SYMATEC SOLUTIONS DEPLOYMENT GUIDES

Storage Foundation Cluster File System HA on VMware VMDK Deployment Guide

Author: Carlos Carrero

Technical Product Manager

Version: Feb-2013

Table of Contents

Introduction

This deployment guide will explain how to install and configure Cluster File System High Availability (HA) when running in a VMware virtual server using VMware filesystem (VMFS) virtual disks (VMDKs) as the storage subsystem. This guide is not a replacement or substitute for the administration and installation guides for Storage Foundation Cluster File System nor for the VMware documentation. This guide is complementary to, but not a replacement for, those other documents.

Architecture

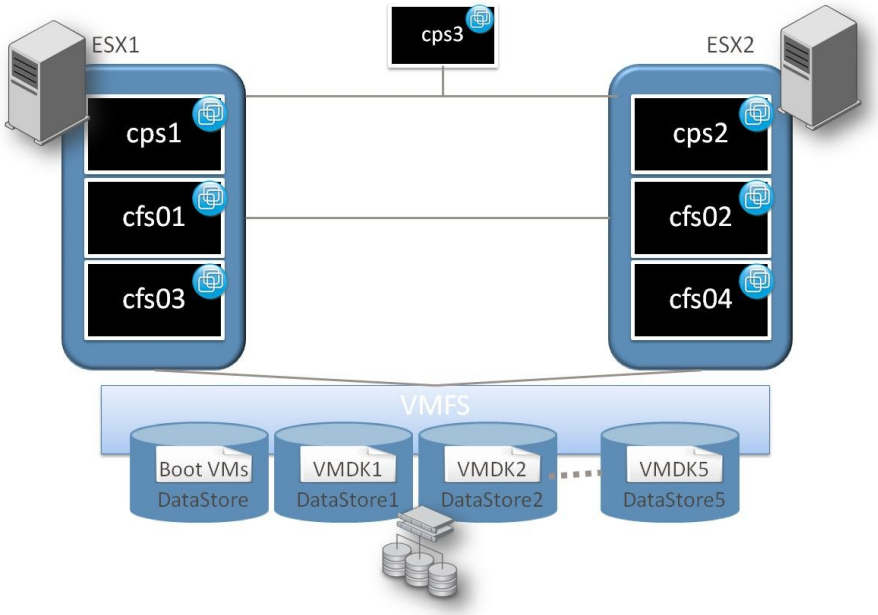
The following product versions and architecture are used in this guide:

RedHat Enterprise Linux Server 6.2

Storage Foundation Cluster File System HA 6.0.1

ESXi 5.1

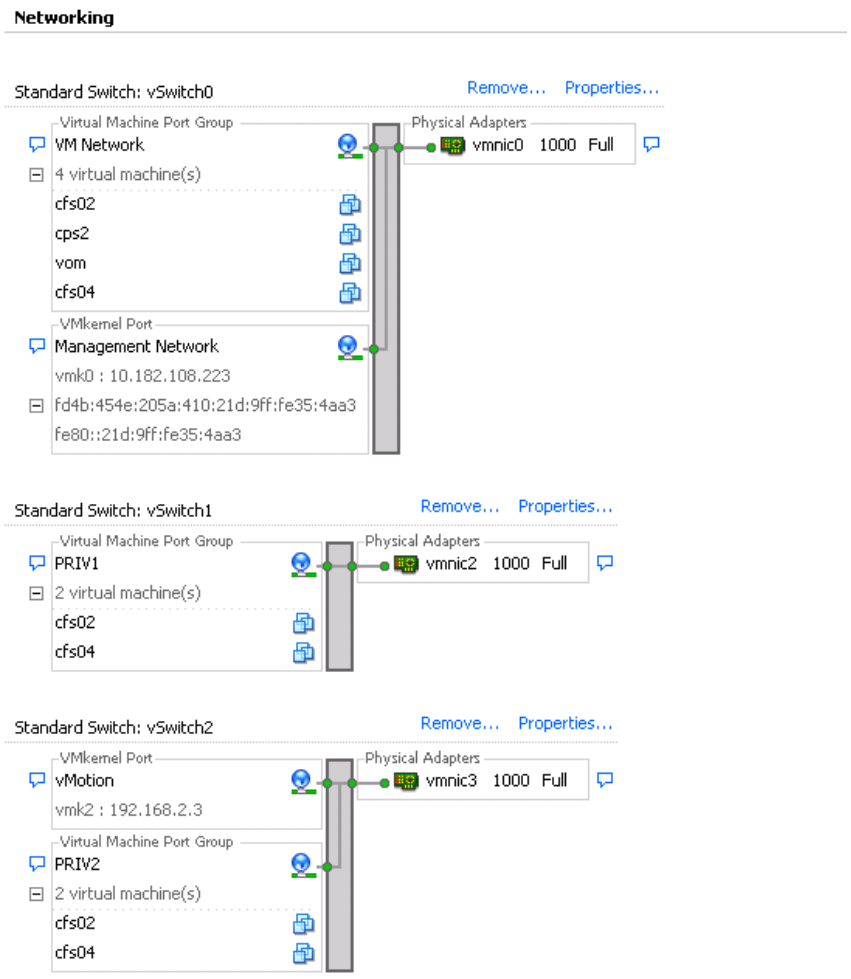
A four node virtual machine cluster will be configured on 2 VMware ESX servers. Shared storage between the two ESX servers using Fibre Channel has been setup. The Cluster File System will exist across four virtual machines: cfs01, cfs02, cfs03, and cfs04. Three Symantec Coordination Point (CP) Servers will be used: cps1, cps2, and cps3 (this one placed in a different ESX server). For storage, five data stores will be used and one shared VMDK file will be placed in each data store.



Network Configuration

Two private networks will be used for cluster heartbeat. They are called PRIV1 and PRIV2. Virtual switch vSwitch2 also has the VMkernel Port for vMotion enabled. vSwitch0 is used for management traffic and the public IP network.

Some blades have a two network limit. If this is the case, configure one network for heartbeats and the other one as a heartbeat backup (low priority setting).

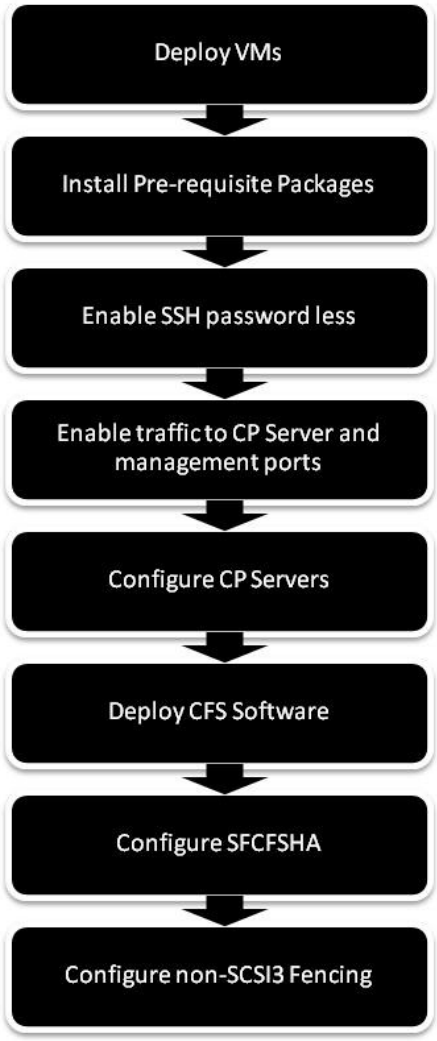


Storage Foundation Cluster File System HA Configuration

Planning overview

There are a number of recommended steps in this guide that must be followed to achieve a successful implementation. This section covers the steps needed to install and configure Cluster File System and use CP Servers using the product versions stated at the beginning of the document. Different software versions may require different steps, so please refer to the admin guides and release notes for additional information.

These will be the steps needed to complete the deployment:



These steps are discussed and documented on the following pages.

Checking Pre-Requisites

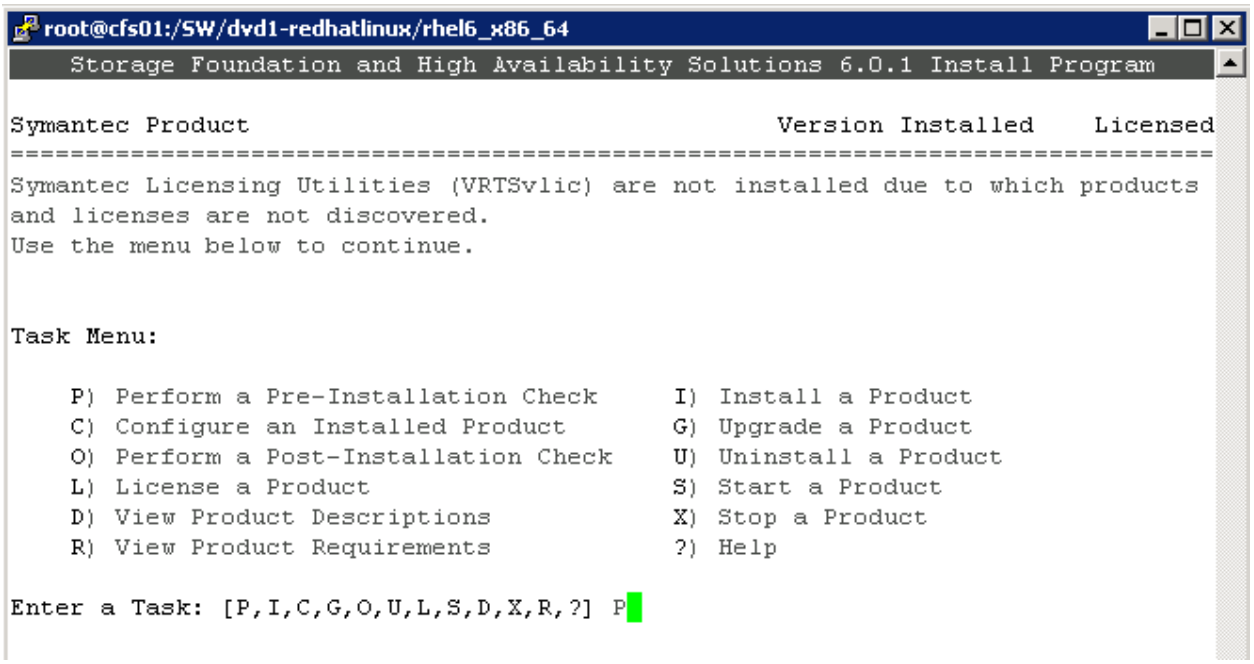
Execute the installer script :

/<mntpoint>/<platform>/<release>/install

We are installing SFCFSHA 6.0.1 on RedHat 6.2 version, so use this path:

/SW/dvd1-redhatlinux/rhel6_x86_64

The CPI installer will show all the options available first we are going to run a Pre-Installation Check, so enter task **P**



The product that will be installed is SFCFSHA (Storage Foundation Cluster File System High Availability), so option 5 is chosen. After that, we enter the name of the four nodes that will be configured (cfs01, cfs02, cfs03 and cfs04):

```
Storage Foundation and High Availability Solutions 6.0.1 Precheck Program

     1)  Veritas Dynamic Multi-Pathing (DMP)
     2)  Veritas Cluster Server (VCS)
     3)  Veritas Storage Foundation (SF)
     4)  Veritas Storage Foundation and High Availability (SFHA)
     5)  Veritas Storage Foundation Cluster File System HA (SFCFSHA)
     6)  Symantec VirtualStore (SVS)
     7)  Veritas Storage Foundation for Sybase ASE CE (SFSYBASECE)
     8)  Veritas Storage Foundation for Oracle RAC (SF Oracle RAC)
     b)  Back to previous menu

Select a product to perform pre-installation check for: [1-8,b,q] 5

Enter the 64 bit RHEL6 system names separated by spaces: [q,?] cfs01 cfs02 cfs03
 cfs04
```

The pre-installation test starts. First it will check the communication status across all the nodes. SSH must be configured on the nodes to perform a successful installation. If your systems already have SSH configured, this step will not be necessary. The CPI installer will offer to automatically enable no-password/password-less SSH. The recommended action is to allow the CPI installer to configure it. If you need to perform any other cluster reconfiguration later, SSH/RSH password-less will have to be enabled manually. Detailed instructions are provided at the end of this document. Enter the password:

```
Veritas Storage Foundation Cluster File System HA 6.0.1 Precheck Program
                        cfs01 cfs02 cfs03 cfs04

Logs are being written to /var/tmp/installer-201212200037PXg while installer is
in progress

    Verifying systems: 25%  ____________________________________________

    Estimated time remaining: (mm:ss) 4:55                          2 of 8

    Checking system communication ..................................... Done
    Checking release compatibility .................................... Done

Either ssh or rsh needs to be set up between the local system and cfs02 cfs03
cfs04 for communication

Would you like the installer to setup ssh or rsh communication automatically
between the systems?
Superuser passwords for the systems will be asked. [y,n,q] (y) y

Enter the superuser password for system cfs02:

 Do you want to use the same password for all systems? [y,n,q] (y) y
```

Select SSH:

```
Do you want to use the same password for all systems? [y,n,q] (y) y

     1)  Setup ssh between the systems
     2)  Setup rsh between the systems
     b)  Back to previous menu

Select the communication method [1-2,b,q,?] (1) 1
```

Notice that one of the steps that has failed:

```
    Checking system communication ..................................... Done
    Checking release compatibility .................................... Done
    Checking installed product ........................................ Done
    Checking prerequisite patches and rpms ......................... Failed
    Checking platform version ......................................... Done
    Checking file system free space ................................... Done
    Checking product licensing ........................................ Done
    Performing product prechecks ...................................... Done

Precheck report completed
```

When running the CPI on RHEL 6.2/6.3, an error message will appear with a list of RPMs that could not be found (same for each of the virtual servers, as they have all been cloned):

```
CPI ERROR V-9-30-2225 The following required OS rpms (or higher version) were
not found on cfs01:
        nss-softokn-freebl-3.12.9-3.el6.i686 glibc-2.12-1.25.el6.i686
pam-1.1.1-8.el6.i686 libstdc++-4.4.5-6.el6.i686 libgcc-4.4.5-6.el6.i686
ksh-20100621-6.el6.x86_64
```

Install Pre-requisite Packages

The resolution for this error is documented in Symantec support article TECH196954:

http://www.symantec.com/business/support/index?page=content&id=TECH196954

The following package versions must be installed before deploying Storage Foundation:

glibc-2.12-1.25.el6.i686
libgcc-4.4.5-6.el6.i686
libstdc++-4.4.5-6.el6.i686
nss-softokn-freebl-3.12.9-3.el6.i686
pam-1.1.1-10.el6.i686.rpm
ksh-20100621-12.el6.x86_64.rpm

We are deploying on top of RedHat 6.2, so these are the RPMs to be installed:

```
rpm -ivh glibc-2.12-1.47.el6.i686.rpm
rpm -ivh libgcc-4.4.6-3.el6.i686.rpm
rpm -ivh libstdc++-4.4.6-3.el6.i686.rpm
rpm -ivh nss-softokn-freebl-3.12.9-11.el6.i686.rpm
rpm -ivh pam-1.1.1-10.el6.i686.rpm
rpm -ivh ksh-20100621-12.el6.x86_64.rpm
```

Additionally you may use the yum tool to install the pre-requisite packages if that is your preferred option.

Verify Successful Completion of the Verification Checks

Complete any other pre-requisite you may have until all the verification checks complete successfully:

```
    Checking system communication ..................................... Done
    Checking release compatibility .................................... Done
    Checking installed product ........................................ Done
    Checking prerequisite patches and rpms ............................ Done
    Checking platform version ......................................... Done
    Checking file system free space ................................... Done
    Checking product licensing ........................................ Done
    Performing product prechecks ...................................... Done

Precheck report completed

System verification checks completed successfully

No issues found in prechecks

Would you like to install SFCFSHA on cfs01 cfs02 cfs03 cfs04? [y,n,q] (n)
```

At this point you can exit the script or open a new shell to configure cluster CPS communications. We will return to install SFCFSHA later in the document.

Enable Password-less SSH

The installer will be able to password-less configure SSH/RSH among the cluster nodes, but it will not be able to enable this required functionality between the cluster nodes and the CP servers. For example, later setting changes, like modifying the IO fencing configuration, may need password-less SSH/RSH. In this configuration we are going to configure password-less SSH between the node that we will be using to configure the cluster and the rest of the nodes. These are the instances where Password-less SSH will be enabled:

Source	Target	Reason
cfs01	cfs02	Cluster configuration

cfs01	cfs03	Cluster configuration
cfs01	cfs04	Cluster configuration
cfs01	cps1	Non-SCSI-3 fencing configuration
cfs01	cps2	Non-SCSI-3 fencing configuration
cfs01	cps3	Non-SCSI-3 fencing configuration
cps1	cfs01	Secure cluster configuration
cps2	cfs01	Secure cluster configuration
cps3	cfs01	Secure cluster confiugration

If you do not enable Password-less SSH, then follow the manual configuration instructions given at the end of this document.

Enable TCP traffic to CP Server and management ports

For successful intra-cluster communication, make sure that cluster nodes and CP Servers can be reached on port 14250 (or any other if you changed the default). If RedHat Firewall has been enabled, make sure there is a rule to allow the connection to ports 14250 and 14149.

Stop iptables service:

```
[root@cps3 sysconfig]# service iptables stop
iptables: Flushing firewall rules:                         [  OK  ]
iptables: Setting chains to policy ACCEPT: filter          [  OK  ]
iptables: Unloading modules:                               [  OK  ]
```

Enter the following lines at the /etc/sysconfig/iptables file:

```
-A INPUT -p tcp -m tcp --dport 14250 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 14149 -j ACCEPT
```

Start the service:

```
[root@cps2 ~]# service iptables restart
iptables: Flushing firewall rules:                         [  OK  ]
iptables: Setting chains to policy ACCEPT: filter          [  OK  ]
iptables: Unloading modules:                               [  OK  ]
iptables: Applying firewall rules:                         [  OK  ]
[root@cps2 ~]#
```

And verify the new rule is in place:

```
[root@cps3 sysconfig]# iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:cps
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:vrts-tdd
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:xprtld
```

These rules must be enabled on cfs01, cfs02, cfs03, cfs04, cps1, cps2 and cps3

Configure Coordination Point Servers

In order to protect the cluster from data corruption caused by a cluster failure that results in "split-brain," Coordination Point Servers must be deployed. At this point it is recommended to configure the CP Servers that are going to be used to provide non-SCSI-3 fencing protection. The last section of this document describes clearly how to configure the CP Server. Please refer to that part in the documentation of this guide if a new CP Server deployment is needed. CP Servers can be used for multiple clusters, so this step will only be necessary the first time a cluster is configured and no CP Servers are available.

SFCFSHA Software Deployment

The next step will be to deploy SFCFSHA in each of the four virtual machines that make up the cluster. In order to do that, we could have either selected yes in the previous CPI step, so the install could continue, or run the **`installer`** script again. In the latter case select:

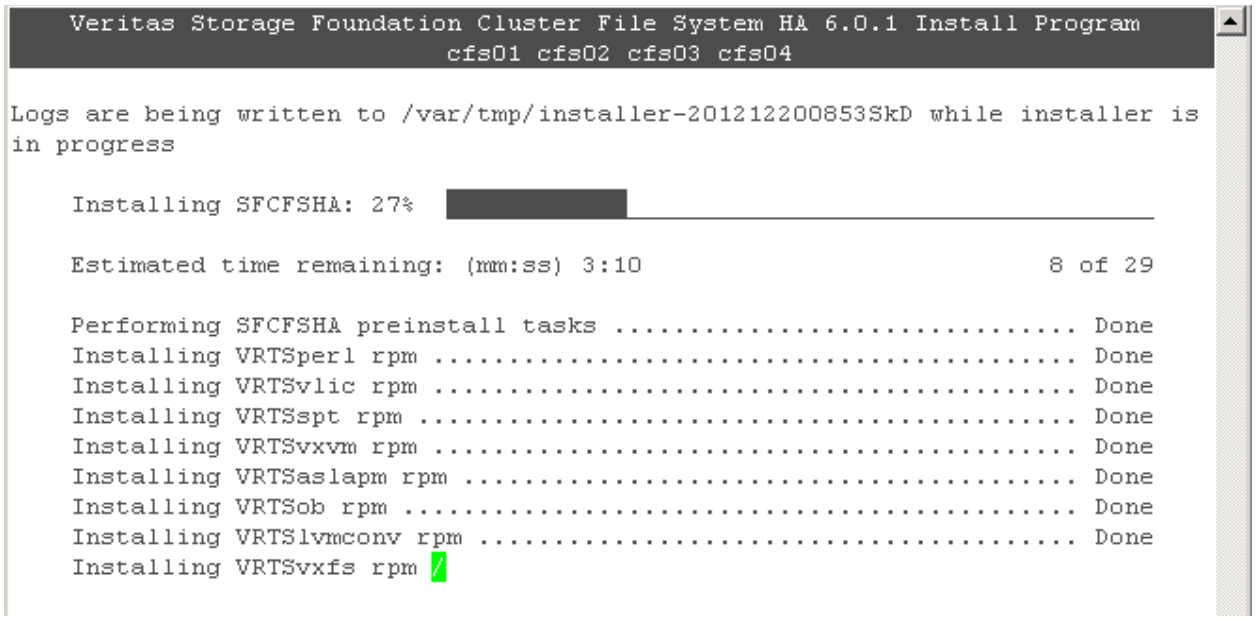
- I) Install a Product
- 5) Veritas Storage Foundation Cluster File System HA (SFCFSHA)
- Agree the terms of the EULA

Select option 3, Install **all** RPM

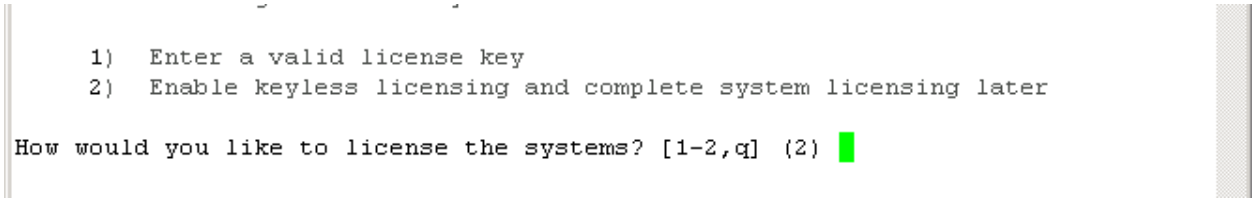
```
    Veritas Storage Foundation Cluster File System HA 6.0.1 Install Program

     1)  Install minimal required rpms - 406 MB required
     2)  Install recommended rpms - 769 MB required
     3)  Install all rpms - 793 MB required
     4)  Display rpms to be installed for each option

Select the rpms to be installed on all systems? [1-4,q,?] (2) 3
```

- Enter the name of the nodes of the cluster (cfs01 cfs02 cfs03 cfs04)

The installer then will verify the pre-requisites again, and a list of all the RPMs that will be installed will be printed. Then, the RPM installation will be performed.



Once the RPMs have been installed, the installer will ask for the product license. This cluster will be managed by VOM (Veritas Operation Manager), so select option 2 to enable keyless licensing:



- Replication license will not be enabled in this deployment
- Global Cluster Option will not be enabled in this deployment

Once the licenses have been registered, the installer has finished with the deployment. Now configuration can be started. If you want a Virtual Machine template with the SFCFSHA software already deployed, stop here and take a snapshot or other copy of this image. The next step will be to run "`installer -configure`" to continue with the configuration.

Software Configuration

Run "`installer -configure`" or just continue from where we left in the previous step entering **"y"**:

```
    Veritas Storage Foundation Cluster File System HA 6.0.1 Install Program
                              cfs01 cfs02 cfs03 cfs04

Would you like to enable replication? [y,n,q] (n)
Would you like to enable the Global Cluster Option? [y,n,q] (n)

Registering SFCFSHA license
SFCFSHA vxkeyless key (SFCFSHAENT) successfully registered on cfs01
SFCFSHA vxkeyless key (SFCFSHAENT) successfully registered on cfs02
SFCFSHA vxkeyless key (SFCFSHAENT) successfully registered on cfs03
SFCFSHA vxkeyless key (SFCFSHAENT) successfully registered on cfs04

Would you like to configure SFCFSHA on cfs01 cfs02 cfs03 cfs04? [y,n,q] (n) y
```

The next step in the installer flow is I/O fencing configuration. However, in order to provide a systematic approach in this guide, we are not going to enable I/O fencing in this step. Because I/O fencing configuration depends on other factors, such as whether VMDKs or RDMP storage devices are used, how I/O and network paths are configured, and configuration of Coordination Point Server (or, in some cases, Coordination Disks) we cover IO fencing in the next section, and at this point we will just enter **"n"** to the question of configuring IO fencing in enabled mode.

```
Would you like to configure SFCFSHA on cfs01 cfs02 cfs03 cfs04? [y,n,q] (n) y

I/O Fencing

It needs to be determined at this time if you plan to configure I/O Fencing in
enabled or disabled mode, as well as help in determining the number of network
interconnects (NICS) required on your systems. If you configure I/O Fencing in
enabled mode, only a single NIC is required, though at least two are
recommended.

A split brain can occur if servers within the cluster become unable to
communicate for any number of reasons. If I/O Fencing is not enabled, you run
the risk of data corruption should a split brain occur. Therefore, to avoid data
corruption due to split brain in CFS environments, I/O Fencing has to be
enabled.

If you do not enable I/O Fencing, you do so at your own risk

See the Administrator's Guide for more information on I/O Fencing

Do you want to configure I/O Fencing in enabled mode? [y,n,q,?] (y) n
```

Now, cluster name, NICs used for heartbeat, and cluster ID will have to be entered to continue the configuration. The cluster name chosen for our deployment is **cfs0**

LLT (Low Latency Protocol) can be configured over Ethernet or UDP. UDP will be needed only when routing between the nodes is necessary. If not needed, then Ethernet is the clear recommendation.

```
    Veritas Storage Foundation Cluster File System HA 6.0.1 Install Program
                            cfs01 cfs02 cfs03 cfs04

     1)  Configure heartbeat links using LLT over Ethernet
     2)  Configure heartbeat links using LLT over UDP
     3)  Automatically detect configuration for LLT over Ethernet
     b)  Back to previous menu

How would you like to configure heartbeat links? [1-3,b,q,?] (1) 1
```

In our deployment, eth4 and eth5 are the private links. Eth3 is the public link, and it will be only used as low priority heartbeat path (so it only will be used if the other two paths fail).

```
    Discovering NICs on cfs01 ..................... Discovered eth3 eth4 eth5

Enter the NIC for the first private heartbeat link on cfs01: [b,q,?] (eth4)
Would you like to configure a second private heartbeat link? [y,n,q,b,?] (y)
Enter the NIC for the second private heartbeat link on cfs01: [b,q,?] (eth5)
Do you want to configure an additional low-priority heartbeat link? [y,n,q,b,?]
(n) y
Enter the NIC for the low-priority heartbeat link on cfs01: [b,q,?] (eth3)
Are you using the same NICs for private heartbeat links on all systems?
[y,n,q,b,?] (y) y
```

All media speed checking should succeed. If not, please review your node interconnections.

```
    Checking media speed for eth4 on cfs01 ....................... 10000Mb/s
    Checking media speed for eth5 on cfs01 ....................... 10000Mb/s
    Checking media speed for eth4 on cfs02 ....................... 10000Mb/s
    Checking media speed for eth5 on cfs02 ....................... 10000Mb/s
    Checking media speed for eth4 on cfs03 ....................... 10000Mb/s
    Checking media speed for eth5 on cfs03 ....................... 10000Mb/s
    Checking media speed for eth4 on cfs04 ....................... 10000Mb/s
    Checking media speed for eth5 on cfs04 ....................... 10000Mb/s

Enter a unique cluster ID number between 0-65535: [b,q,?] (8483)
```

A unique cluster ID is needed. It is quite important to choose a number that is not used in any other cluster. This is especially true when using the same network interconnection (both private and public). The CPI will generate a random number, and will check the network to make sure that packets with that ID do not exist. But the CPI cannot guarantee that the ID is not being used in a cluster that is currently powered off. The best practice is to maintain a register of the cluster IDs used across the data center to avoid use of duplicate IDs.

In our configuration, no other clusters with that ID have been found:

```
Enter a unique cluster ID number between 0-65535: [b,q,?] (8483)

The cluster cannot be configured if the cluster ID 8483 is in use by another
cluster. Installer can perform a check to determine if the cluster ID is
duplicate. The check will take less than a minute to complete.

Would you like to check if the cluster ID is in use by another cluster? [y,n,q]
(y) y

    Checking cluster ID ..................................................... Done

Duplicated cluster ID detection passed. The cluster ID 8483 can be used for the
cluster.

Press [Enter] to continue:
```

At this point a summary of the configuration to be deployed is presented. Examine the summary and enter **"y"** if everything is correct. If not enter **'n'** and go through the steps again.

```
        Cluster Name:      cfs0
        Cluster ID Number: 8483
        Private Heartbeat NICs for cfs01:
                link1=eth4
                link2=eth5
        Low-Priority Heartbeat NIC for cfs01:
                link-lowpri1=eth3
        Private Heartbeat NICs for cfs02:
                link1=eth4
                link2=eth5
        Low-Priority Heartbeat NIC for cfs02:
                link-lowpri1=eth3
        Private Heartbeat NICs for cfs03:
                link1=eth4
                link2=eth5
        Low-Priority Heartbeat NIC for cfs03:
                link-lowpri1=eth3
        Private Heartbeat NICs for cfs04:
                link1=eth4
                link2=eth5
        Low-Priority Heartbeat NIC for cfs04:
                link-lowpri1=eth3

Is this information correct? [y,n,q,?] (y)
```

Now the installer asks for a Virtual IP to manage the cluster. This is not mandatory, and the cluster can be configured without that IP. Depending on your implementation, it might be a best practice. For example, if you are using the Java Console to administer SFCFSHA, only that Virtual IP will be needed (instead of a potentially unavailable node name). In our deployment this will not be used.

```
    Veritas Storage Foundation Cluster File System HA 6.0.1 Install Program
                              cfs01 cfs02 cfs03 cfs04

The following data is required to configure the Virtual IP of the Cluster:

        A public NIC used by each system in the cluster
        A Virtual IP address and netmask

Do you want to configure the Virtual IP? [y,n,q,?] (n) n
```

The next step is whether or not to use secure mode. In the past, the difficulty in configuring Veritas Cluster Server secure mode deterred many users from using it. SFCFSHA 6.0 has been improved and now secure mode configuration is much easier. In 6.0 the installer takes care of the entire configuration. Instead of using the traditional admin/password login, 6.0 uses a validated user and password from the OS. For demonstration purposes, secure mode will be used in this deployment, but feel free to choose the option that best suits your needs.

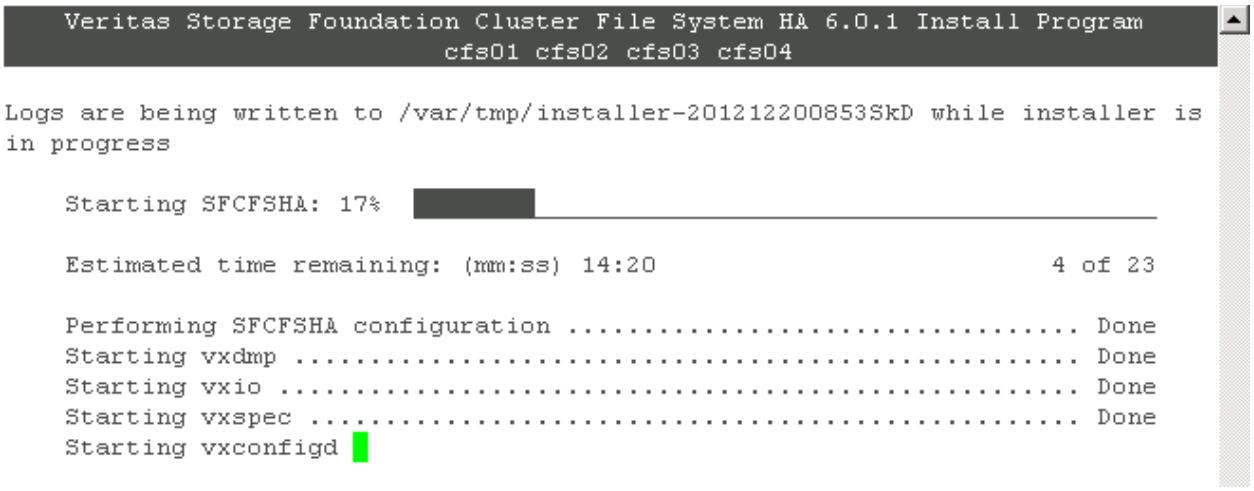
```
    Veritas Storage Foundation Cluster File System HA 6.0.1 Install Program
                              cfs01 cfs02 cfs03 cfs04

Veritas Cluster Server can be configured in secure mode

Running VCS in Secure Mode guarantees that all inter-system communication is
encrypted, and users are verified with security credentials.

When running VCS in Secure Mode, NIS and system usernames and passwords are used
to verify identity. VCS usernames and passwords are no longer utilized when a
cluster is running in Secure Mode.

Would you like to configure the VCS cluster in secure mode? [y,n,q,?] (n) y
```

FIPS will not be used as it is not certified for deployment with CP Servers. Therefore option 1, 'secure mode without FIPS' will be used:

```
Would you like to configure the VCS cluster in secure mode? [y,n,q,?] (n) y
     1)  Configure the cluster in secure mode without fips
     2)  Configure the cluster in secure mode with fips
     b)  Back to previous menu

Select the option you would like to perform [1-2,b,q] (1) 1
```

In our deployment neither SMTP nor SNMP notifications will be used.

At this point the cluster configuration will be initiated:

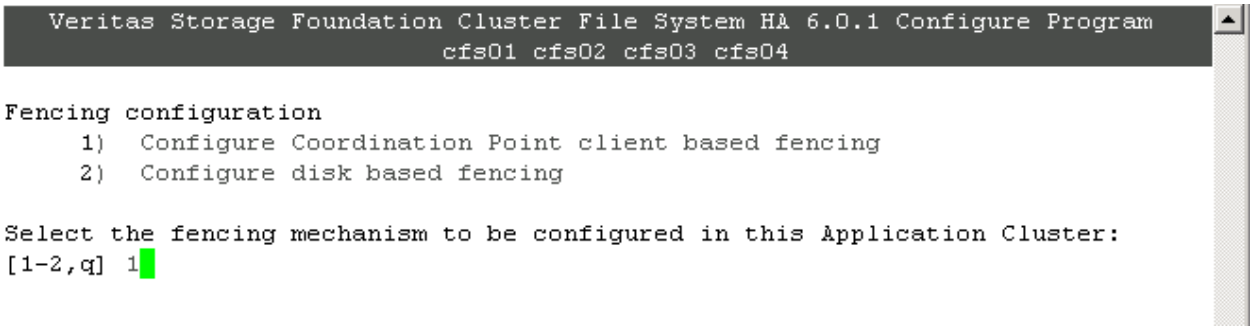


Non-SCSI-3 Fencing Configuration

If, at the beginning of the installation, you selected the enable fencing option, you will be asked to configure fencing. If you chose not to enable fencing at that point, then the cluster configuration is finished and you should now run `installsfcfsha601 -fencing` to enable fencing in the cluster.

VMDK files do not currently support SCSI-3 Persistent Group Reservation and therefore, non-SCSI-3 PGR fencing must be used. Coordination Point Servers will provide this level of server based fencing. At this point the three CP Servers that are going to be used with this cluster should be available and the CP service should be up and running.

Regardless of whether you selected yes to configure fencing during the initial installation or ran the `installsfcfsha601 -fencing` command, you must choose option 1 for Coordination Point client based fencing:



As explained before, VMDK files do not support SCSI-3 PGR, so choose **'n'** to the following question:

```
This fencing configuration option requires a restart of VCS. Installer will stop
VCS at a later stage in this run. Do you want to continue? [y,n,q,b,?] y

Does your storage environment support SCSI3 PR? [y,n,q,b,?] n
```

In the next question select **'y'** to the Non-SCSI-3 fencing question:

```
In virtualized environments that do not support SCSI-3 PR, VCS attempts to
minimize the chances of data corruption with discreet use of timings in the
event of unreachable nodes or network partition. However, if a server becomes
unresponsive, VCS assumes that the node has left the cluster and reconfigures
itself.

This feature only works with UseFence Cluster attribute set to SCSI3 and all
coordination points being Coordination Point servers

In this environment, either Non-SCSI3 fencing can be configured or fencing can
be configured in disabled mode

Do you want to configure Non-SCSI3 fencing? [y,n,q,b] (y) y
```

For production environments, three CP Servers are recommended:

```
Enter the total number of coordination points. All coordination points should be
Coordination Point servers: [b] (3) 3
```

Next we will specify how many interfaces the CP servers will be listening on and the IP address of each interface. If a CP server is reachable via several networks, it is recommended to configure every interface. This allows the SFCFSHA nodes maximum communication flexibility, should a race condition occur.

```
How many IP addresses would you like to use to communicate to Coordination Point
Server #1? [b,q,?] (1)

Enter the Virtual IP address or fully qualified host name #1 for the
Coordination Point Server #1: [b] cps1v.engba.symantec.com

Enter the port in the range [49152, 65535] which the Coordination Point Server
cps1v.engba.symantec.com would be listening on or simply accept the default port
suggested: [b] (14250)

How many IP addresses would you like to use to communicate to Coordination Point
Server #2? [b,q,?] (1)
```

Enter the host names and VIPs for the other CP servers and review the final configuration:

```
   Veritas Storage Foundation Cluster File System HA 6.0.1 Configure Program

CPS based fencing configuration: Coordination points verification

        Total number of coordination points being used: 3
        Coordination Point Server ([VIP or FQHN]:Port):
                1. cps1v.engba.symantec.com ([cps1v.engba.symantec.com]:14250)
                2. cps2v.engba.symantec.com ([cps2v.engba.symantec.com]:14250)
                3. cps3v.engba.symantec.com ([cps3v.engba.symantec.com]:14250)

Is this information correct? [y,n,q] (y)
```

Secure mode will be used:

```
Since the Coordination Point servers are configured in secure mode, installer
will configure the client cluster to secure the communication between
Coordination Point servers and client cluster.

Press [Enter] to continue:
```

Now all the trusted relationships between cluster nodes and CP Servers will automatically be set up:

```
Press [Enter] to continue:
VCS is running in secure mode on cfs01
    Establishing trust between client cluster node cfs01 and Coordination Point
server node cps1v.engba.symantec.com  Done
    Establishing trust between client cluster node cfs01 and Coordination Point
server node cps2v.engba.symantec.com  Done
    Establishing trust between client cluster node cfs01 and Coordination Point
server node cps3v.engba.symantec.com  Done
    Establishing trust between client cluster node cfs02 and Coordination Point
server node cps1v.engba.symantec.com  Done
    Establishing trust between client cluster node cfs02 and Coordination Point
server node cps2v.engba.symantec.com  Done
    Establishing trust between client cluster node cfs02 and Coordination Point
server node cps3v.engba.symantec.com  Done
    Establishing trust between client cluster node cfs03 and Coordination Point
```

Verify that the cluster information is correct:

```
   Veritas Storage Foundation Cluster File System HA 6.0.1 Configure Program

CPS based fencing configuration: Client cluster verification

        CPS Admin utility : /opt/VRTScps/bin/cpsadm
        Cluster ID: 36963
        Cluster Name: cfs0
        UUID for the above cluster: {3891Od38-1dd2-11b2-a898-f1c7b967fd89}

Is this information correct? [y,n,q] (y)
```

And now each node will be registered with each of the CP Servers. Once this is done, the installer will restart VCS to apply the fencing configuration. At this point we don´t have any file system configured yet.

```
    Registering client node cfs04 with Coordination Point Server cps3v.engba.sym
antec.com  Done
    Adding CPClient user for communicating to Coordination Point Server cps3v.en
gba.symantec.com  Done
    Adding cluster cfs0 to the CPClient user on Coordination Point Server cps3v.
engba.symantec.com  Done

Installer will stop VCS before applying fencing configuration. To make sure VCS
shuts down successfully, unfreeze any frozen service group and unmount the
mounted file systems in the cluster.

Are you ready to stop VCS and apply fencing configuration on all nodes at this
time? [y,n,q] (y)
```

Once the configuration has finished, it is recommended to configure the Coordination Point Agent on the client, so CP Servers are proactively monitored from the cluster:

```
    Updating /etc/vxfenmode file on cfs03 ............................ Done
    Updating /etc/vxenviron file on cfs03 ............................ Done
    Updating /etc/sysconfig/vxfen file on cfs03 ...................... Done
    Updating /etc/llttab file on cfs03 ............................... Done

    Updating /etc/vxfenmode file on cfs04 ............................ Done
    Updating /etc/vxenviron file on cfs04 ............................ Done
    Updating /etc/sysconfig/vxfen file on cfs04 ...................... Done
    Updating /etc/llttab file on cfs04 ............................... Done

    Starting Fencing on cfs01 ........................................ Done
    Starting Fencing on cfs02 ........................................ Done
    Starting Fencing on cfs03 ........................................ Done
    Starting Fencing on cfs04 ........................................ Done
    Updating main.cf with fencing ................................... Done
    Starting VCS on cfs01 ............................................ Done
    Starting VCS on cfs02 ............................................ Done
    Starting VCS on cfs03 ............................................ Done
    Starting VCS on cfs04 ............................................ Done

The Coordination Point Agent monitors the registrations on the coordination
points.
Do you want to configure Coordination Point Agent on the client cluster? [y,n,q]
(y)
```

And now the fencing configuration is complete:

```
Do you want to configure Coordination Point Agent on the client cluster? [y,n,q]
(y)
Enter a non-existing name for the service group for Coordination Point Agent:
[b] (vxfen)

    Adding Coordination Point Agent via cfs01 ........................ Done

    I/O Fencing configuration ........................................ Done

I/O Fencing configuration completed successfully

The updates to VRTSaslapm package are released via the Symantec SORT web page:
https://sort.symantec.com/asl. To make sure you have the latest version of
VRTSaslapm (for up to date ASLs and APMs), download and install the latest
package from the SORT web page.

Would you like to send the information about this installation to Symantec to
help improve installation in the future? [y,n,q,?] (y)
```

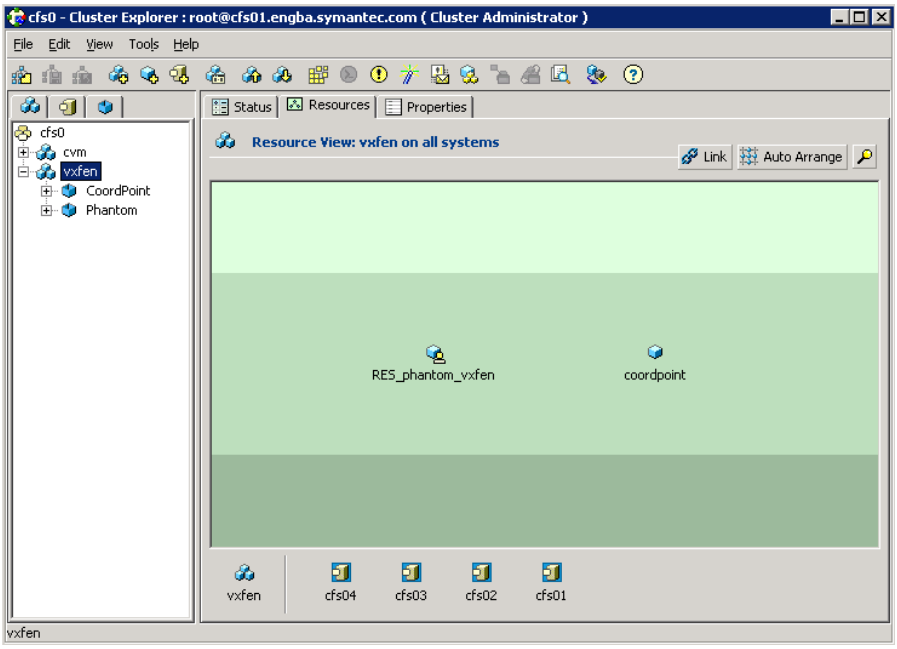
Verify fencing configuration

Once fencing configuration has been finished you can verify it is correct. Query each of the CP Servers to verify each node has been registered.

```
# CCPS_USERNAME=CPSADM@VCS_SERVICES

# CPS_DOMAINTYPE=vx

[root@cfs01 install]# cpsadm -s cps1v -a list_nodes

ClusterName      UUID                                 Hostname(Node ID) Registered

==========   ==================================   ================  ==========

cfs0          {38910d38-1dd2-11b2-a898-f1c7b967fd89}  cfs01(0)          1

cfs0          {38910d38-1dd2-11b2-a898-f1c7b967fd89}  cfs02(1)          1

cfs0          {38910d38-1dd2-11b2-a898-f1c7b967fd89}  cfs03(2)          1

cfs0          {38910d38-1dd2-11b2-a898-f1c7b967fd89}  cfs04(3)          1

[root@cfs01 install]# cpsadm -s cps1v -a list_membership -c cfs0

List of registered nodes: 0 1 2 3

[root@cfs01 install]#
```

The same command can be run against the other CP Servers.

Using the VCS Cluster Explorer screen, we can see that the vxfen service group has been created to monitor CP servers and that it is healthy.



Storage Configuration

There are two options to provide storage to the Virtual Machines (VMs) that will host the Cluster File System. The first option, Raw Device Mapping Protocol (RDMP), uses direct access to external storage and supports parallel access to the LUN, but does not allow vMotion or DRS. For RDMP configuration, you must map the raw device to each VM and make sure you select the Physical (RDM-P) configuration, so SCSI-3 PGR commands are passed along to the disk.

The second option, VMFS virtual disk (VMDK), provides a file that can only be accessed in parallel when the VMFS multi-writer option is enabled. This option supports server vMotion and DRS, but does not currently support SCSI-3 PGR IO fencing. The main advantage of this architecture is the ability to move VMs around different ESX servers without service interruption, using vMotion.

This deployment guide uses VMDK files with the multi-writer option enabled. In this section we will show how to configure the ESX server and virtual machines to share a VMDK file and how to configure SFCFSHA to consume that storage and create a file system.

Support for VMDK files is based on the multi-writer option described in this VMware article:

http://kb.vmware.com/kb/1034165

By default, one VMDK file can only be mounted by one VM at a time. By following the steps in the VMware article, simultaneous write protection provided by VMFS is disabled using the multi-writer flag.

When choosing this configuration, users should be aware of the following limitations and advantages.

Limitations

- Virtual disks must be eager zeroed thick
- VMDK Sharing is limited to eight ESX servers
- Linked clones and snapshots are not supported. Be aware that other vSphere activities utilize cloning and that backup solutions leverage snapshots via the vAPIs, so backups may be adversely impacted.
- SCSI-3 PGR IO fencing is not supported by VMDK files. Special care needs to be taken when assigning VMDKs to VMs. Inadvertently assigning a VMDK file already in use to the wrong VM will likely result in data corruption.
- Storage vMotion is not supported

Advantages

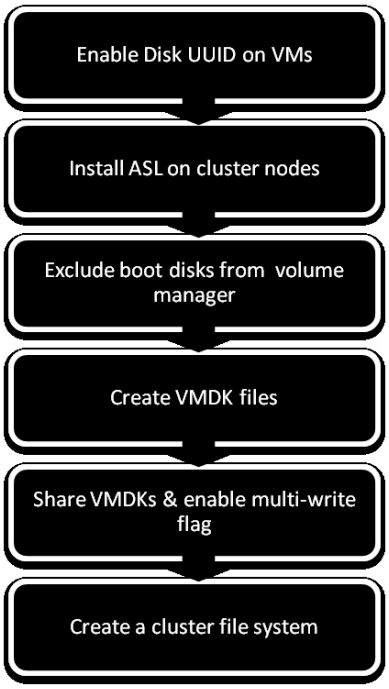
- Server vMotion is supported

The lack of SCSI-3 PGR IO fencing support requires the usage of at least three Coordination Point Servers, to provide non-SCSI-3 fencing protection. In case of a split brain situation, CP Servers will be used to determine what part of the sub-cluster will continue providing service.

Once the multi-writer flag is enabled on a VMDK file, any VM will be able to mount it and write, so special care in the provisioning phase needs to be taken.

Note that if the number of SFCFSHA nodes is greater than eight, several nodes will have to run in the same ESX server, based on the limitation that a maximum of eight ESX servers can share the same VMDK file. For example, if you are running at the SFCFSHA maximum of 64 nodes, those 64 VMs would share the same VMDK file, but you could only use eight ESX servers to host the cluster.

These are the steps that need to be taken when configuring VMDKs as shared backed storage and that will be presented in the next sections:

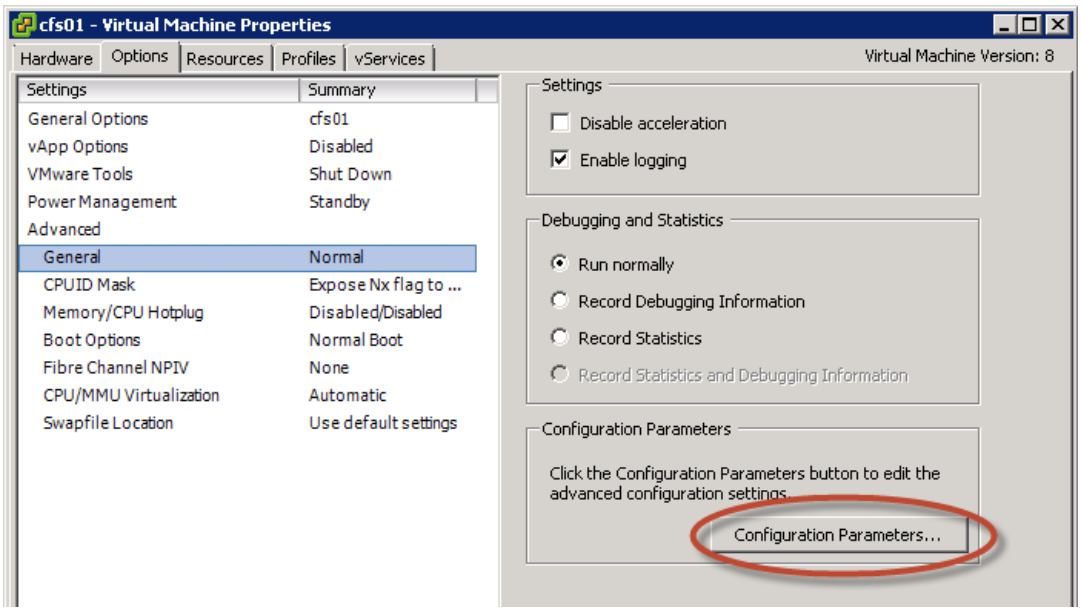


Enable Disk UUID on Virtual Machines

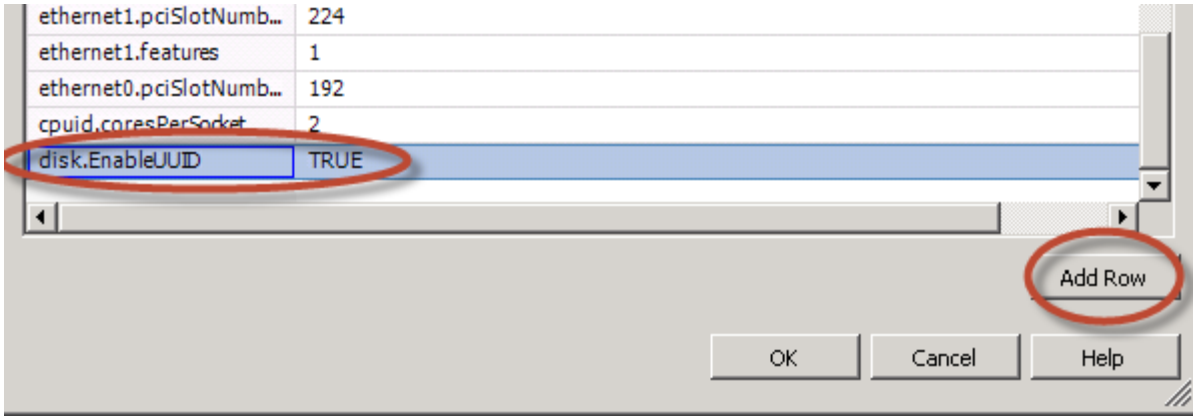
The first step that needs to be taken is to set the **disk.EnableUUID** parameter for each VM to "**TRUE**". This step is necessary so that the VMDK always presents a consistent UUID to the VM, thus allowing the disk to be mounted properly. For each of the nodes (VMs) that will be participating in the cluster, follow these steps:

From vSphere client:

- **Power off** the guest
- Right click on guest and select "**Edit Settings**..."
- Click on "**Options**" tab on top
- Click on "**General**" under the "**Advanced**" section
- Click on the "**Configuration Parameters**.." on right hand side



- Check to see if the parameter "**disk.EnableUUID**" is set, if it is there then make sure it is set to "**TRUE**"
- If not there then click "**Add Row**" and add it.



- **Power on** the guest

Symantec Array Support Library (ASL) for VMDK

In order for the cluster file system to work properly with the VMDK files, an ASL must be installed in the virtual server. The ASL package (VRTSaslapm) version that contains the VMDK ASL is 6.0.100.100. This version is available for downloaded from: http://sort.symantec.com The direct link to this package is: https://sort.symantec.com/asl/details/609

Click on the "Download" (from above direct link) to download this package:

Array Support Library (ASL)/Array Policy Module (APM) Details
VRTSaslapm [Download] - 674 K

To install the package follow the instructions outlined in the Readme file (VRTSaslap_readme.txt) which is displayed towards the end on the above direct link. You can also save this Readme file by clicking on "Save As..." :

Readme file [Save As...]

```
================================================================================

VRTSaslapm package (Array Support Libraries and Array Policy Modules) on

Veritas Volume Manager (tm) 6.0.1 for Linux (SLES and RHEL)

================================================================================
```

These are the steps followed at cfs01 system to install the ASL. Repeat these steps in the other cluster file system nodes.

First, we check the downloaded file got the correct size according to the release notes and we get it ready to install:

```
[root@cfs01 aslapm]# cksum VRTSaslapm_Linux_6.0.100.100.tar.gz
2350318182 689893 VRTSaslapm_Linux_6.0.100.100.tar.gz
[root@cfs01 aslapm]# gunzip VRTSaslapm_Linux_6.0.100.100.tar.gz
[root@cfs01 aslapm]# tar -xvf VRTSaslapm_Linux_6.0.100.100.tar
RHEL5/
RHEL5/VRTSaslapm-6.0.100.100-GA_RHEL5.x86_64.rpm
RHEL6/
RHEL6/VRTSaslapm-6.0.100.100-GA_RHEL6.x86_64.rpm
SLES10/
SLES10/VRTSaslapm-6.0.100.100-GA_SLES10.x86_64.rpm
SLES11/
SLES11/VRTSaslapm-6.0.100.100-GA_SLES11.x86_64.rpm
[root@cfs01 aslapm]#
```

As stated in the release notes, the procedure will differ depending on a previous package was already installed or not. In our case, a GA version was already installed, so an upgrade is the route to be taken:

```
VRTSaslapm-6.0.100.100-GA_RHEL6.x86_64.rpm
[root@cfs01 RHEL6]# rpm -Uvh VRTSaslapm-6.0.100.100-GA_RHEL6.x86_64.rpm
Preparing...                ########################################### [100%]
   1:VRTSaslapm             ########################################### [100%]
Installing keys for APMs
[root@cfs01 RHEL6]# vxdctl enable
[root@cfs01 RHEL6]#
```

Note that in this case, version for RHEL6 was chosen as that is the platform used during this guide development.

Any future updates to the VMDK ASL will be published in http://sort.symantec.com and it will have a higher revision than 6.0.100.100, such as 6.0.100.200.

After installing the ASL, you will notice that the disk has been renamed from disk_0 to vmdk0_0.

Before ASL:

```
# vxdisk list

DEVICE       TYPE            DISK         GROUP        STATUS

disk_0       auto:none       -            -            online invalid
```

After ASL has been deployed:

```
# vxdisk list

DEVICE       TYPE            DISK         GROUP        STATUS

vmdk0_0      auto:none       -            -            online invalid
```

vmdk0_0 is the boot disk that we are going to exclude from Volume Manger configuration

Exclude boot disk from Volume Manager configuration

It is a best practice to exclude the boot disk from Volume Manager. This will allow the shared VMDK files to be configured to use the same name. In order to exclude the disk, run the command vxdmpadm with the name of the boot disk. In our case:

```
[root@cfs01 RHEL6]# vxdmpadm exclude dmpnodename=vmdk0_0
```

And verify that the boot disk is no longer reported under VxVM configuration:

```
[root@cfs01 RHEL6]# vxdisk list

DEVICE       TYPE            DISK         GROUP        STATUS
```

```
[root@cfs01 RHEL6]#
```

VMDK creation

The VMDKs that will be used by SFCFSHA can be created either by the vSphere GUI or using the command line. Using the GUI, there is no control for the name of the file used, and they will be stored under the folder belonging to the VM that is creating the files. We would prefer in this case to control those file names, so we will use the command line to create the following configuration:

Data Store	Virtual Disk on ESX	VMDK Name	Virtual Device	Virtual SCSI Driver	VMDK Size (GB)
DS1	Hard disk 2	cfs0/shared1.vmdk	SCSI 1:0	Paravirtual	90
DS2	Hard disk 3	cfs0/shared2.vmdk	SCSI 1:1	Paravirtual	90
DS3	Hard disk 4	cfs0/shared3.vmdk	SCSI 1:2	Paravirtual	90
DS4	Hard disk 5	cfs0/shared4.vmdk	SCSI 1:3	Paravirtual	90
DS5	Hard disk 6	cfs0/shared5.vmdk	SCSI 1:4	Paravirtual	90

These are the commands used to create that infrastructure:

1. Connect to one of the ESX

2. Create a folder called cfs0 (the name of the cluster) in each of the datastores:

```
mkdir /vmfs/volumes/DS1/cfs0

mkdir /vmfs/volumes/DS2/cfs0

mkdir /vmfs/volumes/DS3/cfs0

mkdir /vmfs/volumes/DS4/cfs0

mkdir /vmfs/volumes/DS5/cfs0
```

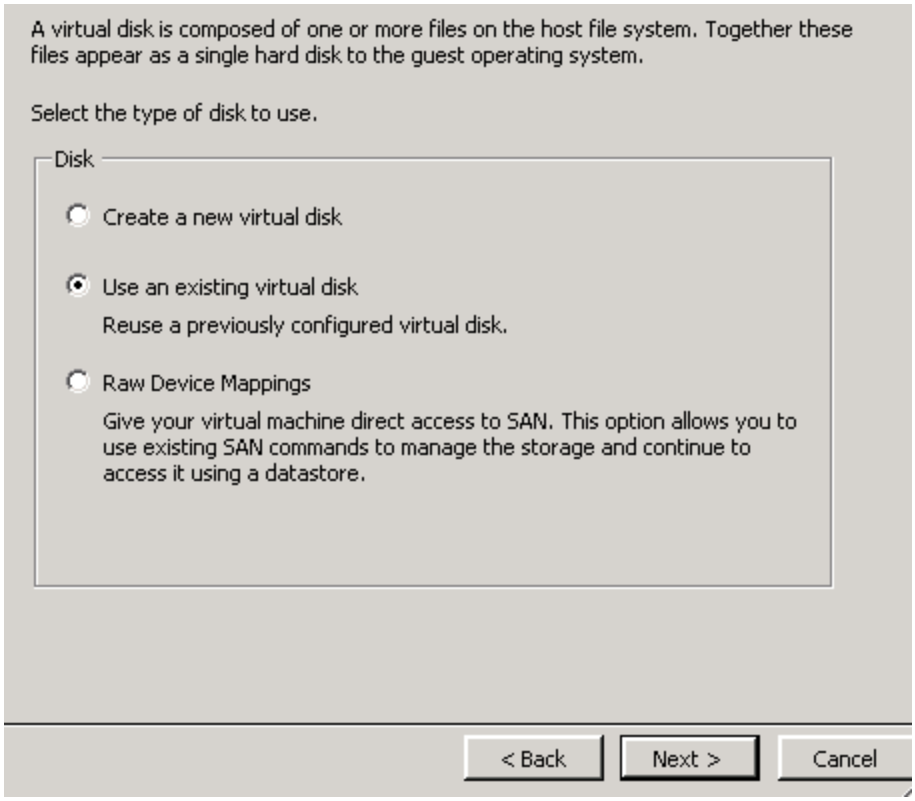
3. Create each of the VMDKs that will be used:

```
vmkfstools -c 90G  -d  eagerzeroedthick  /vmfs/volumes/DS1/cfs0/shared1.vmdk

vmkfstools -c 90G  -d  eagerzeroedthick  /vmfs/volumes/DS2/cfs0/shared2.vmdk

vmkfstools -c 90G  -d  eagerzeroedthick  /vmfs/volumes/DS3/cfs0/shared3.vmdk

vmkfstools -c 90G  -d  eagerzeroedthick  /vmfs/volumes/DS4/cfs0/shared4.vmdk

vmkfstools -c 90G  -d  eagerzeroedthick  /vmfs/volumes/DS5/cfs0/shared5.vmdk
```

Map VMDKs to each VM

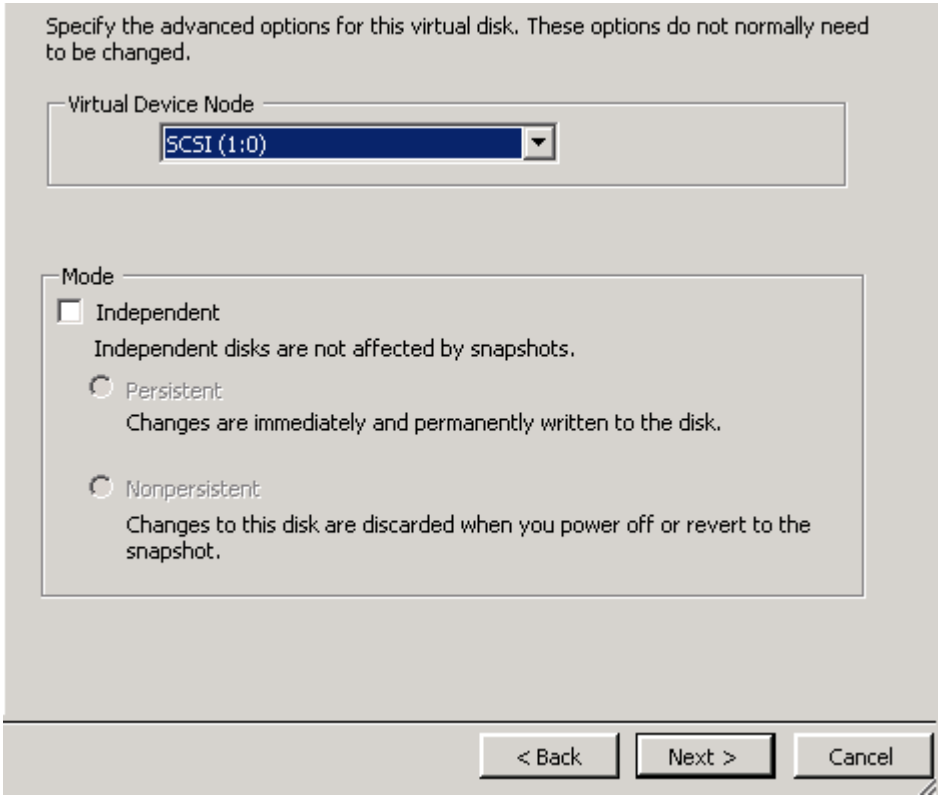
The next step is to map each of the created VMDK files to each VM. We will show the procedure for cfs01 node and all steps should be followed for each of the other nodes.

1. Shut down the guest
2. Right click on guest and select "**Edit Settings**..."
3. Click on "**Add**" and select "**Hard disk**" and click "**Next**"
4. Select "**Use an existing virtual disk**" and click "**Next**"

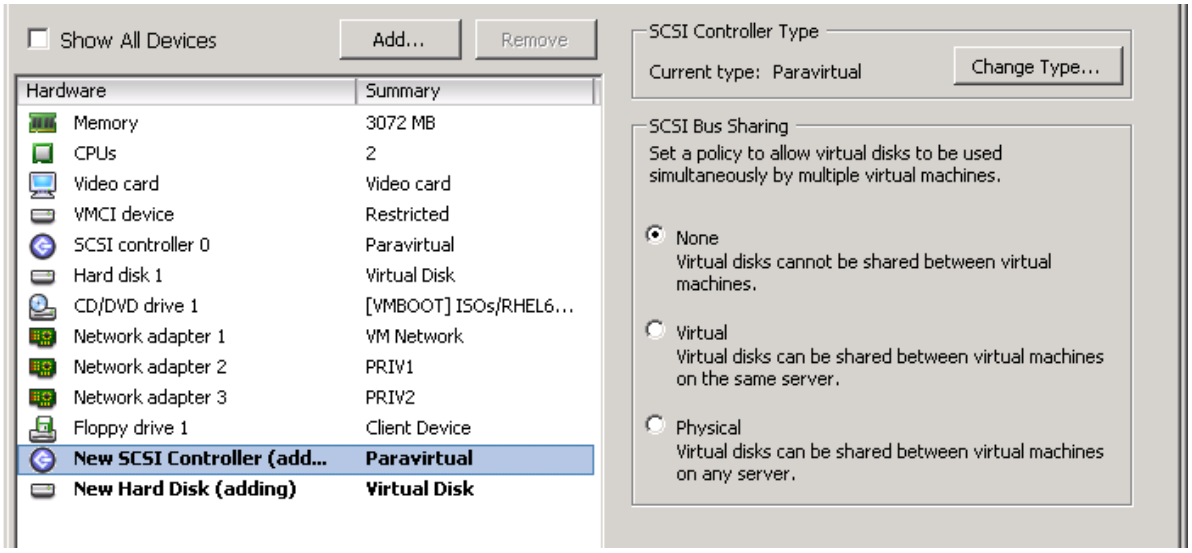


5. Click on "**Browse**" and choose **DS1** data store.
6. Click on folder **cfs0** and select **shared1.vmdk** file
7. Click the "**Next**" button.

8. On Virtual Device Node select **SCSI (1:0)**



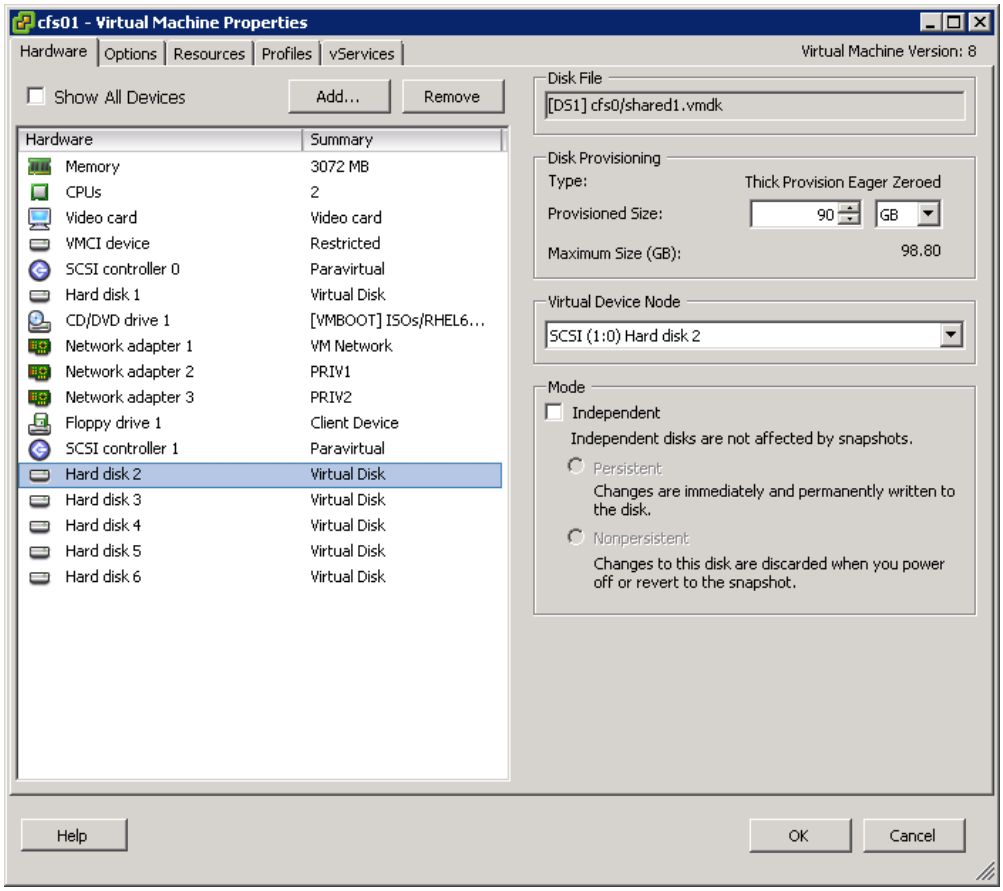
9. Click "Next"
10. Review the details are correct and click on "**Finish**"
11. Note that because this is the first disk added under SCSI controller 1, a new SCSI controller is added. Modify the type to **Paravirtual**, if that is not the default, and check that **SCSI Bus Sharing** is set to "**None**", as this is key to allow vMotion for the VMs.



Follow steps 3 to 10 for the rest of disks that will be added to each of the VMs. In our configuration, this will be parameters for steps 5, 6 and 8:

Data Store	VMDK Name	Virtual Device
DS1	cfs0/shared1.vmdk	SCSI 1:0
DS2	cfs0/shared2.vmdk	SCSI 1:1
DS3	cfs0/shared3.vmdk	SCSI 1:2
DS4	cfs0/shared4.vmdk	SCSI 1:3
DS5	cfs0/shared5.vmdk	SCSI 1:4

This will be the final configuration for the first node of the cluster (cfs01):



Now follow the same steps for each node of the cluster and map each VMDK file to the VM following the instructions above.

Once all the steps are completed, all the VMs should have access to the same VMDK files. Note that at this point, all the VMs are still powered off and that multi-writer flag has not been enabled yet (it will be done in the next step). Any attempt to power on the VMs in this state will prevent a second VM start because it will violate the restrictions to access a VMDK by only a host at a time.

Enabling the multi-write flag

For a detailed instruction about how to enable the multi-writer flag, please follow the steps in the following VMware article:

http://kb.vmware.com/kb/1034165

Below are the steps taken in our lab environment during the configuration.

Remember that so far we have configured five VMDK files that are shared by four VMs (the four nodes of the cluster) and that the VMs are powered off. Now it is time to enable the multi-writer flag for each of the VMs. These are the steps that need to be taken:

1. On the vSphere Client, right-click on the **cfs01** virtual machine. Go to "**Edit Settings**", then click on the "**Options**" tab. Click on "**General**" under the "**Advanced**" option. Press the "**Configuration Parameters…**" button.
2. Click on the "**Add Row**" button.
3. Enter **scsi1:0.sharing** on the Name column
4. Enter **multi-writer** on the Value column
5. Repeat steps 2 through 4 and enter the multi-writer value for the rest of the SCSI controllers and targets. In our case:

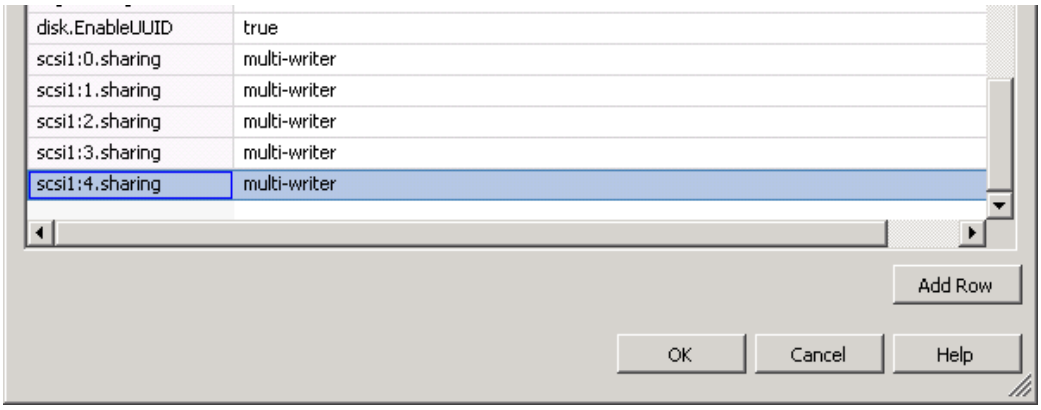
   scsi1:1.sharing multi-writer

   scsi1:2.sharing multi-writer

   scsi1:3.sharing multi-writer

   scsi1:4.sharing multi-writer

6. Once those steps are done, the VM configuration will look like this:



7. Press OK

Now repeat steps 1 to 7 for the other virtual machines (cfs02, cfs03 and cfs04 in our configuration)

Once all the virtual machines have been configured correctly, power them on and check that there are no issues.

Note that the disks have been added to each of the hosts. This is the configuration for cfs01:

```
[root@cfs01 ~]# vxdisk list
DEVICE       TYPE            DISK         GROUP        STATUS
vmdk0_1      auto:none       -            -            online invalid
vmdk0_2      auto:none       -            -            online invalid
vmdk0_3      auto:none       -            -            online invalid
vmdk0_4      auto:none       -            -            online invalid
vmdk0_5      auto:none       -            -            online invalid
[root@cfs01 ~]#
```

Get consistent names across nodes

It is likely that the VMDK files are presented in a different order on each system and that the name given by Volume Manager may vary. To have a consistent deployment it is recommended to rename the disk so the configuration is clear. Here one example of initial discrepancies between cfs01 and cfs03:

At cfs01 the disk name associated to device ending on serial number 226 is vmdk0_5::

```
[root@cfs01 ~]# /etc/vx/bin/vxgetdmpnames
enclosure vendor=VMware product=disk serial=vmdk name=vmdk0
        dmpnode serial=6000c2993a8d6030ddf71042d4620cec name=vmdk0_1
        dmpnode serial=6000c29ac083abd0a86fa46b509d69f5 name=vmdk0_2
        dmpnode serial=6000c29e13f6aff58ac3d543b022dfe2 name=vmdk0_3
        dmpnode serial=6000c29f2447768317937e574e6ca1bb name=vmdk0_4
        dmpnode serial=6000c297c0411b0c0c201dff6a720226 name=vmdk0_5
```

And observe how cfs03 named the same device vmdk_0_0:

```
[root@cfs03 ~]# /etc/vx/bin/vxgetdmpnames
enclosure vendor=VMware product=disk serial=vmdk name=vmdk0
        dmpnode serial=6000c297c0411b0c0c201dff6a720226 name=vmdk0_0
        dmpnode serial=6000c2993a8d6030ddf71042d4620cec name=vmdk0_1
        dmpnode serial=6000c29ac083abd0a86fa46b509d69f5 name=vmdk0_2
        dmpnode serial=6000c29e13f6aff58ac3d543b022dfe2 name=vmdk0_3
        dmpnode serial=6000c29f2447768317937e574e6ca1bb name=vmdk0_4
```

In order to get the same names across all the cluster nodes the command vxddladm is used For each node of the cluster, run the command:

```
# vxddladm assign names
```

Observe now how cfs03 got the right name for device ending at 226 serial number:

```
[root@cfs03 ~]# /etc/vx/bin/vxgetdmpnames
enclosure vendor=VMware product=disk serial=vmdk name=vmdk0
        dmpnode serial=6000c2993a8d6030ddf71042d4620cec name=vmdk0_1
        dmpnode serial=6000c29ac083abd0a86fa46b509d69f5 name=vmdk0_2
        dmpnode serial=6000c29e13f6aff58ac3d543b022dfe2 name=vmdk0_3
        dmpnode serial=6000c29f2447768317937e574e6ca1bb name=vmdk0_4
        dmpnode serial=6000c297c0411b0c0c201dff6a720226 name=vmdk0_5
```

Creating a Clustered File System

The next step will be to configure a common mount point across all the nodes, mounted on the same storage. In order to simplify the examples given here, a single disk group containing all the disks and a single volume will be created. Depending on the application requirements the number of disk groups and volumes may vary.

The boot disk has been excluded from Volume Manger configuration, so the 5 available disks (vmdk0_1, vmdk0_2, vmdk0_3, vmdk0_4 and vmdk0_5) will be the ones added to the disk group. These are the steps:

1. Initialize the disks:

```
[root@cfs01 ~]# vxdisksetup -i vmdk0_1
[root@cfs01 ~]# vxdisksetup -i vmdk0_2
[root@cfs01 ~]# vxdisksetup -i vmdk0_3
[root@cfs01 ~]# vxdisksetup -i vmdk0_4
[root@cfs01 ~]# vxdisksetup -i vmdk0_5
[root@cfs01 ~]#
```

2. Create a new disk group and add the disks

```
[root@cfs01 ~]# vxdg -s init dg01 disk01=vmdk0_1
[root@cfs01 ~]# vxdg -g dg01 adddisk disk02=vmdk0_2
[root@cfs01 ~]# vxdg -g dg01 adddisk disk03=vmdk0_3
[root@cfs01 ~]# vxdg -g dg01 adddisk disk04=vmdk0_4
[root@cfs01 ~]# vxdg -g dg01 adddisk disk05=vmdk0_5
[root@cfs01 ~]#
```

3. Verify the configuration. Note the DISK and GROUP information

```
[root@cfs01 ~]# vxdisk list
DEVICE       TYPE            DISK         GROUP        STATUS
vmdk0_1      auto:cdsdisk    disk01       dg01         online shared
vmdk0_2      auto:cdsdisk    disk02       dg01         online shared
vmdk0_3      auto:cdsdisk    disk03       dg01         online shared
vmdk0_4      auto:cdsdisk    disk04       dg01         online shared
vmdk0_5      auto:cdsdisk    disk05       dg01         online shared
[root@cfs01 ~]#
```

4. Create a striped volume with the 5 disks available

```
[root@cfs01 ~]# vxassist -g dg01 make data01 maxsize layout=stripe disk01 disk02
 disk03 disk04 disk05
[root@cfs01 ~]#
```

5. Create a File System

```
[root@cfs01 ~]# mkfs -t vxfs /dev/vx/rdsk/dg01/data01
    version 9 layout
    942845952 sectors, 471422976 blocks of size 1024, log size 65536 blocks
    rcq size 8192 blocks
    largefiles supported
[root@cfs01 ~]#
```

6. Add the newly created file system to the cluster configuration. Given that this will be mounted by all the nodes at the same time, we will add it as a cluster resource, and commands cfsmntadm and cfsmount will be used

```
[root@cfs01 ~]# cfsmntadm add dg01 data01 /data01 all=crw
  Mount Point is being added...
  /data01 added to the cluster-configuration
[root@cfs01 ~]# cfsmount /data01
  Mounting...
  [/dev/vx/dsk/dg01/data01] mounted successfully at /data01 on cfs01
  [/dev/vx/dsk/dg01/data01] mounted successfully at /data01 on cfs02
  [/dev/vx/dsk/dg01/data01] mounted successfully at /data01 on cfs03
  [/dev/vx/dsk/dg01/data01] mounted successfully at /data01 on cfs04
[root@cfs01 ~]#
```

7. Finally, verify that the new directory is available in all the nodes by running the `cfscluster status` command or by verifying with `df` in each of the nodes

Appendix A: Coordination Point Server Configuration

This appendix will show how to configure a Coordination Point Server (CPS). In our deployment, three CPS are used. Each CPS will be housed in a virtual machine, with each one forming a single node CPS cluster. Each of our two physical ESX Servers will contain one CPS, and a third CPS will be located in another location.

Here we will show how to deploy **cps1**.

Pre-requisites

The installer script will be used to perform the deployment of Veritas Cluster Server (option 2). When running the Pre-Installation Check, the following packages will be detected as not installed:

```
CPI ERROR V-9-30-2225 The following required OS rpms (or higher version) were
not found on cfs01:
        nss-softokn-freebl-3.12.9-3.el6.i686 glibc-2.12-1.25.el6.i686
pam-1.1.1-8.el6.i686 libstdc++-4.4.5-6.el6.i686 libgcc-4.4.5-6.el6.i686
ksh-20100621-6.el6.x86_64
```

The requirement for those missing packages SF 6.0 and 6.0.1 on RHEL 6.2/6.3 is documented under article TECH196954:

http://www.symantec.com/business/support/index?page=content&id=TECH196954

The document lists the following packages to be installed before deploying Storage Foundation:

glibc-2.12-1.25.el6.i686
libgcc-4.4.5-6.el6.i686
libstdc++-4.4.5-6.el6.i686
nss-softokn-freebl-3.12.9-3.el6.i686

We are deploying on top of RedHat 6.2, and these are the RPMs installed:

rpm -ivh --nodeps glibc-2.12-1.47.el6.i686.rpm
rpm -ivh --nodeps libgcc-4.4.6-3.el6.i686.rpm
rpm -ivh --nodeps libstdc++-4.4.6-3.el6.i686.rpm
rpm -ivh --nodeps nss-softokn-freebl-3.12.9-11.el6.i686.rpm
rpm -ivh --nodeps pam-1.1.1-10.el6.i686.rpm
rpm -ivh --nodeps ksh-20100621-12.el6.x86_64.rpm

Verify that CP Servers can listen on port 14250. Disable the firewall rules or enter a new rule as explained at the beginning of this document to allow communication to this port

Verify that the CP Servers have Password-less SSH connection to the cluster node where fencing configuration will be run.

Veritas Cluster Server single node configuration

Run the installer script and perform a **Pre-Installation Check** to verify that the server is ready to have VCS installed, then press option 1 for **Install a Product**

```
    Storage Foundation and High Availability Solutions 6.0.1 Install Program

     1)  Veritas Dynamic Multi-Pathing (DMP)
     2)  Veritas Cluster Server (VCS)
     3)  Veritas Storage Foundation (SF)
     4)  Veritas Storage Foundation and High Availability (SFHA)
     5)  Veritas Storage Foundation Cluster File System HA (SFCFSHA)
     6)  Symantec VirtualStore (SVS)
     7)  Veritas Storage Foundation for Sybase ASE CE (SFSYBASECE)
     8)  Veritas Storage Foundation for Oracle RAC (SF Oracle RAC)
     b)  Back to previous menu

Select a product to install: [1-8,b,q] 2
```

Select option 3 to install all RPMs so that the VRTScps package will be included:

```
                Veritas Cluster Server 6.0.1 Install Program

     1)  Install minimal required rpms - 274 MB required
     2)  Install recommended rpms - 456 MB required
     3)  Install all rpms - 478 MB required
     4)  Display rpms to be installed for each option

Select the rpms to be installed on all systems? [1-4,q,?] (2) 3
```

Enter the name of the host where you are running the configuration, **cps1** in this example. After reviewing all the packages that will be installed, the package installation will start.

In our environment, keyless licensing will be used because a Veritas Operation Manager host is deployed, so option 2 will be our option for licensing.

Global Cluster Option will not be enabled. And the next step will be to configure VCS, so we type "**y**":

```
                Veritas Cluster Server 6.0.1 Install Program
                                cps1

Would you like to enable the Global Cluster Option? [y,n,q] (n)

Registering VCS license
VCS vxkeyless key (VCS) successfully registered on cps1

Would you like to configure VCS on cps1? [y,n,q] (n) y
```

Given this is a single node cluster, I/O fencing will not be enabled:

```
If you do not enable I/O Fencing, you do so at your own risk

See the Administrator's Guide for more information on I/O Fencing

Do you want to configure I/O Fencing in enabled mode? [y,n,q,?] (y) n
```

The next step is important, because although configuring a single node, LLT and GAB must be enabled in order for CPS clients to connect to the CPS server. Therefore, answer **"y"** to the following question:

```
If you plan to run VCS on a single node without any need for adding cluster node
online, you have an option to proceed without starting GAB and LLT. Starting GAB
and LLT is recommended.

Do you want to start GAB and LLT? [y,n,q] (y) y
```

We enter the cluster name (same as node): **cps1**

Select configure heartbeat links using LLT over Ethernet

```
                Veritas Cluster Server 6.0.1 Configure Program
                                    cps1

     1)  Configure heartbeat links using LLT over Ethernet
     2)  Configure heartbeat links using LLT over UDP
     b)  Back to previous menu

How would you like to configure heartbeat links? [1-2,b,q,?] (1) 1
```

In our case an additional NIC had to be configured. That NIC will be used for the private network and must be configured. This step is necessary even with a single node cluster. Enter a unique cluster ID that is not already in use.

```
    Discovering NICs on cps1 ......................... Discovered eth4 eth5

Enter the NIC for the first private heartbeat link on cps1: [b,q,?] (eth5)
Would you like to configure a second private heartbeat link? [y,n,q,b,?] (y) n
Enter the NIC for the low-priority heartbeat link on cps1: [b,q,?] (eth4)
    Checking media speed for eth5 on cps1 ....................... 10000Mb/s

Enter a unique cluster ID number between 0-65535: [b,q,?] (41146)
```

Then the installer will verify that the cluster ID is not already in use:

```
The cluster cannot be configured if the cluster ID 41146 is in use by another
cluster. Installer can perform a check to determine if the cluster ID is
duplicate. The check will take less than a minute to complete.

Would you like to check if the cluster ID is in use by another cluster? [y,n,q]
(y) y

    Checking cluster ID ..... Done

Duplicated cluster ID detection passed. The cluster ID 41146 can be used for the
cluster.

Press [Enter] to continue:
```

We do not enter a Virtual IP, as the same one used for the host will be ok.

The following answer will depend on your needs. In our environment, we have configured SFCFSHA to use secure mode, so the Coordination Point Servers must also use secure mode.

```
                Veritas Cluster Server 6.0.1 Install Program
                                    cps1

Veritas Cluster Server can be configured in secure mode

Running VCS in Secure Mode guarantees that all inter-system communication is
encrypted, and users are verified with security credentials.

When running VCS in Secure Mode, NIS and system usernames and passwords are used
to verify identity. VCS usernames and passwords are no longer utilized when a
cluster is running in Secure Mode.

Would you like to configure the VCS cluster in secure mode? [y,n,q,?] (n) y
```

The FIPS option has not been qualified yet with CP Servers, therefore secure mode without fips will be used. This also matches the configuration done for the cluster nodes.

```
Would you like to configure the VCS cluster in secure mode? [y,n,q,?] (n) y
     1)  Configure the cluster in secure mode without fips
     2)  Configure the cluster in secure mode with fips
     b)  Back to previous menu

Select the option you would like to perform [1-2,b,q] (1) 1
```

We are not using SMTP, nor SNMP notifications

At this point the VCS configuration will start. Once it is completed, we can verify VCS is running:

```
[root@cps1 rhel6_x86_64]# hastatus -sum

-- SYSTEM STATE
-- System               State                Frozen

A  cps1                 RUNNING              0
[root@cps1 rhel6_x86_64]#
```

Coordination Point Server Service Group Configuration

Even in a single node cluster, a virtual IP address (VIP) will be used. This will allow the creation of a VCS resource to control its availability. A VIP for each CP Server has been assigned. Verify that you have a VIP available for each of your CP Servers.

To configure CPS run the command:

```
# /opt/VRTS/install/installvcs601 -configcps
```

The installer will verify that we want to configure a CP Server:

```
                Veritas Cluster Server 6.0.1 Configure Program

Cluster information verification:

        Cluster Name: cps1

        Cluster ID Number: 34864

        Systems: cps1

Would you like to configure CP Server on the cluster? [y,n,q] y
```

As we are deploying a single node cluster, option 1 will be our choice:

```
                Veritas Cluster Server 6.0.1 Configure Program

     1)  Configure Coordination Point Server on single node VCS system
     2)  Configure Coordination Point Server on SFHA cluster
     3)  Unconfigure Coordination Point Server

Enter the option: [1-3,q] 1
```

The name of the CP Server will be the same one as the hostname plus “v” at the end, for our first CP Server it will be **cps1v**

We will enter our Virtual IP address associated to cps1 single node cluster, which will be 10.182.99.124 and we will accept the default port suggested.

As discussed before, security will be enabled:

```
Enter the name of the CP Server: [b] cps1v

Enter valid IP addresses for Virtual IPs for the CP Server, separated by space:
[b] 10.182.99.124

Enter corresponding port number for each Virtual IP address in the range [49152,
65535], separated by space, or simply accept the default port suggested: [b]
(14250)

Symantec recommends secure communication between the CP server and application
clusters. Enabling security requires Symantec Product Authentication Service to
be installed and configured on the cluster. Do you want to enable Security for
the communications? [y,n,q,b] (y) y
```

The database will be installed locally, so the default location will be good:

```
CP Server uses an internal database to store the client information.
As the CP Server is being configured on a single node VCS, database can reside
on local file system.

Enter absolute path of the database: [b] (/etc/VRTScps/db)
```

After reviewing the configuration parameters we continue with the configuration of the CP Server Service Group. The NIC used at cps1 is eth4 and in our case we are not using NetworkHosts. Enter the netmask and configuration will be completed:

```
Configuring CP Server Service Group (CPSSG) for this cluster

Enter a valid network interface on cps1 for NIC resource - 1: eth4

Symantec recommends configuring NetworkHosts attribute to ensure NIC resource to
be always online
Do you want to add NetworkHosts attribute for the NIC device eth4 on system
cps1? [y,n,q] n

Enter the netmask for virtual IP 10.182.99.124: (255.255.240.0)

    Updating main.cf with CPSSG service group ..... Done

Successfully added the CPSSG service group to VCS configuration.

Trying to bring CPSSG service group ONLINE and will wait for upto 120 seconds

The Veritas Coordination Point Server is ONLINE

The Veritas Coordination Point Server has been configured on your system.

Would you like to send the information about this installation to Symantec to
help improve installation in the future? [y,n,q,?] (y)
```

The CPSSG Service Group is now online:

```
[root@cps1 rhel6_x86_64]# hastatus -sum

-- SYSTEM STATE
-- System               State                Frozen

A  cps1                 RUNNING              0

-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State


B  CPSSG           cps1                 Y          N               ONLINE

[root@cps1 rhel6_x86_64]#
```

Appendix B: Enable password-less SSH/RSH

Password-less SSH/RSH is required on nodes in the following scenarios:

- The node where a reconfiguration is happening and the rest of the nodes
- The node where fencing is being configured and the CP Servers
- The CP Servers and the node where fencing is being configured

These are the steps to enable Password-less SSH between “client” and “server”:

```
[client~]# cd /root
[client~]# SSH-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/root/.SSH/id_dsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.SSH/id_dsa.
Your public key has been saved in /root/.SSH/id_dsa.pub.
The key fingerprint is:
38:53:48:cf:41:53:f9:b7:d9:ba:08:51:d9:39:0e:31 root@seintcfsG01n1
[client~]#

[client~]# cd /root/.SSH

[client.SSH]# scp id_dsa.pub server:/root/id_dsa_node1.pub
The authenticity of host 'server (10.182.162.33)' can't be established.
RSA key fingerprint is 8d:ac:75:6f:23:8b:b5:e7:0a:ac:dd:32:6c:23:cb:2f.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'server,10.182.162.33' (RSA) to the list of known
hosts.
root@server's password:
id_dsa.pub
100%  608     0.6KB/s   00:00
[client.SSH]#

[client.SSH]# SSH server
root@server's password:
Last login: Sat Apr  2 04:42:57 2011 from 172.19.75.91

[server~]#
[server~]# mkdir /root/.SSH
[server~]# cd /root/.SSH

[server.SSH]# cat /root/id_dsa_node1.pub >> /root/.SSH/authorized_keys

[server.SSH]# exit
logout
Connection to server closed.
```

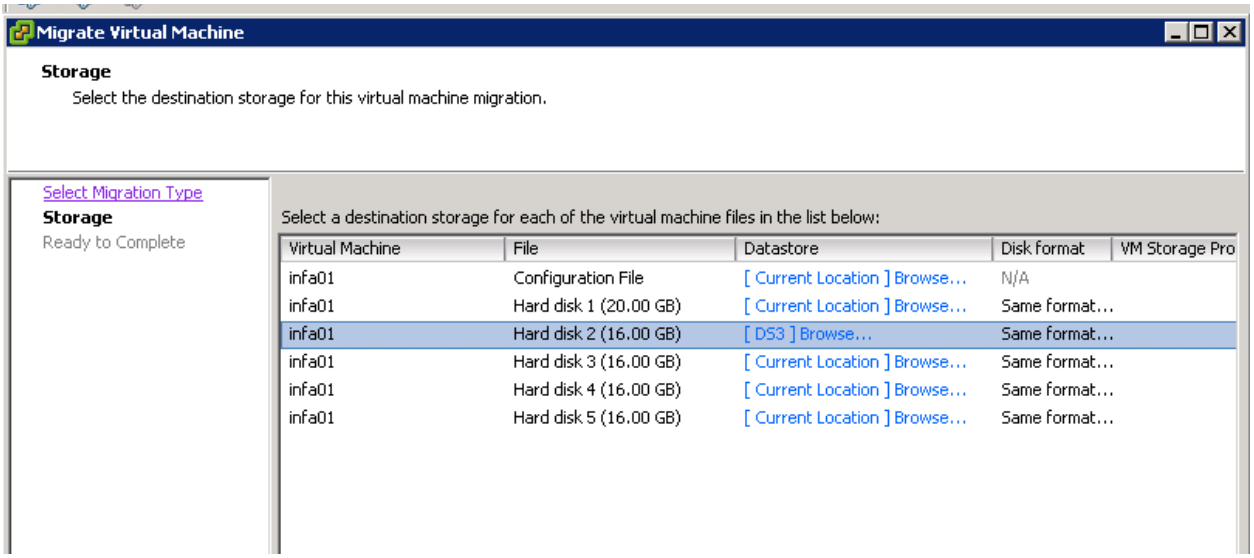
Test that SSH works fine:

```
[client.SSH]# SSH server uname -a
Linux server 2.6.18-194.el5 #1 SMP Tue Mar 16 21:52:39 EDT 2010 x86_64 x86_64
x86_64 GNU/Linux
[client.SSH]#
```

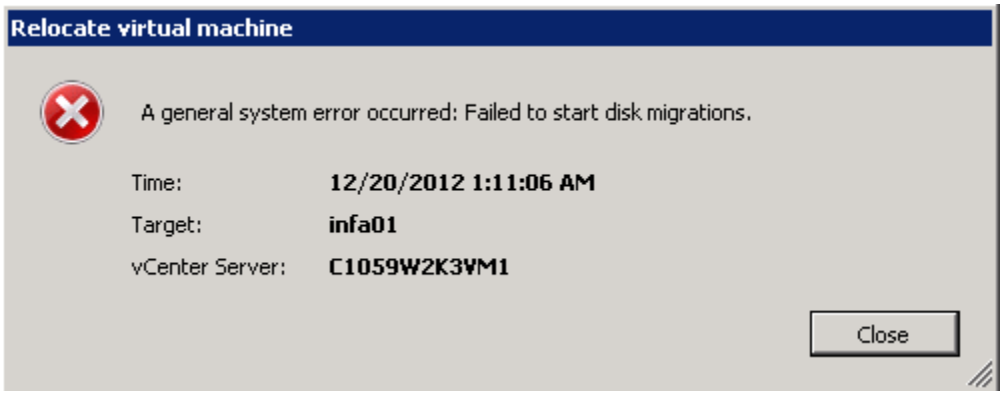
Appendix C: Known Issues & Limitations

Prevention of Storage vMotion

In a configuration where VMDK files are used with the multi-writer flag, any attempt of migrating the VMDK file to another data store will be prevented with an error.



The operation is unable to succeed:



In order to migrate VMDK to different storage, SFCFSHA functionalities can be used to transparently migrate data between different disks.

Need to enable LLT and GAB on CP Servers

When using CP Servers, even if they are running in a single node cluster, The cluster LLT and GAB protocols must be enabled. If not, the CP Clients (cluster nodes) will not be able to communicate properly with the CP Servers. The following error will be shown during configuration:

```
[root@cfs01 install]# cpsadm -s cps1 -a ping_cps
Connection failed for host cps1 on port 14250
Failed to create connection
Error in connecting with CPS
[root@cfs01 install]#
```

Resolution: Configure the CP Servers with LLT and GAB enabled.