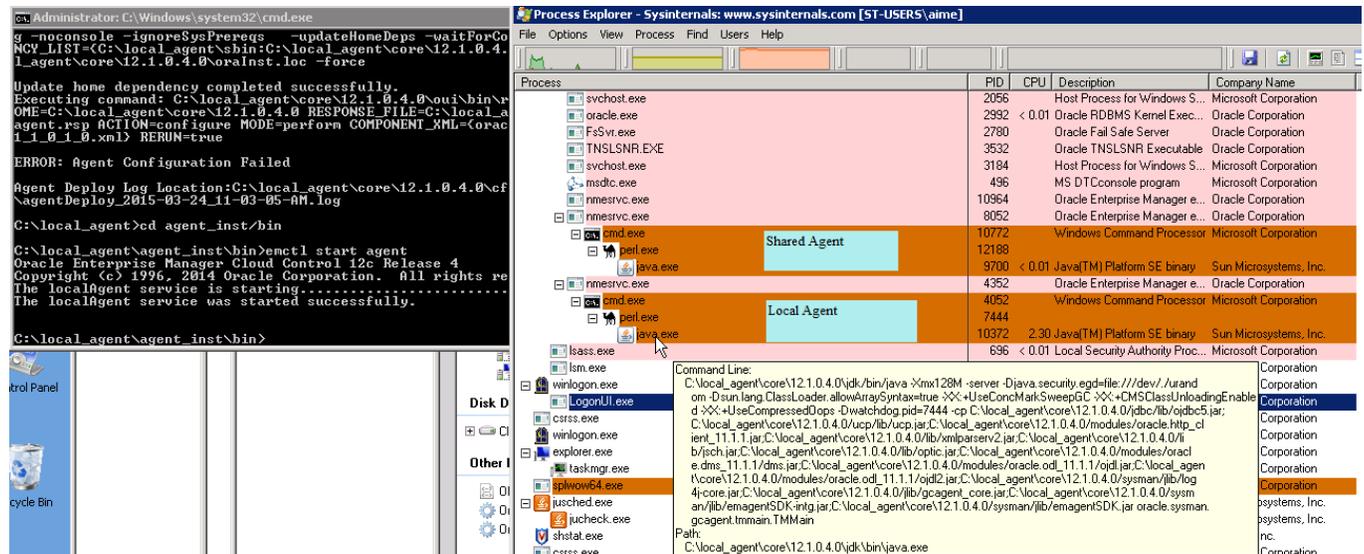


Figure 25 . Two agent process running on active Windows node

Check the Enterprise Manager Cloud Console and see that the alias hostname agent and two physical agents show Status UP.

Target Name	Target Type	Target Status
slc03zzo.us.oracle.com:1830 <span style="color: red;">Physical Node Agent</span>	Agent	↑
slc03zozp-r.us.oracle.com:3872 <span style="color: red;">Alias Hostname Agent</span>	Agent	↑
slc03zpz.us.oracle.com:1830 <span style="color: red;">Physical Node Agent</span>	Agent	↑

Figure 26. Agent process seen in Enterprise Manager Cloud Control console

Ensure that the physical node agents monitor only the Windows physical nodes while the alias hostname agent monitors all the targets that come with Enterprise Manager installation.

## Verify Failover

As a general recommendation, it is good to test the failover after the switchover verification is completed to ensure the cluster configuration is geared to handle abrupt failures. To simulate failover (network disconnect / disk failure on active primary Windows node) and test the functionality, follow the below steps as shown in Figure 27.

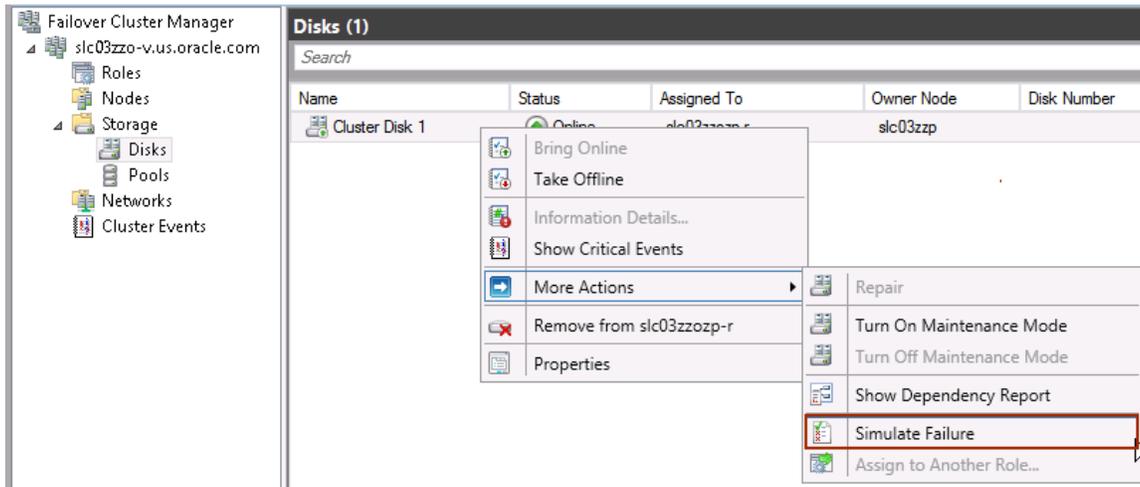


Figure 27. Failover Simulation.

This simulates crash on the active Windows node. Move the cluster resource to standby Windows node. The cluster resources become online on standby Windows node but the java processes in the crashed node are not shutdown completely. Now switchback the cluster resource from current active standby node to primary node. The CleanProcess() function within the script if uncommented and have been modified to include the logic as discussed prior, will function to start the Enterprise Manager process cleanly on the primary Windows node.



## Troubleshooting

If there are any issues when OMS services are stopped /started on any cluster node, refer to `$INSTANCE_HOME/sysman/log/emctl.log` for diagnosis.

For advanced troubleshooting, cluster log provides verbose logging for the cluster service. Refer to Windows Failover Cluster Administration Guide for enabling cluster logs.

## Conclusion

Enterprise Manager Cloud Control is a crucial data center application and as such, availability of Enterprise Manager Cloud Control infrastructure is of critical importance. The solution outlined in this document shows how standard high availability technologies in Windows platform like Microsoft Windows Failover Clustering solution can be leveraged for Enterprise Manager Cloud Control deployments, thus ensuring continuous operation of this mission-critical application.

## Appendix

### Failover Script

'Script-Level Global Variables

```
Resource.LogInformation("OMS failover script begins execution")
```

```
Dim EmctlCmdPath, WshShell, oExec, oLooksAlive, oIsAlive, oWait, aliveState, returnCode
```

```
Set WshShell = CreateObject("WScript.Shell")
```

**###Please update and replace ORACLE\_HOME value before using###**

```
EmctlCmdPath = "ORACLE_HOME\BIN\emctl.bat"
```

```
aliveState = 1
```

```
Function Open( )
```

```
    Resource.LogInformation "VBScript BuildVersion: " & ScriptEngineBuildVersion
```

```
    Resource.LogInformation "VBScript Version: " & ScriptEngineMajorVersion _
```

```
    & "." & ScriptEngineMinorVersion
```

```
    Resource.LogInformation "Opening Script File: " & ScriptName
```

```
    Open = 0
```

```
End Function
```

Function CleanProcess()

```
#####!!PLEASE READ BEFORE USING BELOW!!#####  
#####  
'# The cleanup procedure to clean OMS-related processes is #  
'# provided only as a guide and is specific to the version #  
'# of OMS installed. #  
'# #  
'# No support will be provided for the cleanup procedure - #  
'# customer will use at own risk!!! #  
'# #  
'# Oracle is not responsible for any unintended processes #  
'# cleaned by the script due to similarity in search #  
'# patterns. #  
#####
```

Resource.LogInformation "Cleaning up weblogic processes"

servArg = "%weblogic.Name=%"

nmArg = "% weblogic.NodeManager%"

istopArg = "% istop%"

stopPyArg = "%stopOMS.py%"

'query to kill node manager process'

nmQuery = "select \* from win32\_process where CommandLine LIKE " & "'''' & nmArg & "''''"

'query to kill weblogic server processes'

servQuery = "select \* from win32\_process where CommandLine LIKE " & "'''' & servArg & "''''"

'query to kill weblogic server processes'

istopQuery = "select \* from win32\_process where CommandLine LIKE " & "'''' & istopArg & "'''' OR CommandLine  
LIKE " & "'''' & stopPyArg & "''''"



```

pids = ""
Comp = "."
Set FileSystem = CreateObject("Scripting.FileSystemObject")
Set WMIService = GetObject("winmgmts:\\." & Comp & "\root\cimv2")
Set Items = WMIService.ExecQuery(nmQuery, , 48)
For Each SubItems In Items
  pids = pids & " " & SubItems.ProcessId
  SubItems.Terminate()
Next
Set Items = WMIService.ExecQuery(servQuery, , 48)
For Each SubItems In Items
  pids = pids & " " & SubItems.ProcessId
  SubItems.Terminate()
Next
Set Items = WMIService.ExecQuery(istopQuery, , 48)
For Each SubItems In Items
  pids = pids & " " & SubItems.ProcessId
  SubItems.Terminate()
Next

Resource.LogInformation "weblogic pids "" & pids & "" were cleaned up"
End Function

```

```

Function Online( )
  Resource.LogInformation "Entering Online"

  '#####!!PLEASE READ BEFORE UNCOMMENTING BELOW!!#####
  '#####
  '# The cleanup procedure to clean OMS-related processes is #
  '# provided only as a guide and is specific to the version #
  '# of OMS installed. #
  '# #

```



```
'# No support will be provided for the cleanup procedure - #  
'# customer will uncomment and use at own risk!!!      #  
'#                #  
'# Oracle is not responsible for any unintended processes #  
'# cleaned by the script due to similarity in search    #  
'# patterns.                #  
#####
```

**'Uncomment procedure to force clean up OMS-related processes  
'before starting up the OMS service**

```
'CleanProcess()
```

```
Online = 0
```

```
End Function
```

```
Function LooksAlive( )
```

```
Resource.LogInformation "Entering LooksAlive"
```

```
LooksAlive = 0
```

```
End Function
```

```
Function IsAlive( )
```

```
Resource.LogInformation "Entering IsAlive"
```

```
IsAlive = 0
```

```
End Function
```

```
Function Offline( )
```

```
Resource.LogInformation "Entering Offline"
```

```
ReturnCode = WshShell.Run(""" & EmctlCmdPath & "" stop oms -all -debug", 0, true)
```

```
Resource.LogInformation """" & EmctlCmdPath & "" stop oms -all exited with " & ReturnCode
```



```
If ReturnCode <> 0 Then  
    Resource.LogInformation oExec.StdErr.ReadAll  
End If
```

```
Offline = ReturnCode  
End Function
```

```
Function Close( )  
    Close = 0  
End Function
```

```
Function Terminate( )  
    Resource.LogInformation "Entering Terminate"  
    Terminate = 0  
End Function
```



**Oracle Corporation, World Headquarters**

500 Oracle Parkway  
Redwood Shores, CA 94065, USA

**Worldwide Inquiries**

Phone: +1.650.506.7000  
Fax: +1.650.506.7200

CONNECT WITH US

-  [blogs.oracle.com/oracle](http://blogs.oracle.com/oracle)
-  [facebook.com/oracle](http://facebook.com/oracle)
-  [twitter.com/oracle](http://twitter.com/oracle)
-  [oracle.com](http://oracle.com)

**Integrated Cloud Applications & Platform Services**

Copyright © 2015, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0615

Enterprise Manager Cloud Control 12c: Configuring Microsoft Windows Server Failover Clustering  
December 2015

Author: Angeline Janet Dhanarani  
Contributing Authors: Mingyan Fan