HP Data Protector

Configuring and integrating Data Protector Cell Manager with Veritas Cluster Server on Windows

Technical white paper

Table of contents

Abstract 2

Introduction 2

Overview of Cell Manager cluster 2
  Failover in a cluster 2

Veritas cluster configuration 3
  VCS service and resource groups 3
  Configuring a VCS generic resource group for Cell Manager 3
  Failover of the VCS service 4

Configuring Data Protector 4
  Installing Data Protector on cluster nodes 5

Data Protector limitations 7

For more information 8

Call to action 8

Abstract

This white paper describes the steps necessary to implement the configuration and integration of a Cell Manager in a Cluster environment with Veritas Cluster Server. It covers Data Protector A.06.11 and Data Protector A.06.20 with Veritas Cluster Server 5.1 SP2 (VrtsSFHA 5.1 SP2 for Windows).

Introduction

This document introduces the configuration and integration of Data Protector with the Veritas Cluster Environment on Windows.

It also tells how auto-failover of the Cell Manager occurs on secondary nodes of the cluster when the primary or active node goes down.

Unlike MSCS cluster, Data Protector does not recognize cluster availability during installation, so Data Protector is installed as a standalone Cell Manager in all the nodes of the cluster and then manually integrated with Veritas Cluster service groups.

Just like MSCS Cluster, in VCS the Cell Manager connectivity will be performed through the virtual IP, and the Internal Database of the Cell Manager resides on the shared disks.

Overview of Cell Manager cluster

Failover in a cluster

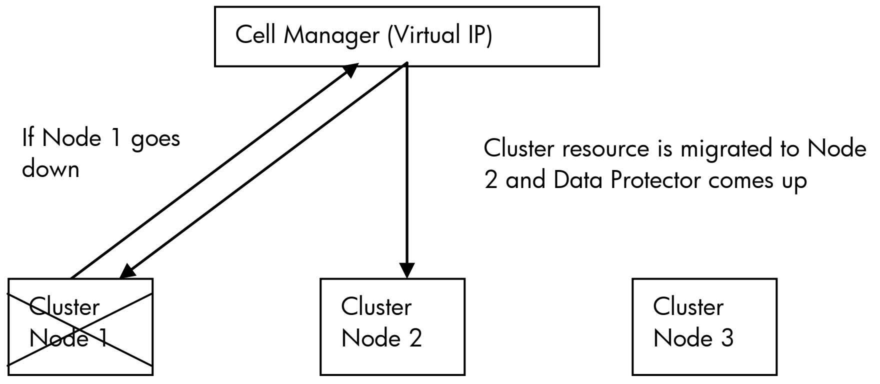
A cluster's ability to redirect requests from one server to another is called *failover*.

When the active node of the cluster goes down, along with the other cluster resources, Data Protector services are moved to another node, so that they are available for users to continue with their backup processes. As the Internal Database of the Cell Manager resides on the shared disks, all the pre-executed sessions will also be available to users.

The Cluster Manager on each cluster server sends out probes to each of the other cluster servers to determine the availability of each server. The Cluster Manager also checks continually if Data Protector services are running on the active node of the cluster. If the services go down, it performs auto-failover of the cluster and brings the services up and running on the other node of the cluster.

Example

This example describes how Data Protector fails over. This cluster contains three nodes. Node 1 is currently unavailable. The Cluster Managers on Node 2 and Node 3 are aware that Node 1 is unavailable.


Cell Manager (Virtual IP)
If Node 1 goes down
Cluster resource is migrated to Node 2 and Data Protector comes up
Cluster Node 1
Cluster Node 2
Cluster Node 3

The user tries to connect to the Cell Manager (Virtual IP).

When the server stops responding, the cluster migrates the resources from Node 1 to Node 2 and brings the Data Protector services up and available for the user.

Veritas cluster configuration

Veritas Cluster Server 5.1 SP2 is installed on all the nodes and the cluster resource groups should be up and running in the active node of the cluster.

VCS service and resource groups

After installing Veritas Cluster Server 5.1 SP2 on all the nodes of the cluster, configure a new VCS service for Data Protector and create all the following resources:

- **NIC** — this has the MAC address of the public Ethernet where the Virtual IP resides. The MAC address is added for all the available cluster nodes.
- **IP** — this has details of the Virtual IP to be used, and its subnet mask.
- **VMDg** — this has information about the shared diskgroup used that is used as the shared diskgroup.
- **MountV** — this has details of the shared volume name and its mount point. This mount point should be free for use on all nodes of the cluster.
- **Lanman** — this is used to resolve the hostname of the Virtual IP address used.
- **FileShare** — this is used to create a shared folder and make it accessible through Virtual IP from the outside.

Configuring a VCS generic resource group for Cell Manager

This generic resource must be created after installing and configuring Cell Manager on all nodes of the cluster with Virtual IP.

Before creating the generic resource for Cell Manager, stop Data Protector Services on all the nodes.

When creating the generic resource for Data Protector, get the service name of the Cell Manager services using the command `sc query state=all` from the `cmd` prompt.

Example

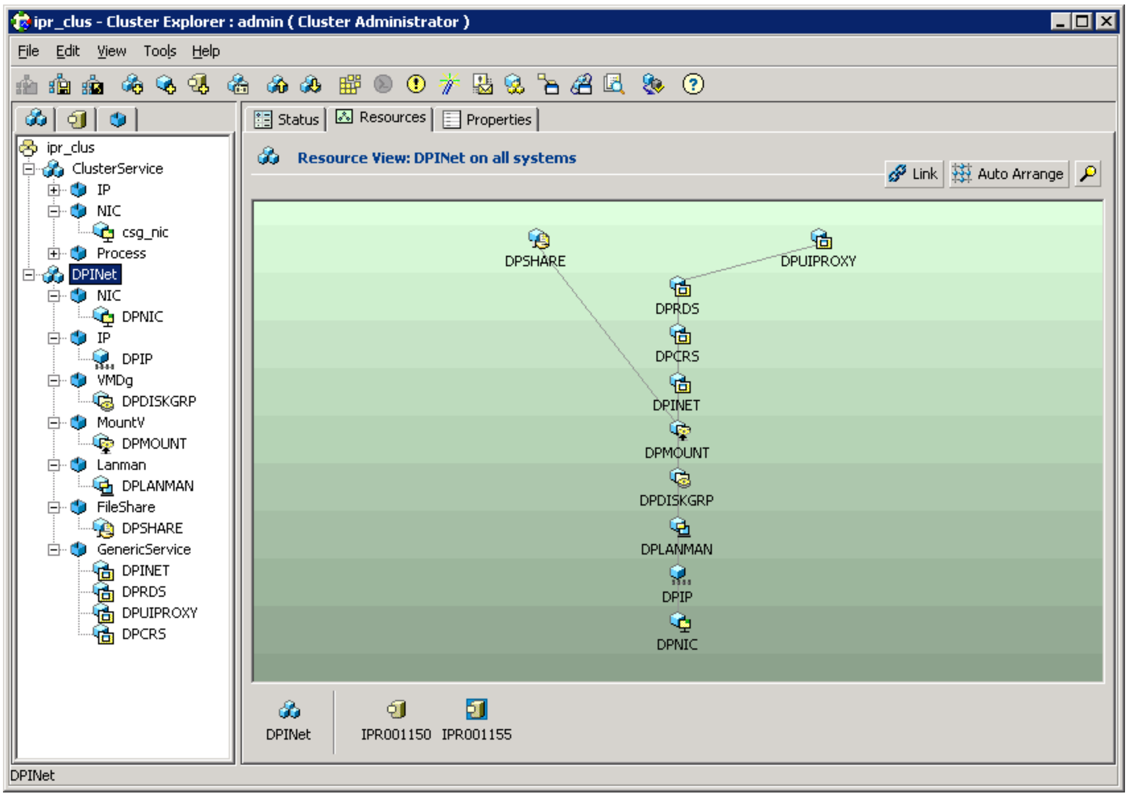
```
>Sc query state= all
SERVICE_NAME: omniInet
DISPLAY_NAME: Data Protector Inet
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 1  STOPPED
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

SERVICE_NAME: omniback_crs
DISPLAY_NAME: Data Protector CRS
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 1  STOPPED
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

SERVICE_NAME: Velocis (ob2_40)
DISPLAY_NAME: Data Protector RDS
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 1  STOPPED
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

SERVICE_NAME: uiproxy
DISPLAY_NAME: Data Protector UIProxy
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 1  STOPPED
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

C:\Users\administrator.IPR>
```

After getting the service name for all the resources of the Cell Manager, create the following generic resources for the Cell Manager:

- **DPCRS** – this has the service name of the Data Protector CRS service.
- **DPRDS** – this has the service name of the Data Protector RDS service.
- **DPINET** – this has the service name of the Data Protector INET service.
- **DPUIPROXYD** – this has the service name of the Data Protector UIPROXY service.

After creating all the generic services for Cell Manager, link them in with the other resources created for dependencies.

Link the database as in the following figure:



Failover of the VCS service

Failover of the resources to secondary or other nodes of the cluster happens if any of the resources in the service becomes faulty or goes down in the active node.

You can also fail-over the resources manually through the VCS console or through VCS HA commands.

Example

```
C:\Users\administrator.IPR>hagrp -switch DPINet -to IPR001150
C:\Users\administrator.IPR>
```

Here, the service group DPINET is moved from the current active node to the secondary node `IPR001150` of the cluster.

When the service has moved to the other node, all the resources created under the service come up automatically along with the Data Protector related generic service.

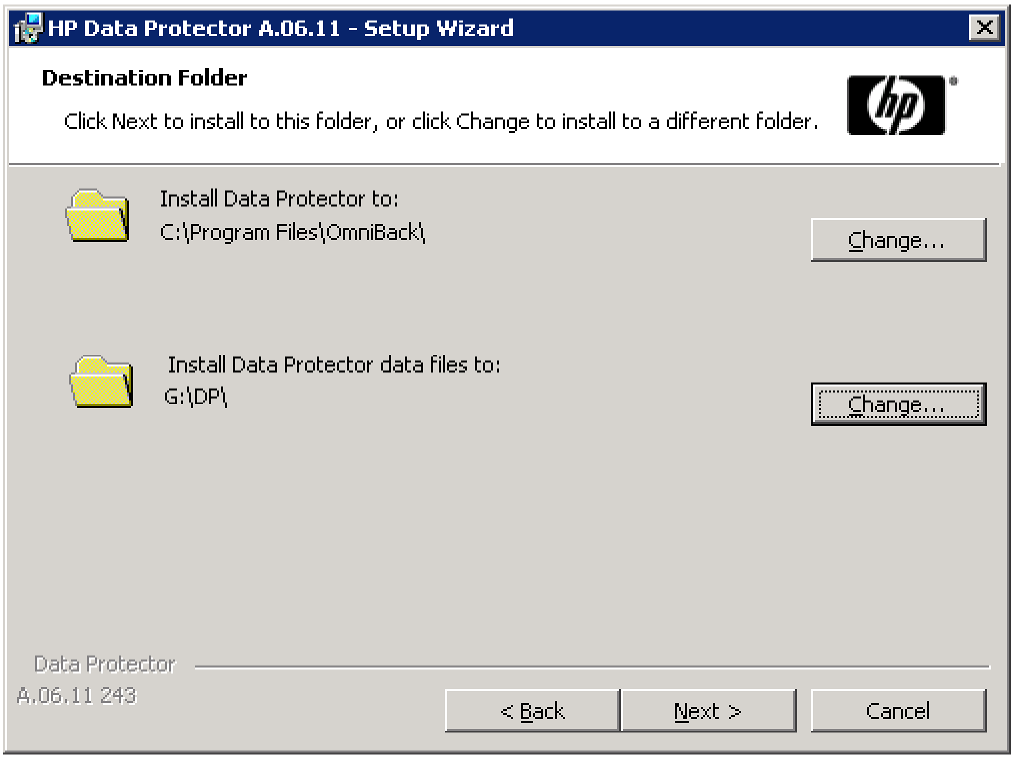
Configuring Data Protector

When configuring Data Protector with Veritas Cluster Server, determine if the disk on which the Internal Database resides should be available on the other nodes of the cluster.

Installing Data Protector on cluster nodes

Unlike MSCS cluster, Data Protector does not recognize cluster availability during installation, so Data Protector is installed as a standalone Cell Manager in all the nodes of the cluster, and then manually integrated with Veritas Cluster Service Groups.

Install the Data Protector Software as a standalone Cell Manager in all the nodes of the cluster in turn, with the Internal Database residing on the shared disk. Make sure that the shared disk is mounted on the node while installing the Cell Manager.


HP Data Protector A.06.11 - Setup Wizard

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install Data Protector to:
C:\Program Files\OmniBack\

Install Data Protector data files to:
G:\DP\

Here, the Internal Database is set as `G:\DP`, which is the shared disk mounted on the active node of the cluster.

As the Data Protector is installed as a standalone server, configure it with the Virtual IP as follows:

1. Access the Internal Database catalog cell name as Virtual IP:

```
C:\Users\administrator.IPR>omnidbutil -show_cell_name
Catalog database owner: "ipr001155.ipr.home.net"
```

```
C:\Users\administrator.IPR>omnidbutil -change_cell_name IPR001154.ipr.home.net
-
force
DONE!
```

2. Check the Catalog cell name of the Data Protector:

   C:\Users\administrator.IPR>omnidbutil -show_cell_name
   Catalog database owner: "ipr001154.ipr.home.net"

3. Import the Virtual Host as a Data Protector client:

```
C:\Users\administrator.IPR>omnicc -import_host ipr001154.ipr.home.net –virtual
Import host successful.
```

```
C:\Users\administrator.IPR>omnisv –stop
HP Data Protector services successfully stopped.
```

4. Manually change the client node registry entry of Cell Manager name:

```
Regpath:HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OpenView\OmniBackII\Site
```

```
CellServer Virtual_NAME

C:\Users\administrator.IPR>omnisv -start
HP Data Protector services successfully started.
```

5. Manually import Virtual IS, and remove the physical IS server name of the node.

   Note: You can also importing a client as installation server and client through the Data Protector GUI.

6. Stop the Cell Manager services.

   Go to the command prompt to the following path "`C:\Program Files\OmniBack\bin`" and execute the command "`Omnisv -stop`":

```
C:\Program Files\OmniBack\bin>omnisv -stop
HP Data Protector services successfully stopped.

C:\Program Files\OmniBack\bin>omnisv -status
    ProcName  Status  [PID]
===============================
    rds          : Down
    crs          : Down
    mmd          : Down
    kms          : Down
    uiproxy      : Down
    omniinet     : Down
    Sending of traps disabled.
===============================
Status: At least one of Data Protector relevant processes/services is not
running.
```

7. Start the Cell Manager services.

   Go to the command prompt to the following path "`C:\Program Files\OmniBack\bin`" and execute the command "`Omnisv -start`":

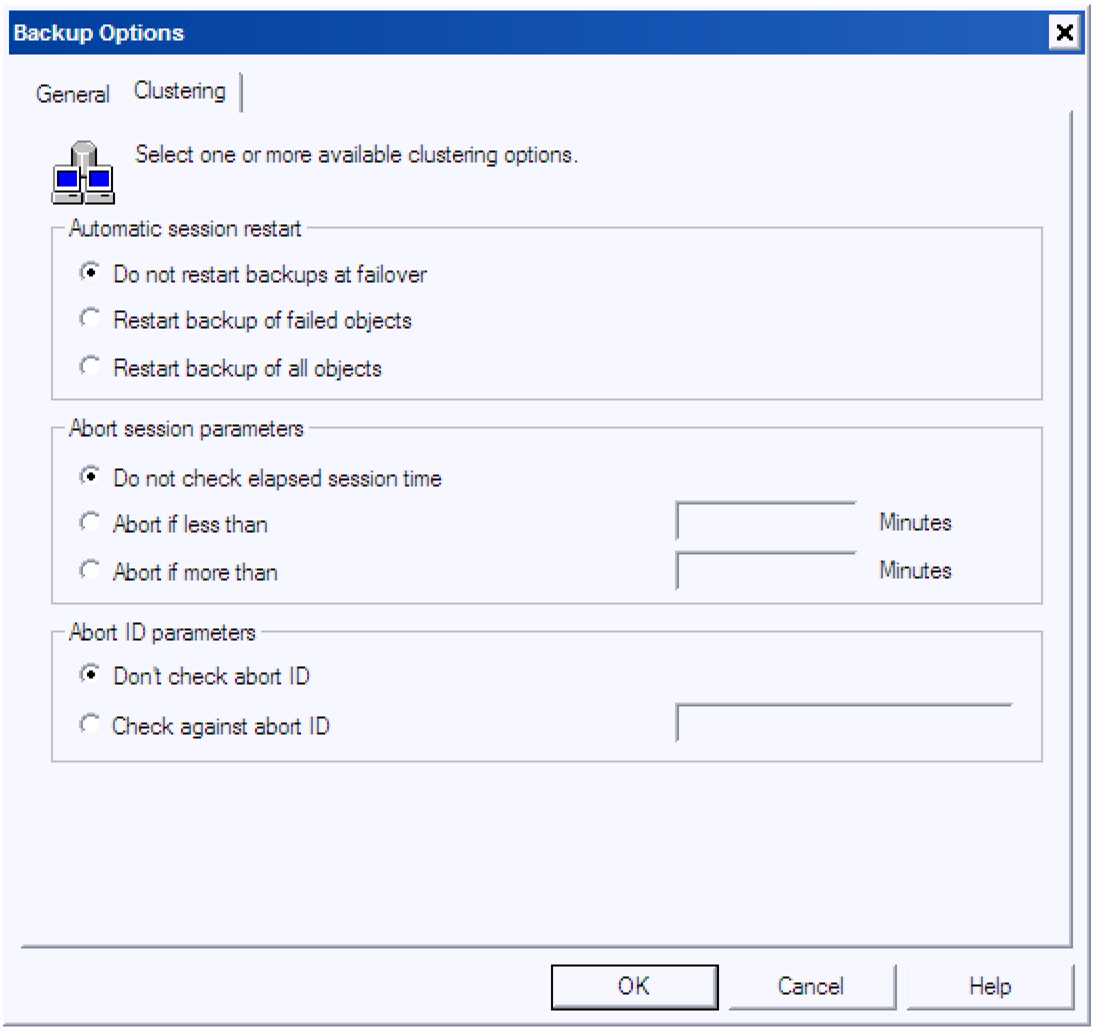
```
C:\Program Files\OmniBack\bin>omnisv -start
HP Data Protector services successfully stopped.

C:\Program Files\OmniBack\bin>omnisv -status
    ProcName  Status  [PID]
===============================
    rds          : Active  [3288]
    crs          : Active  [5636]
    mmd          : Active  [1848]
    kms          : Active  [2544]
    uiproxy      : Active  [3408]
    omniinet     : Active  [4888]
    Sending of traps disabled.
===============================
Status: All Data Protector relevant processes/services up and running.
```

Note: Start the Cell Manager services only on the active node of the cluster, on which the virtual IP and shared disks reside.

After configuring the Cell Manager on the first node of the cluster, stop the Cell Manager services, migrate the VCS services to the second node of the cluster and follow the same steps to install and configure the Cell Manager. Follow the same steps on all the nodes of the cluster.

Data Protector limitations

Data Protector clustering options are not applicable for Cell Manager clustering with Veritas Cluster Suite on Windows.



Select one or more available clustering options.

Automatic session restart

● Do not restart backups at failover

○ Restart backup of failed objects

○ Restart backup of all objects

Abort session parameters

● Do not check elapsed session time

○ Abort if less than Minutes

○ Abort if more than Minutes

Abort ID parameters

● Don't check abort ID

○ Check against abort ID

For more information

To read more about Data Protector go to http://www.hp.com/go/dataprotector

Call to action

http://www.hp.com/go/dataprotector

4AA3-5761ENW, Created October 2011