SUPPORT DOCUMENT

NetApp 7-Mode Data ONTAP Upgrade Procedure

Ian Daniel | DCO Design & Engineering – Storage Designer
18th August 2015

Synopsis
This document describes the TR Data ONTAP 7-Mode upgrade process within TR..

Document Version
V2.0

Contributors
Gunasekar Venkatraman

Document Status
Distributable (Draft)

Internal/External Use
Internal and Support & Engineering only

THOMSON REUTERS

1 Contents

This test plan contains the following sections:

1.1 Introduction

This document gives an overview of upgrading the ONTAP versions specific to the current TR environment. This document also helps to familiarizing you with requirements and issues before you upgrade (ONTAP/Shelves/Disks)

1.2 Objectives

The objectives are as follows:

- To define the TR upgrade process for NetApp Data ONTAP Upgrades.

1.3 References

No.	Document	URL	Date	Author
1	NetApp Release Notes (8.2.3)	https://library.netapp.com/ecm/ecm_get_file/ECMP12365050	N/A	NetApp
2	NetApp 8.2 Upgrade Guide	https://library.netapp.com/ecm/ecm_get_file/ECMP1511541	N/A	NetApp
3				

1.4 Pre-requisites

Prior to undertaking any upgrade activities a signed off Change Request must be in place. Upgrade activities should be staged to ensure that downtime is kept to a minimum. It is recommended to upgrade disk and shelf firmware prior to any upgrade activity via an appropriate Change Request.

2 Upgrade Options

There are two types of upgrade method available and this are named as per the availability of the client service during the Data ONTAP upgrade process.

2.1 Disruptive Upgrade

When storage services are disrupted during takeover/giveback operations:

a. State information is lost
b. User/application must restart the operation,

It is deemed a **Disruptive Upgrade**.

Upgrades might be disruptive if any of the following conditions are true:

- If storage systems are actively serving CIFS to clients. Because CIFS is session-oriented, sessions must be terminated before upgrade procedures to prevent data loss and client must re-establish the sessions.
- If a storage system actively serving File Transfer Protocol (FTP) or Network Data Management Protocol (NDMP) clients that cannot be postponed - State is lost, client must retry operations.
- Backups and Restores – State is lost, client must retry operations.
- AT-FCX FW 36 and prior versions:

  Any update of these versions of FW, on either of the AT-FCX modules installed, is disruptive and will result in a minimum 70-second outage and could be substantially more, depending on system configuration.

  This rule applies even with Data ONTAP 7.3.1 and Multi-Path cabling in place
- Disk firmware updates automatically take disks in RAID4 aggregates offline until the update is complete. Services and data are unavailable until they are back online. (But in RAID_DP it is non-disruptive). It is always recommended to convert RAID4 to RAID_DP before upgrading the Data ONTAP version.
- If the application/client doesn't have the timeout value correctly set which means it will expire prior to the upgrade completing.

2.2 Non-Disruptive upgrade (NDU)

System NDU is a mechanism that takes advantage of active/active controller technology to minimize client disruption during a rolling upgrade of Data ONTAP or controller firmware. This procedure allows each node of active/active controllers to be upgraded individually to a newer version of Data ONTAP or firmware. Minor release NDU was first supported in Data ONTAP 6.5.1. Major release NDU is now supported from Data ONTAP 7.0.6 and 7.1.2 to 7.2.3 and higher.

Major NDU Components:

- System NDU
    a. End-user-performable process that takes advantage of Active/Active takeover and giveback operations
    b. Maintains data service availability during upgrade reboots
- Disk firmware NDU
    a. Utilizes momentary disk offline technology
    b. Supported for volumes and aggregates employing RAID-DP or SyncMirror® software
- Shelf firmware NDU
    a. Dependent on LRC or ESH-based shelves:
    b. Not supported for AT-FC or AT-FC2
- AT-FCX module and SAS enclosure FW upgrades
    a. AT-FCX incurs two 70-sec pauses in I/O
    b. SAS incurs two 40-sec pauses in I/O
    Both are sustainable by many NFS or iSCSI-attached applications.

Types of system NDUs:

Major
A major version system NDU is an upgrade from one major release of Data ONTAP to another. For major release NDU, the NVRAM and file system layout can change. Consequently, controller takeover functionality is disabled while the 2 nodes are on different major releases

For example, an upgrade from Data
ONTAP 8.1.x to Data ONTAP 8.2.x is considered a major system NDU.

Minor
A minor version system NDU is an upgrade within the same release family. For example, an upgrade from Data ONTAP 8.1.1 to Data ONTAP 8.1.3 is considered a minor system NDU.

The following are things that constitute a minor version system NDU:

- No version number change to RAID, WAFL®, NVLOG, FM, or SANOWN
- No change to NVRAM format
- No change to on-disk format

- Automatic takeover must be possible while the two controllers of the HA pair are running different versions within the same release Family.

For additional information, see the Data ONTAP Release Model available on NOW (NetApp on the Web).

Hardware requirements for NDU:

- System NDU is supported on any NetApp FAS series.
- Systems must be cabled and configured in an HA pair controller configuration. This includes all InfiniBand interconnect cables, proper NVRAM slot assignments, and appropriate controller-to-shelf cabling, including (as applicable) multipath high-availability storage.

Software Requirements for NDU:

Predictable takeover and giveback performance is essential to a successful NDU.
It is important not to exceed Data ONTAP configuration limits. Flexvol limits per storage controller can be found from,

https://now.netapp.com/NOW/knowledge/docs/ontap/ontap_index.shtml (select the Ontap version)

Under that search for “Storage Management Guide” → this has all the flexvol limitations.

3 Steps To Complete Before Upgrade

3.1 Check List

Following checks are required before performing a major or minor system NDU.All the below methods/tools helps to find/fix the issue prior to the actual upgrade process,

1. Check Filer Interfaces
2. Use Upgrade Advisory
3. Use HA Configuration Checker and NetApp rc_check (entry order)
4. Remove all failed disks
5. Verify system load
6. Synchronize date and time
7. Verify the connectivity to the storage controller
8. DR/Data Production consideration
9. Determining latest Firmware for Shelves/Disks
   A. Upgrading Shelves
   B. Upgrading Disks
10. Check for all Vfiler status
11. Check for stale fingerprint and utilization of infra volumes
12. Exports entry check for VM volumes
13. Exports check script
14. File Handle check script
15. IP Space check
16. Perfstat collection

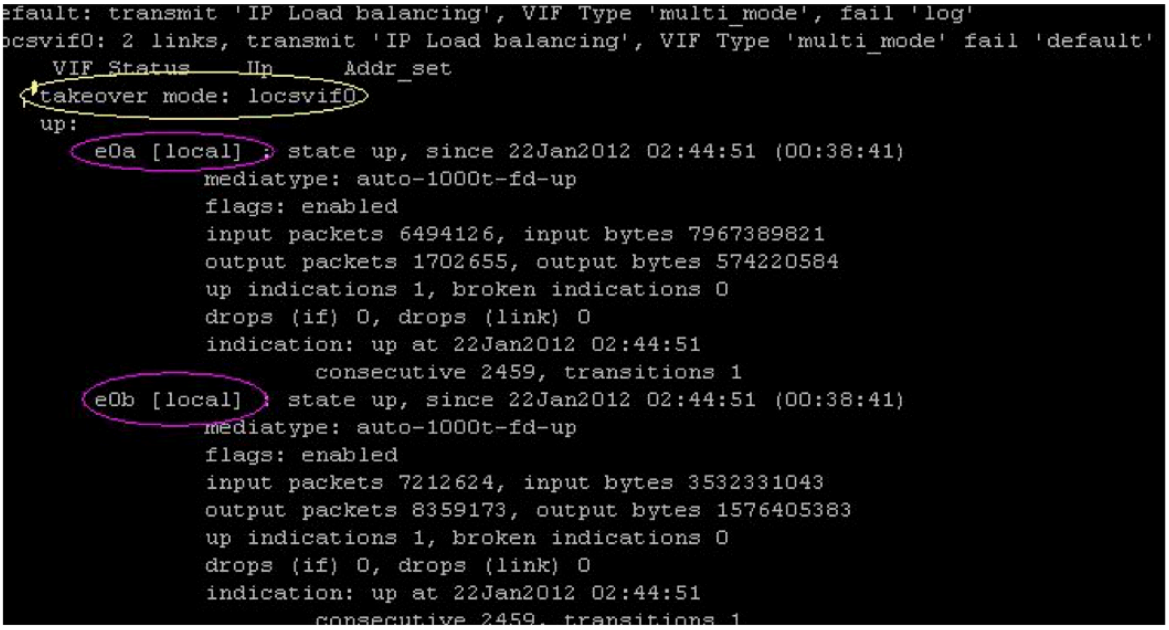
Note: Please complete the following pre-checks before performing the Giveback during the upgrade or any maintenance activity (Flow control changes).

3.1.1 Check Filer Interfaces

Check the filer interface status (Use the following commands and look for few areas to confirm the status of the interfaces, Commands: go to 'partner' and type "`ifconfig -a`" and check for the interfaces status (up /down)

```
nas6040b/nas6040b-2> ifconfig -a
e0f: flags=0x6de8867<UP,BROADCAST,RUNNING,MULTICAST,MULTIHOST,PARTNER_UP,TCPCKSUM,NOWINS> mtu 1500
        inet 10.226.14.73 netmask-or-prefix 0xffffff00 broadcast 10.226.14.255
        takeover mode (e0f)
        ether 00:a0:98:0f:5e:27 (auto-1000t-fd-up) flowcontrol full
lo: flags=0x19e8049<UP,LOOPBACK,RUNNING,MULTICAST,MULTIHOST,PARTNER_UP,TCPCKSUM> mtu 8160
        inet 127.0.0.1 netmask-or-prefix 0xff000000 broadcast 127.0.0.1
        takeover mode (lo)
        ether 00:00:00:00:00:00 (VIA Provider)
locsvif0: flags=0x22de8863<UP,BROADCAST,RUNNING,MULTICAST,MULTIHOST,PARTNER_UP,TCPCKSUM> mtu 1500
        inet 10.225.48.95 netmask-or-prefix 0xfffffc00 broadcast 10.225.51.255
        takeover mode (locsvif0)
        ether 02:a0:98:0f:5e:22 (Enabled virtual interface)
uilvif1: flags=0x22de8863<UP,BROADCAST,RUNNING,MULTICAST,MULTIHOST,PARTNER_UP,TCPCKSUM> mtu 1500
        inet 10.225.17.139 netmask-or-prefix 0xffffff80 broadcast 10.225.17.255
        takeover mode (uilvif1)
        ether 02:a0:98:0f:5e:23 (Enabled virtual interface)
```

Please Note: only the interfaces, which are up, will be show up and the interfaces, which are down, will not be visible here. Need to reconfirm with another command: "`ifgrp status`" to find the exact status of the interfaces,



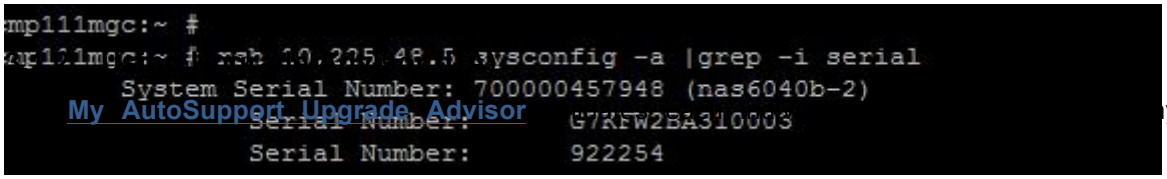
It should be showing as takeover mode and the interface name. (Yellow)

Commands: `ifstat -a` (check for the current status of the port in the below portion of the command output.

Above status should be "up" and also if this is part of the flow control check for the flow control status in the same output.

Obtaining Serial Numbers
Pulling the serial number/hostname from filer end.

From the command line of any DFM/Adminbox (unix) which has RSH/SSH access to the filer,



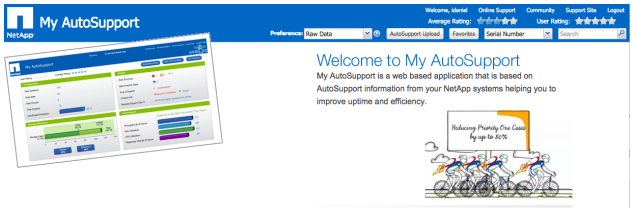
My AutoSupport, Upgrade Advisor y issues before

upgrading, and it also provides the ability to create detailed upgrade test procedure documents as well as back out plans.

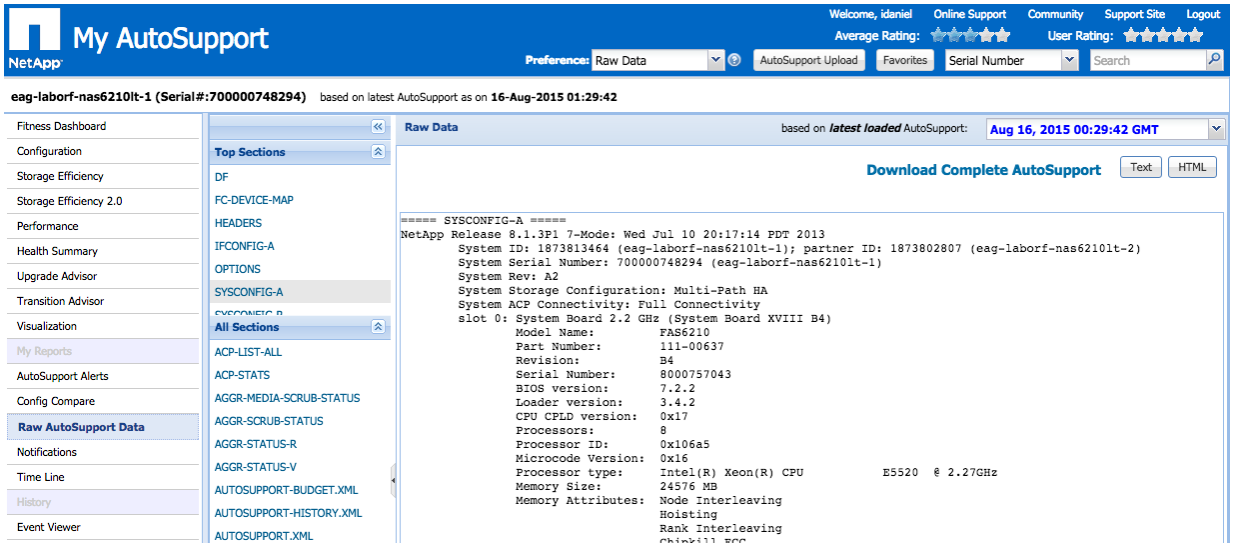
Please find the details with screenshot below.

To generate the basic overview and the step by step commands to perform the upgrade. Using specific filer system ID or serial number we can generate the upgrade plan from UA. This also provides a few warning messages with respect to the specific serial/system to be fixed before going for the ONTAP upgrade.

UA link: GO TO **http://mysupport.netapp.com/myautosupport/home.html** --- Enter Serial Number

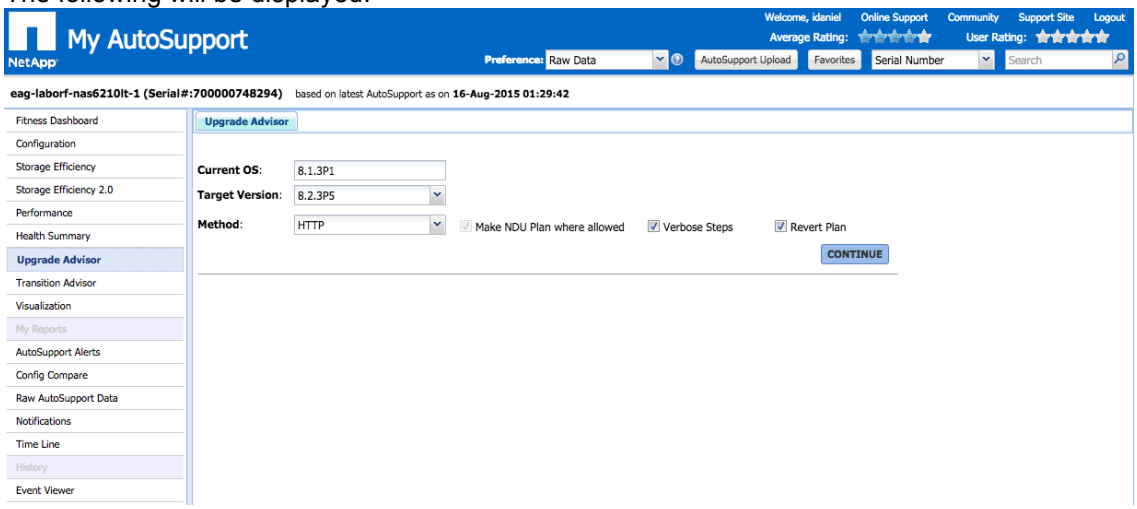


This will take you to the MYASUP page

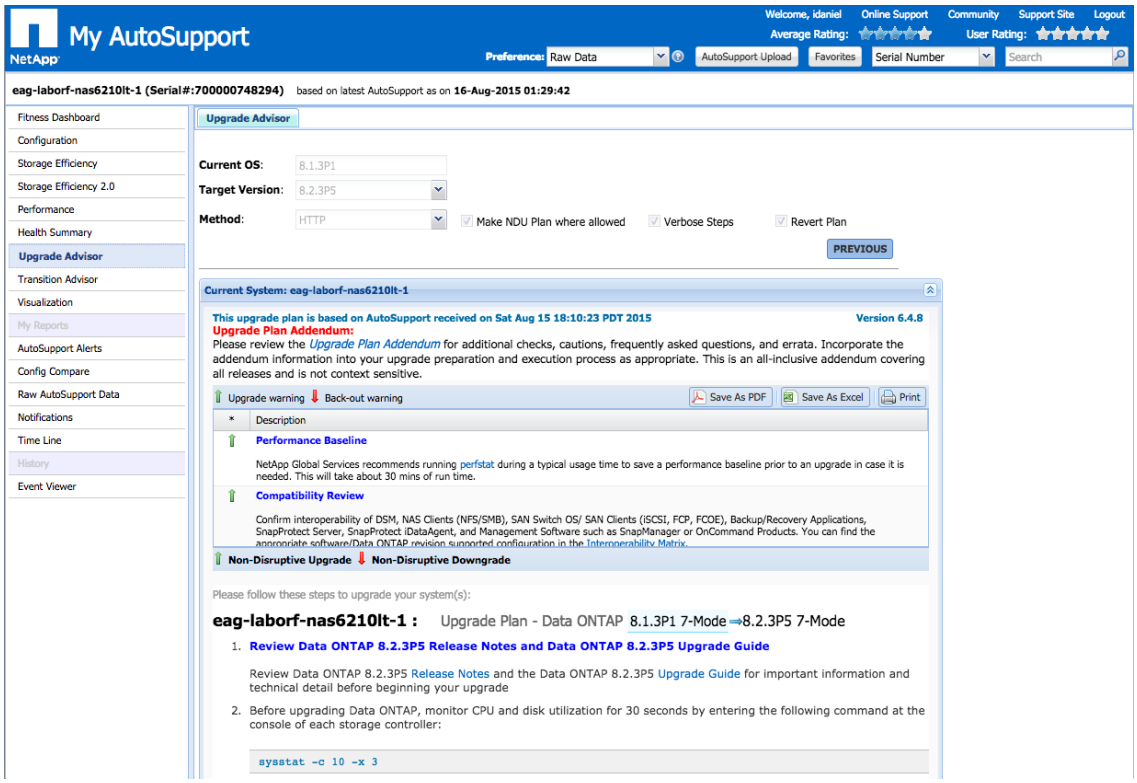


→ Click Upgrade Advisor

The following will be displayed.



Enter the Current and Destination OS versions. Make sure all boxes are checked and then press continue.



Note: In the first section UA gives the warning(s), this is needs to be addressed before performing the ONTAP upgrade.

3.1.3 HA Configuration Checker

The HA Configuration Checker is a Perl script that detects errors in the configuration of a pair of NetApp HA (active-active) storage controllers. It will run as a command from a Unix shell or Windows prompt, but also doubles as a CGI script that can be executed by a Unix web server. The script uses ssh to communicate with the storage controllers you're checking, so you'll need to have the appropriate permissions for rsh or ssh to run on both storage controllers in the HA pair.

Requirements
The tool is a Perl script. To run in a UNIX environment, Perl must be installed on the system.In all of our DFM servers Perl is installed already and is available under (/usr/bin/perl). Additionally, the client that runs the script must have rsh or ssh access

to the filers in the HA configuration. This is how the script gathers the information. If rsh is used, the script can be run with OR without a `/etc/hosts.equiv` entry on the node. If no `/etc/hosts.equiv` entry exists, then the username and password must be provided to the script. If ssh is to be used, a trusted public key must be set up on the nodes in the HA configuration.

This tool can be downloaded from NOW.netapp.com using below link,

http://now.netapp.com/NOW/download/tools/cf_config_check/

This HA script checks the following things,

- Data ONTAP versions mismatch
- Licenses mismatch
- High Availability(HA) configuration check
- Cluster status(cf status)
- fcp cfmode settings –Incase of using FCP service
- Options mismatch
- network configuration (Network interfaces configured wrong (clients will disconnect during takeover)
- /etc/rc mismatch (Checks ***/etc/rc*** on each storage controller to see that all interfaces have a failover set)

Command to run the Ha-configuration checker :

```
ha-config.check.cgi  [-s] [r shell] [-l] <name/IP_of_node_1> <name/IP_of_node_2>
```

Since our setup allows RSH by default we can use the same method to run this script,

Example : using filers (eg-nasapp-a05.westlan.com -10.221.252.225) and (eg-nasapp-a06.westlan.com - 10.221.252.254)

```
cmp111cwq:~/kan/HA-CHK # ./ha-config-check.cgi -r  rsh  10.221.252.225 10.221.252.254
== NetApp HA Configuration Checker v2.0.0 ==


Checking rsh logins. rsh 10.221.252.225 version


Checking rsh logins. rsh 10.221.252.254 version

OK

Checking Data ONTAP versions...

OK

Checking licenses...

snapmirror exists on 10.221.252.254, but not on 10.221.252.225

Checking HA configuration identity...

OK

Checking cf status...

OK

Checking fcp cfmode settings...

fcp: FCP is not licensed.
N/A

Checking options...

OK

Checking network configuration...

OK

Checking network config in /etc/rc

OK
HA configuration issue(s) found above. Please correct them and rerun this script.
Done.
```

RC filer check: `/dfm/netapp/scripts/netapp_rc_check.pl`

Command: `/dfm/netapp/scripts/netapp_rc_check.pl <filername>`

```
nerstrand:~ #
nerstrand:~ # /dfm/netapp/scripts/netapp_rc_check.pl eg-nas-b01

Parsing RC file.

Gathering running configuration.

Starting RC file checks.

RC WARNING: VIF ecommulti1 nas no "vlan create" commands associated with it.
    Verify that VLAN tagging is not in use for this VIF.

RC WARNING: VIF corpvif0 nas no "vlan create" commands associated with it.
    Verify that VLAN tagging is not in use for this VIF.

RC WARNING: VIF ecommulti2 nas no "vlan create" commands associated with it.
    Verify that VLAN tagging is not in use for this VIF.

RC WARNING: VIF corpmulti2 nas no "vlan create" commands associated with it.
    Verify that VLAN tagging is not in use for this VIF.

RC WARNING: VIF ecomvif0 nas no "vlan create" commands associated with it.
    Verify that VLAN tagging is not in use for this VIF.

RC WARNING: VIF corpmulti1 nas no "vlan create" commands associated with it.
    Verify that VLAN tagging is not in use for this VIF.

RC WARNING: No ifconfig statement found for corresponding VIF-VLAN statments on ecommulti1.
    This is OK for lower level VIFs.

RC WARNING: No ifconfig statement found for corresponding VIF-VLAN statments on ecommulti2.
    This is OK for lower level VIFs.

RC WARNING: No ifconfig statement found for corresponding VIF-VLAN statments on corpmulti2.
    This is OK for lower level VIFs.

RC WARNING: No ifconfig statement found for corresponding VIF-VLAN statments on corpmulti1.
    This is OK for lower level VIFs.

RC ERROR: Did not find IP address or hostanme configured for interface e0b.
    This should be investigated immediately in both the running and stored configuration.

RC ERROR: The "ifconfig" command for interface corpvif0 exists in the rc file but not the running config.
    This should be investigated immediately.

RC ERROR: The "ifconfig" command for interface e0 exists in the rc file but not the running config.
    This should be investigated immediately.

RC ERROR: The "ifconfig" command for interface e0b exists in the rc file but not the running config.
    This should be investigated immediately.

RC ERROR: The "ifconfig" command for interface ecomvif0 exists in the rc file but not the running config.
    This should be investigated immediately.

All RC file checks complete.

Starting running configuration checks.

All running configuration checks complete.
nerstrand:~ #
```

1. The netapp_rc check shown on the previous page performs the following:

2. The rc file has a valid hostname command.
3. The rc file has vlan creation statements that match the VIF and ifconfig related statemetns with vlan tagging.
4. The rc file has ifconfig lines for all VIF and vlan tagged VIFs that are created by the rc file.
5. Each ifconfig line in the rc file has an IP address assigned to it.
6. Each ifconfig line in the rc file has a valid partner argument.
7. Each ifconfig line in the rc file has a mtusize setting.
8. Each ifconfig line in the rc file has a netmask setting.
9. All vlan create/add statements in the rc file have a corresponding vlan in the running config.
10. All vif create statements in the rc file have a corresponding vif in the running config.
11. All ifconfig statements in the rc file have a corresponding interface in the running config.
12. The vif create statement for each VIF in the running config is present in the rc file with a matching VIF type.
13. The vlan create/add statement for each VLAN in the running config is in the rc file.
14. Each interface used in the running config has a valid partner argument.
15. The netmask found in the running config matches the netmask found in the rc file.
16. The mtusize found in the running config matches the mtusize found in the rc file.
17. Each vsip vfiler in the running config has a default route line in /etc/rc.

Check for the RC file entry Order: It is always recommended to check the RC file entry order before performing any takeover/giveback.

Order should be always like this:

Ifconfig entry
Route IP entry
Vfiler (vfiler route etc)

3.1.4 Remove all failed disks

Follow the following steps to remove the failed disks from the filer.

Use commands: eg : `ssh <filername> vol status –f`

vol status –f (this will show the broken/failed disks in the filer)
sysconfig (check for any BYP – Bypassed Disks)
fcadmin device_map (check for any BYP symbol in any of the channels)

Once you have identified the failed disk, check for any open case for this issue or raise a case with NetApp to replace the failed disk.

How to confirm whether this filer has already generated a case or not:

Go to support.netapp.com → "Cases & Parts" → View cases → then,
Use serial number or system ID or hostname to search (please see below screen shot),

Provide the serial number/system ID or hostname ,if this doesn't create a case. Please call the support center or use the same link (left side → "open a case" to open a new case.

Support center call details :

1. 888.4.NETAPP (US and Canada)
2. 00.800.44.NETAPP (EMEA/Europe)
3. +800.800.80.800 (Asia/Pacific)

All the above action helps to remove/replace the failed disks out of the filer.

3.1.5 Verify system load

Perform NDUs only when CPU and disk activity are as low as possible. The upgrade process requires one controller to assume the load normally handled by both controllers. By minimizing system load, you reduce the risk of host I/O requests being delayed or timing out.

Before initiating a Data ONTAP NDU, monitor CPU and disk utilization for 30 seconds by entering the following command at the console of each storage system controller.

Command: `sysstat -c 10 -x 3 (or)  sysstat -x 1`

Please find the screen shot for example:

```
nerstrand:~ # rsh eg-nas-b01 uptime
  4:17am up 622 days,  8:36 1311795285283 NFS ops, 338747065954 CIFS ops, 2252 HTTP ops, 0 FCP ops, 0 iSCSI ops
nerstrand:~ #
nerstrand:~ # rsh eg-nas-b01 sysstat -c 10 -x 3
 CPU   NFS  CIFS  HTTP   Total     Net kB/s   Disk kB/s     Tape kB/s Cache Cache  CP   CP Disk    FCP iSCSI   FCP  kB/s
                           in   out   read  write  read write   age   hit time  ty util                 in   out
 48% 13071   115     0   13186 33659 41901  40366   2841     0     0    10s  96%  18%  T    8%       0     0     0     0
 34% 11402   172     0   11574  3245 43966  40649     11     0     0    10s  96%   0%  -    7%       0     0     0     0
 61%  7448   190     0    7638  7254 35691  33020      8     0     0    11s 100%   0%  -    6%       0     0     0     0
 60%  8998    96     0    9094  6063 41784  43600  11316     0     0    14s  99%  26%  Tf  11%       0     0     0     0
nerstrand:~ #
nerstrand:~ # rsh eg-nas-b01 sysstat -x 1
 CPU   NFS  CIFS  HTTP   Total     Net kB/s   Disk kB/s     Tape kB/s Cache Cache  CP   CP Disk    FCP iSCSI   FCP  kB/s
                           in   out   read  write  read write   age   hit time  ty util                 in   out
 29% 14953    91     0   15044  2966  2967   966     24     0     0     1   99%   0%  -    6%       0     0     0     0
 31% 15618   131     0   15749  3221  2921  1011      0     0     0     1   99%   0%  -    7%       0     0     0     0
 31% 15764    68     0   15832  3775  2922   910      0     0     0     1   98%   0%  -    6%       0     0     0     0
 29% 14523    50     0   14573  2853  2871  1586     24     0     0     1   96%   0%  -    6%       0     0     0     0
nerstrand:~ #
```

Recommended values in the CPU and Disk Utilization columns should not be above 50% for all 10 measurements reported. Make sure that no additional load is added to the storage system until the upgrade completes.

3.1.6 Synchronize date and time:

Make sure that the date and time are synchronized between the two controllers. Although synchronized time is not required for the update to complete, it is important in case an issue arises that requires examining time- and date-based logs from both controllers.

Since we have a NTP server, time will be synced and to make sure the filer is running with correct timings, follow the below steps,

```
-bash-3.2$ for i in eg-nasapp-e07 eg-nasapp-e08; do echo "============$i==============" ; ssh $i  date; done
============eg-nasapp-e07==============
Tue Jul 28 08:15:25 CDT 2015
============eg-nasapp-e08==============
Tue Jul 28 08:15:26 CDT 2015
-bash-3.2$ for i in eg-nasapp-e07 eg-nasapp-e08; do echo "============$i==============" ; ssh $i  options timed  ; done
============eg-nasapp-e07==============
timed.enable                on          (same value in local+partner recommended)
timed.log                   off         (same value in local+partner recommended)
timed.max_skew              30m         (same value in local+partner recommended)
timed.min_skew              0           (same value in local+partner recommended)
timed.proto                 ntp         (same value in local+partner recommended)
timed.sched                 hourly      (same value in local+partner recommended)
timed.servers               ntpe1.westlan.com,ntpe2.westlan.com,ntpf1.westlan.com,ntpf2.westlan.com (same value in local+partner recommended)
timed.window                0s          (same value in local+partner recommended)
============eg-nasapp-e08==============
timed.enable                on          (same value in local+partner recommended)
timed.log                   off         (same value in local+partner recommended)
timed.max_skew              30m         (same value in local+partner recommended)
timed.min_skew              0           (same value in local+partner recommended)
timed.proto                 ntp         (same value in local+partner recommended)
timed.sched                 hourly      (same value in local+partner recommended)
timed.servers               ntpe1.westlan.com,ntpe2.westlan.com,ntpf1.westlan.com,ntpf2.westlan.com (same value in local+partner recommended)
timed.window                0s          (same value in local+partner recommended)
```

In a cluster, all timed options values on both filers must be configured the same. Run date commands on both the filer and the DFM server this gives the time difference. By default this schedule updates every hour, on the hour. Also make sure all the options are correctly set.

3.1.7 Verify the connectivity to the storage controller:

HOW TO CONNECT TO THE STORAGE CONTROLLERS:

Using serial cables, a console server, and the system's remote LAN module (RLM) or a baseboard management controller (BMC), open a terminal session to the console port of the two storage controllers. Network connections to the controllers are lost during takeover and giveback operations. Therefore telnet, SSH, and FilerView® sessions do not work for the NDU process.

Connect to RLM through user: naroot and password (as root password).(Hope all knows the root password ☺)
SSH <RLM IP> ,

Login: naroot Passwd :

RLM> system console

This will get to the system and login through default password.

This will login to system console as like this “netapp>”

For example:

login as: naroot naroot@10.224.128.63's password:
Last login: Fri Feb 6 07:15:33 2009 from 141.147.33.108 RLM netapp>
RLM netapp> system
system console - connect to the system console system core - dump the system core and reset system log - print system console logs

system power - commands controlling system power system reset - reset the system using the selected firmware

RLM netapp> system console Type Ctrl-D to exit.

Data ONTAP (netapp.Thomson.com) login: root
passwd : <root passwd> netapp>

Verify the connectivity between the cluster nodes using few commands as follows:
cf status
cf monitor (this shows the interconnect link status, takeover capability etc) “priv set –q diag;Cf monitor all” (check for the mailbox disks status)

```
cmp111cwq:~ # rsh eg-nasapp-a05 cf status
Cluster enabled, eg-nasapp-a06 is up.
cmp111cwq:~ #
cmp111cwq:~ # rsh eg-nasapp-a05 cf monitor
  current time: 29Sep2011 09:36:39
  UP 581+22:06:30, partner 'eg-nasapp-a06', cluster monitor enabled
  VIA Interconnect is up (link 0 up, link 1 up), takeover capability on-line
  partner update TAKEOVER_ENABLED (29Sep2011 09:36:39)
cmp111cwq:~ #
cmp111cwq:~ #
cmp111cwq:~ # rsh eg-nasapp-a05 "priv set -q diag;cf monitor all"
cf: Current monitor status (29Sep2011 09:36:52):
partner 'eg-nasapp-a06', VIA Interconnect is up (link 0 up, link 1 up)
state UP, time 50278003915, event CHECK_FSM, elem ChkMbValid (12)
mirrorConsistencyRequired TRUE
takeoverByPartner 0x2000 <TAKEOVER_ON_PANIC>
mirrorEnabled TRUE, lowMemory FALSE, memio UNINIT, killPackets TRUE
degraded FALSE, reservePolicy ALWAYS_AFTER_TAKEOVER, resetDisks TRUE
timeouts:
    fast 1000, slow 2500, mailbox 10000, connect 5000
    operator 600000, firmware 10000 (recvd 50278003915), dumpcore 60000
    booting 300000 (recvd 0)
    transit timer enabled TRUE, transit 600000 (last 44742)
mailbox disks:
Disk 0a.33 is a local mailbox disk
Disk 0c.16 is a local mailbox disk
Disk 0d.16 is a partner mailbox disk
Disk 0b.16 is a partner mailbox disk
primary state:
        version 2, senderSysid 101172826
        cluster_time 1267072276, hbt 67869169, node_status TAKEOVER_ENABLED
        info 0x2000 <TAKEOVER_ON_PANIC>
        flags 0x0 <>
        channel CHANNEL_MAILBOX, abs_time 1317307011, sk_time 50278002915
        channel_status 0
        channel CHANNEL_IC, abs_time 1317307012, sk_time 50278003915
        channel_status 0
        channel CHANNEL_NETWORK, abs_time 0, sk_time 0
        channel_status -1
backup state:
        version 2, senderSysid 101171265
        cluster_time 1267072276, hbt 167162884, node_status TAKEOVER_ENABLED
        info 0x2000 <TAKEOVER_ON_PANIC>
        flags 0x0 <>
        channel CHANNEL_MAILBOX, abs_time 1317307011, sk_time 50278002895
        channel_status 0
        Channel Read Ctx:
        version 2, senderSysid 101171265
        cluster_time 1267072276, hbt 167162883, node_status TAKEOVER_ENABLED
        info 0x2000 <TAKEOVER_ON_PANIC>
        flags 0x0 <>
        channel CHANNEL_IC, abs_time 1317307012, sk_time 50278003915
        channel_status 0
        Channel Read Ctx:
        version 2, senderSysid 101171265
        cluster_time 1267072276, hbt 167162884, node_status TAKEOVER_ENABLED
        info 0x2000 <TAKEOVER_ON_PANIC>
        flags 0x0 <>
        channel CHANNEL_NETWORK, abs_time 0, sk_time 0
        channel_status -1
        Channel Read Ctx:
        version 2, senderSysid 0
        cluster_time 0, hbt 0, node_status UNKNOWN
        info 0x0 <>
        flags 0x0 <>
takeoverState FT_NONE, takeoverString 'No takeover information'
givebackState FT_NONE, givebackString 'No giveback information'
givebackRetries 0, givebackRequested FALSE
autoGivebackEnabled FALSE, autoGivebackWasDone FALSE, autoGivebackCifsStopping FALSE
autoGivebackLastVetoCheck 0, autoGivebackAttemptsExceeded FALSE
Maximum primary disk mailbox io times: normal = 4350, transition = 0
Maximum backup disk mailbox io times: normal = 2826, transition = 0
Num times logs unsynced : 0
Total system uptime: 50278004623 msec
  Sync state total time : 50277850919 msec
  Sync state  Max  time : 50277850919 msec
cmp111cwq:~ #
```

From the above commands should be able to view all the connectivity details and mailbox details. Until all of these details are visible it will not allow the cluster to failover to the partner filer.

3.1.8 DR/Data Production consideration:

It is always recommended to upgrade the target filer first and then the source filer when there is any snapmirror/snapvault relationship exists.
When you upgrade Data ONTAP on storage systems that have a mirrored relationship with each other using SnapMirror, the order in which you upgrade the storage systems is critical. If you do not upgrade in the correct order, you can cause a lapse in SnapMirror replication coverage.

A SnapMirror transfer is possible only when the destination storage system can read a Snapshot copy of data on the source system. Therefore, the destination system must be upgraded first, so that it can read the Snapshot copies of the earlier release. If the source system is upgraded first, the destination system cannot read the source system's file system, so SnapMirror does not work.

Command : <primary> snapmirror status |grep –l <target filername> or IP address

Primary > snapmirror destinations

3.1.9 Determining The Latest Firmware and Upgrading Disks/Shelves.

Shelf firmware upgrades must be completed before performing Data ONTAP NDU.
NetApp disk shelves incorporate controller modules that support firmware upgrades as a means of providing greater stability or functionality. Because of the need for uninterrupted data I/O access by clients, these firmware updates can, depending on the model of module involved, be performed non-disruptively.

All shelf modules which has LRC/ESH/ESH2/ESH4 supports NON-DISTRUPTIVE UPGRADES.

AT-FCX Also supports NDU. If all below the criteria are met,

- If both the system AT-FCX modules are at FW37 (or above)
- Data ONTAP 7.3.2 or higher is being run on the system
- The system is correctly cabled for MPHA

3.1.9A SHELF UPGRADE:

HOW DOES SHELF FIRMWARE UPGRADE OCCUR?

The following subsections address how shelf controller module firmware upgrades can occur.

What happens during shelf firmware upgrade? (Below applies only if the Current FW is less than 37)

For systems incorporating AT-FC, AT-FC2, or AT-FCX shelf modules, including mixed environments with LRC or ESHx modules, shelf firmware upgrades occur in two steps—first to all A shelf modules and then to all B shelf modules.

The storage download shelf process requires 5 minutes to download the code to all A shelf modules.

During this time, I/O is allowed to occur. When the download completes, all A shelf modules are rebooted, which incurs up to a 70-second disruption in I/O for the shelf on both controller modules (when running a firmware version prior to version 37). This affects data access to the shelves regardless of whether multipath is configured. When the upgrade of the A shelf modules completes, the process repeats for all B modules. It takes 5 minutes to download the code (nondisruptively), followed by up to a 70-second disruption in I/O. The entire operation incurs two separate pauses of up to 70 seconds in I/O to all attached storage, including FC if present in the system. Systems employing multipath HA are also affected. The storage download shelf command is issued only once to perform both A and B shelf module upgrades.

AT-FCX – Disruptive(If FW < 37): If in case upgrading shelf firmware is missed before the ONTAP upgrade this will lead to disruptive upgrade. Shelf firmware upgrade occurs automatically during the boot process when the system is halted and rebooted. System boot is delayed until the shelf firmware upgrade process completes. This will lead to delay in upgrade and can bring down the application. Upgrading all shelf modules entails two downloads of 5 minutes PLUS two reboot cycles of up to 70 seconds each.
This must be completed before the system is allowed to boot and results in a total delay in the boot process of approximately 12 minutes. Upgrading shelf firmware during reboot suspends I/O for the entire 12-minute period for all storage attached to the system, including the partner node in HA pair configurations.

MANUAL FIRMWARE UPGRADE:

A manual shelf firmware upgrade prior to the Data ONTAP NDU operations is the preferred method.

Download the most recent firmware from the NOW site to the controller's /etc/shelf_fw directory and issue the “storage download shelf” command.

Shelf FW can be downloaded from https://now.netapp.com/NOW/download/tools/diskshelf/

Download the software
Place under filer (/etc/shelf_fw) folder
During the upgrade period issue command: “Storage download shelf”

Steps in details:

1. Get the firmware from the NOW site.
2. Use a web browser to connect to http://now.netapp.com/
3. Select the "Log In" button on the right side.
4. Enter your username and password.
5. Hover over "Downloads" on the gray bar, and then select "Disk Shelf Firmware"

6. Select the link "all current Disk Shelf & I/O Module Firmware"
7. Read over the instruction page.
8. Select "Download tar" at the bottom of the page. Save the file "all_shelf_fw.tar" to your local hard drive.
9. Close the web browser.
10. Determine the appropriate DFM server for the storage controller to have the firmware update applied.
11. Transfer "all_shelf_fw.tar" to your account on the DFM server using WINSCP or a similar program.
12. Log into the DFM server.
13. Change directory to the location you saved "all_shelf_fw.tar"
14. Extract the updated firmware with the following command:

    tar xvf all_shelf_fw.tar

15. Gain root privileges with "sudo bash".
16. Change directory into the extracted shelf_fw.
17. Look at the contents of the directory with the unix command "ls".
18. Look at the contents of the destination directory on the filer with the following command Replace "eg-nasbkp-e01" with the name of the storage controller you are updating the firmware on.

    ls /filers/eg-nasbkp-e01/shelf_fw

19. Copy the contents of the shelf_fw directory to the target NetApp storage controller with the following command. Be sure to replace "eg-nasbkp-e01" with the name of the storage controller you are updating,

    cp * /filers/eg-nasbkp-e01/shelf_fw

20. Change directory into the extracted acpp_fw.
21. Look at the contents of the directory with the unix command "ls".
22. Look at the contents of the destination directory on the filer with the following command Replace "eg-nasbkp-e01" with the name of the storage controller you are updating the firmware on.

    ls /filers/eg-nasbkp-e01/acpp_fw

23. If the directory acpp_fw doesn't exist on the NetApp storage controller, then you don't need to install the ACPP firmware. Jump ahead to step number 25. You will need to remember this decision later in step number 28.

24. Copy the contents of the acpp_fw directory to the target NetApp storage controller with the following command. Be sure to replace "eg-nasbkp-e01" with the name of the storage controller you are updating,

    cp * /filers/eg-nasbkp-e01/acpp_fw

25. Stop having root privileges with "exit".

    Log into the targeted NetApp storage controller with username "root".

26. Validate the current versions: **sysconfig -v**

27. Update the disk shelf firmware as follows:

    priv set advanced
    storage download shelf

28. If you copied the ACPP firmware to the NetApp storage controller in step number 24, you also need to update the ACPP firmware as follows:

    storage download acp

29. Type “y” when asked if you want to continue.

30. The download can be verified as follows: **sysconfig -v**

    This will show the latest version of the shelf.

AUTOMATIC FIRMWARE UPGRADE:
For disruptive (non-NDU) Data ONTAP upgrades, shelf firmware is updated automatically on reboot while upgrading Data ONTAP only if the firmware on the shelf controller modules is older than the version bundled with the Data ONTAP system files.

UPGRADING INDIVIDUAL SHELF MODULES:
Follow steps 1 to 21 to save the latest downloaded Firmware to filers /etc/shelf_fw folder. This below steps shows how to upgrade the individual shelf modules.
By default, all shelf modules are upgraded. For LRC, ESH, ESH2, and ESH4 series modules it is possible to upgrade a single shelf module or the shelf modules attached to a specific adapter by using the following command:

Command: `storage download shelf [adapter_number|adapter_number.shelf_number]`

Eg: netapp> storage download shelf 2a.1

For downloading the software please follow the above link in (manual firmware upgrade)

The above command informs the user if the upgrade will disrupt client I/O and offers an option to cancel the operation. Systems using only LRC, ESH, ESH2, or ESH4 shelf modules (in any combination) do not incur disruption during the upgrade process, regardless of whether the upgrade is performed manually or during storage controller reboot.

3.1.9B Disk Firmware Upgrade:

Depending on the configuration, NetApp provides the ability to conduct disk firmware upgrades nondisruptively (without affecting client I/O). Disk firmware NDU upgrades target one disk at a time, which reduces performance impact and results in zero downtime.

a) BACKGROUND DISK FIRMWARE NDU :

Beginning with Data ONTAP 7.0.1, nondisruptive disk firmware upgrades take place automatically in the background.

By enabling the option “raid.background_disk_fw_update.enable”,all the disks can be upgraded in the background.

This step has to be carried out before the actual ONTAP upgrade to avoid any delay in overall upgrade process.

Nondisruptive upgrades are performed by downloading the most recent firmware from the NOW site (http://now.netapp.com/NOW/download/tools/diskfw/) and place the software under,

/etc/disk_fw directory(/filer/etc/disk_fw)

Updates start automatically for any disk drives that are eligible for an update.
Data ONTAP polls approximately once per minute to detect new firmware in the /etc/disk_fw directory.

Firmware must be downloaded to each node in an HA pair configuration because, during an automatic download, the firmware is not downloaded to an HA pair partner's disks.

Background disk firmware updates do not occur if either of the following conditions is encountered:

- Degraded volumes exist on the storage system.
- Disk drives that need a firmware update are present in a volume or plex that is in an offline state.

b) Manually upgrading disk firmware :

1. Get the firmware from the NOW site.
2. Use a web browser to connect to http://now.netapp.com/
3. Select the "Log In" button on the right side.
4. Enter your usrname and password.
5. Hover over "Downloads" on the gray bar, and then select "Disk Drive & Firmware Matrix"
6. Select the link "all current Disk Firmware"
7. Read over the instruction page.
8. Select "Download gz" at the bottom of the page. Save the file "all.gz" to your local hard drive.

9. Close the web browser.
10. Determine the appropriate DFM server for the storage controller to have the firmware update applied.
11. Transfer "all.gz" to your account on the DFM server using WINSCP or a similar program.
12. Log into the DFM server.
13. Change directory to the location you saved "all.gz"
14. Extract the updated firmware with the following command:

    gzip -cd all.gz | tar xvf -

15. Change directory into the extracted etc/disk_fw.
16. Look at the contents of the directory with the unix command "ls".
17. Gain root privladges with "sudo bash".
18. Look at the contents of the destination directory on the filer with the following command Replace "eg-nasbkp-e01" with the name of the storage controller you are updating the firmware on.

    ls /filers/eg-nasbkp-e01/disk_fw

19. Copy the contents of the current directory to the target NetApp storage controller with the following command. Be sure to replace "eg-nasbkp-e01" with the name of the storage controller you are updating,

    cp * /filers/eg-nasbkp-e01/disk_fw

20. Stop having root privileges with "exit".
21. Log into the targeted NetApp storage controller with username "root"
22. Execute command : disk_fw_update to upgrade the disk firmware manually.

On systems configured with software disk ownership, the firmware upgrade must be performed separately on each node individually in sequence, meaning that you must wait for the first node to complete before starting the second.

3.1.10 Check for all Vfiler status

Check the Vfiler status regularly after the following steps:

a. After first Takeover and giveback is done
b. After partner filer Takeover and giveback is completed

3.1.11 Check for stale finger print and utilization of infra volumes

A. Find out any ESX datastore above 85% utilization ,If any are listed here we need to temporarily expand the volume size by enough to reduce the volume utilization below 85%.This is already in practice

Example :

```
bash-3.2$ ssh eg-nasecom-e13 'df -h' | grep -i 'infra_' | egrep "8[5-9]%|9[0-
9]%|100%" | egrep -v 'snapshot'
```

B. Find out the highly utilized infra volume >70% having stale finger print above 50% . Run a 'sis start –s' to clear up the stale finger print

Please remember this is a resource hungry process so consider filer performance and free space on the volume while running this. Add temporary space if needed.We do pre-check well ahead of ontap upgrade hence they can be staggered .

Example :

```
-bash-3.2$ for i in `ssh eg-nasecom-e13 'df -h' | grep -i 'infra_' | egrep
"7[0-9]|8[0-9]%|9[0-9]%|100%" | egrep -v 'snapshot' |cut -d"/" -f1,2,3`; do
echo "Checking $i"; ssh eg-nasecom-e13 "sis status -l $i"| grep -i stale ; done
Checking /vol/infra_virtual_pee0517_nosnap
Stale Fingerprints:              11%
Checking /vol/infra_virtual_pee0518_nosnap
Stale Fingerprints:              32%
Checking /vol/infra_virtual_pee0518_snap07
Stale Fingerprints:              13%
Checking /vol/infra_virtual_pee0518_snap14
Stale Fingerprints:              31%
```

C. Check for Last Operation Size 0 in sis status -l , if any volume has "Last Operation Size" and stale finger print , run sis start -s to clear it "

```
for i in `ssh eg-nasecom-e13 'df -h' | grep -i 'infra_' | egrep -v 'snapshot'
|cut -d"/" -f1,2,3`; do echo "Checking $i"; ssh eg-nasecom-e13 "sis
status -l $i"| grep -i 'Last Operation Size' ; done
```

The above filer is clear and no need to run any 'sis start –s' or add any space

Post Check: After the ONTAP upgrade check if there is any abnormal growth on stale finger print

Example:

```
for i in eg-nasecom-e13 eg-nasecom-e14;do echo "-----------------$i----------------"
; ssh $i "sis status -l"| grep -i stale ; done
```

If you found rapid increment of stale finger print, run a `sis start -s` consider filer performance and free space on the volume while running this. Add temporary space if needed, please collect below information and let us know:

```
df -h
df -s
sis ls (priv set diag; sis ls /vol/testvol)
```

```
sis status -l  (priv set diag; sis status -l /vol/testvol)
sis.log
```

3.1.12 Exports entry check for VM volumes

Check for any VM related volumes exist on the filer (example : infra etc) ,if so please make sure to check the exports entry for all the volumes .If there is no exports entry or no specific client machines are specified, please reach out to the VM team and ask for the specific hosts details which are accessing the volume. Add those hosts to the exports entry and this will avoid any VM inaccessible issues.

E.g.: command: `ssh eg-naslowc-e03 vfiler status -a |egrep -i "infra|runn" prod-corp-e0104 running`

```
Path: /vol/infra_opsware_prod2_n01ora1_nosnap
Path: /vol/infra_opsware_prod2_s01ora1_snap
```

```
nerstrand:~ # /usr/sbin/showmount -e prod-corp-e0104 |grep -i infra_opsware_prod2_n01ora1_nosnap
/vol/infra_opsware_prod2_n01ora1_nosnap/oracluster1 optima-nas.int.westgroup.net
/vol/infra_opsware_prod2_n01ora1_nosnap/oraflash1   optima-nas.int.westgroup.net
/vol/infra_opsware_prod2_n01ora1_nosnap/oraadmin1   optima-nas.int.westgroup.net
/vol/infra_opsware_prod2_n01ora1_nosnap/oradata1    optima-nas.int.westgroup.net
/vol/infra_opsware_prod2_n01ora1_nosnap/oraarch1    optima-nas.int.westgroup.net
nerstrand:~ #
```

3.1.13 Exports check script

It compares the export permission in running config i.e Cache with the configuration file (/etc/exports or "<vfiler_root_volume>/etc/exports"

Run the script "`/filers/admin/scripts/support/exports_check.sh`" and check for the outputs

```
-bash-3.2$ /filers/admin/scripts/support/exports_check.sh
rm: cannot remove `/tmp/a1': No such file or directory
rm: cannot remove `/tmp/b1': No such file or directory
 please enter the filer name
eg-nasapp-e30

Testing volume ded_ecom_e0023_root on vfiler ded-ecom-e0023 of filer eg-nasapp-e30

##################################
 Entry on the configuration

/vol/ded_ecom_e0023_root        -
sec=sys,rw=newpoint.int.westgroup.net:nerstrand.int.westgroup.net:newnan.int.westgroup.net:nid
aros.int.westgroup.net,anon=0

Entry on the cache

/vol/ded_ecom_e0023_root        -
sec=sys,rw=newpoint.int.westgroup.net:nerstrand.int.westgroup.net:newnan.int.westgroup.net:nid
aros.int.westgroup.net,anon=0

##################################
```

```
Testing volume ded_ecom_e0024_root on vfiler ded-ecom-e0024 of filer eg-nasapp-e30

###################################
 Entry on the configuration

/vol/ded_ecom_e0024_root        -
sec=sys,rw=newpoint.int.westgroup.net:nerstrand.int.westgroup.net:newnan.int.westgroup.net:nid
aros.int.westgroup.net,anon=0

Entry on the cache

/vol/ded_ecom_e0024_root        -
sec=sys,rw=newpoint.int.westgroup.net:nerstrand.int.westgroup.net:newnan.int.westgroup.net:nid
aros.int.westgroup.net,anon=0

###################################


Testing volume eg_nasapp_e30_ecomvsip2053_root on vfiler eg-nasapp-e30-ecomvsip2053 of filer
eg-nasapp-e30

###################################
 Entry on the configuration

/vol/eg_nasapp_e30_ecomvsip2053_root    -sec=sys,rw,anon=0,nosuid

Entry on the cache

/vol/eg_nasapp_e30_ecomvsip2053_root    -sec=sys,rw,anon=0,nosuid

###################################


Testing volume vol0_vsip_2022 on vfiler eg-nasapp-e30-vsip of filer eg-nasapp-e30

###################################
 Entry on the configuration

/vol/vol0_vsip_2022     -sec=sys,rw,anon=0

Entry on the cache

/vol/vol0_vsip_2022     -sec=sys,rw,anon=0

###################################

Printing results
#############################

 Volume ded_ecom_e0023_root is PASS
 Volume ded_ecom_e0024_root is PASS
 Volume eg_nasapp_e30_ecomvsip2053_root is PASS
 Volume vol0_vsip_2022 is PASS
```

```
############################
 Printing volumes that has volume level export configuration
############################


############################
 Printing volumes that has global RW cofiguration
############################

Below volumes global RW cofiguration on eg-nasapp-e30
#####
#####

############################
-bash-3.2$
```

Check for the printing results for “FAIL” filesystem like below and resolve it by comparing the exports and exportfs command. Make sure the right entry should be in exports file and once resolved, please make the comment in prechecks notepad.

```
Volume clnt_corp_f0388_root is FAIL ---------------- Checked and made entry in exports file
 Volume trs_revfinder1q_n01ora1_nosnap is FAIL -------- Ignored , the volume level entry in
exports file is removed
 Volume trs_revfinder1q_s01oraadm1_snap is FAIL -------- Ignored , the volume level entry in
exports file is removed
 Volume trs_revfinder1q_s01ora1_snap is FAIL -------- Ignored , the volume level entry in
exports file is removed
Volume infra_virtual_pcf0425_snap07 is PASS
 Volume infra_pltm_product_bldr659q_n01ora1_nosnap is PASS
 Volume clnt_corp_f0426_root is PASS
 Volume ct_cppppbqaf_snap is PASS
 Volume infra_pltm_product_bldr659q_s01ora1_snap is PASS
```

If the printing results shows there is a filesystem has volume level exports, Please do the checks for exports.

```
############################
 Printing volumes that has volume level export configuration
############################

 Volume ct_opfanalytical_nosnap has export configuration at volume level on clnt-corp-f0318 --
----- Resolved
 Volume bis_bi1a_n01ora1_nosnap has export configuration at volume level on clnt-corp-f0318 --
----- Resolved
 Volume bis_bi1a_s01ora1_snap has export configuration at volume level on clnt-corp-f0318 ----
--- Resolved

############################
 Printing volumes that has global RW cofiguration
############################
```

Below volumes global RW cofiguration on eg-nasclnt-f03
#####
#####

```
 infra_virtual_ccf0303_nosnap on clnt-corp-f0303 has global RW cofiguration -- Can
be ignored
 eg_nasclnt_f03_corpvsip_3051 on eg-nasclnt-f03-corpvsip-3051 has global RW
cofiguration -- Can be ignored
 trs_revfinder1q_n01ora1_nosnap on clnt-corp-f0388 has global RW cofiguration -
Resolved
```

Steps to compare the file systems exports.

1. Run the exportfs command

```
-bash-3.2$ ssh eg-nasclnt-f03 vfiler run clnt-corp-f0388 exportfs |grep trs_revfinder1q_s01oraadm1_snap
/vol/trs_revfinder1q_s01oraadm1_snap/s01oraadmin1       -sec=sys,rw=c318qaarfdbs1.int.thomsonreuters.com,anon=0,nosuid
```

2. Read the exports file configuration

```
-bash-3.2$ ssh eg-nasclnt-f03 rdfile /vol/clnt_corp_f0388_root/etc/exports|grep trs_revfinder1q_s01oraadm1_snap
/vol/trs_revfinder1q_s01oraadm1_snap/s01oraadmin1       -sec=sys,rw=c318qaarfdbs1.int.thomsonreuters.com,anon=0,nosuid
```

3. Run showmount command to check how the filesystem mounted on hosts(Volume/Qtree level)

```
-bash-3.2$ /usr/sbin/showmount -a clnt-corp-f0388 |grep trs_revfinder1q_s01oraadm1_snap
c318qaarfdbs1.int.thomsonreuters.com:/vol/trs_revfinder1q_s01oraadm1_snap/s01oraadmin1
-bash-3.2$
```

```
Volume clnt_corp_f0388_root is FAIL ---------------- Checked and made entry in exports file
 Volume trs_revfinder1q_n01ora1_nosnap is FAIL -------- Ignored , the volume level entry in
exports file is removed
 Volume trs_revfinder1q_s01oraadm1_snap is FAIL -------- Ignored , the volume level entry in
exports file is removed
 Volume trs_revfinder1q_s01ora1_snap is FAIL -------- Ignored , the volume level entry in
exports file is removed
```

3.1.14 File Handle check script

Check for any file handle by search the string “bad fh:0 0 0 0 0 0” in the output file and check for the exports in both running(cache) and the exports file.

Then check the mounted filesystems on hosts using showmount –a <vfilername> |grep <filesystem>
If there is any mismatch in exports and we need to work with DBA/Platform team to unmount the filesystem , reexport the filesystem and mount the filesystem by having a CR.

```
echo "===============Exports Check====================="
echo "-----------eg-nasapp-e07----------"
/dfm/netapp/scripts/nfs_export_debug.pl eg-nasapp-e07 > /dfm/guna/eg-nasapp-e07_postwork1_output.txt

echo "-----------eg-nasapp-e08----------"
/dfm/netapp/scripts/nfs_export_debug.pl eg-nasapp-e08 > /dfm/guna/eg-nasapp-e08_postwork1_output.txt

echo "---------------BAD FH Check----------------------"
echo "cat /dfm/guna/eg-nasapp-e07_postwork_output.txt |grep -i bad"
cat /dfm/guna/eg-nasapp-e07_postwork_output.txt |grep -i bad
echo "cat /dfm/guna/eg-nasapp-e08_postwork_output.txt |grep -i bad"
cat /dfm/guna/eg-nasapp-e08_postwork_output.txt |grep -i bad
cat /dfm/guna/eg-nasapp-e07_postwork_output.txt
cat /dfm/guna/eg-nasapp-e08_postwork_output.txt
```

3.1.15 IP Space check

IPspaces are distinct IP address spaces in which vFiler units reside. You create IPspaces when you need your vFiler units to have their own secure storage, administration, and routing.

IPspace check should follow the below conditions.

1. Each VLAN should have separate ipspace
2. IPspace should be similar in both the filers in cluster
3. If there is a VLAN and IPspace configured for one node in cluster , the partner node should also have the same IPspace configured eventhough there is no VLAN interfaces assigned to them.
4. Remove any unassigned/unwanted IPspaces(Do doublecheck with other Engineer before removing)

Commands to check the IPspace

a. To list the IPspace configured for the filer

```
# ssh <filername> ipspace list
```

```
-bash-3.2$ ssh eg-nasclnt-f03 ipspace list
Number of ipspaces configured: 4
default-ipspace                    (e0a e0b e0d e0f e0M losk corpvif0)
corp-3002                          (corpvif0-3002)
corp-3051                          (corpvif0-3051)
corp-3053                          (corpvif0-3053)
-bash-3.2$ ssh eg-nasclnt-f04 ipspace list
Number of ipspaces configured: 4
default-ipspace                    (e0a e0b e0d e0f e0M losk corpvif0)
corp-3002                          (corpvif0-3002)
corp-3051                          (corpvif0-3051)
corp-3053                          (corpvif0-3053)
-bash-3.2$
```

b. To check the IPspaces configured for the vfilers

Note: Some IPspace will not reflect in the below output before if there is no vfiler configured , but check for partner node for the details.

```
# ssh <filername> vfiler status -a |egrep "space" |sort |uniq
```

```
-bash-3.2$ ssh eg-nasclnt-f03 vfiler status -a |egrep "space" |sort |uniq
   ipspace: corp-3002
   ipspace: corp-3051
   ipspace: corp-3053
   ipspace: default-ipspace
-bash-3.2$ ssh eg-nasclnt-f04  vfiler status -a |egrep "space" |sort |uniq

   ipspace: corp-3002
   ipspace: corp-3051
   ipspace: corp-3053
   ipspace: default-ipspace
-bash-3.2$
```

c. Check for unwanted IPspace and clean it up if the ipspace not used by any filer/parner interfaces.

```
u0155888@cmp111mgc:~> ssh eg-nasclnt-e05  ipspace list
Number of ipspaces configured: 4
default-ipspace                   (e0a e0b e0c e0d e0e e0f e2b e8b losk corpvif0)
corp-2002                         (corpvif0-2002)
corp-2051                         (corpvif0-2051)
corpvif0-2051                     (no interfaces)
```

```
u0155888@cmp111mgc:~> ssh eg-nasclnt-e05  ipspace list
Number of ipspaces configured: 3
default-ipspace                   (e0a e0b e0c e0d e0e e0f e2b e8b losk corpvif0)
corp-2002                         (corpvif0-2002)
corp-2051                         (corpvif0-2051)
```

3.1.16 Perfstat collection

NetApp recommends running perfstat during a typical usage time to save a performance baseline prior and post to an maintenance activity in case it is needed. This will take about 30+30 mins of
run time.

Prior to maintenance: Minimum 30minutes before the activity.

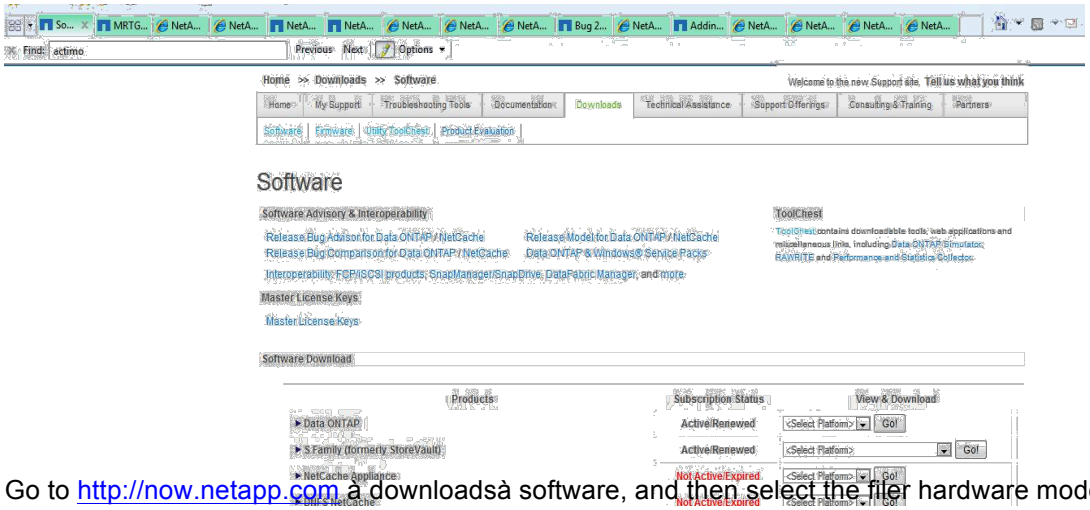
```
bash-3.2# su - svcstg_scriptuser
-bash-3.2$ /filers/admin/scripts/support/perfstat.sh -S -l svcstg_scriptuser -f eg-nassecom-h05 -t 4 -i 5 > /dfm/dfminst/perfdata/eg-nassecom-h05_PRE_perfstat.out
Perfstat: Perfstat v7.39 (4-2013)
Perfstat: Verify host ssh access
Perfstat: Verify filer ssh access
Perfstat: Allowing perfstat to run for a max 2400 seconds
Perfstat: Begin Iteration 1
Perfstat: Collect Prestats
```

Post upgrade:

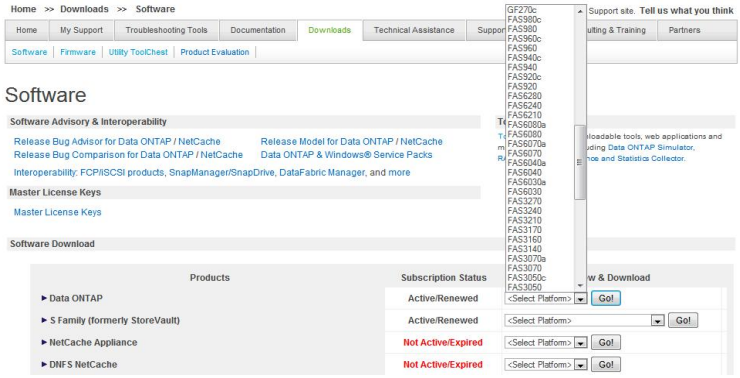
```
bash-3.2# su - svcstg_scriptuser
-bash-3.2$ /filers/admin/scripts/support/perfstat.sh -S -l svcstg_scriptuser -f eg-nassecom-h05 -t 4 -i 5 > /dfm/dfminst/perfdata/eg-nassecom-h05_POST_perfstat.out
Perfstat: Perfstat v7.39 (4-2013)
Perfstat: Verify host ssh access
Perfstat: Verify filer ssh access
Perfstat: Allowing perfstat to run for a max 2400 seconds
Perfstat: Begin Iteration 1
Perfstat: Collect Prestats
Perfstat: Prestats on eg-nassecom-h05; OS: ONTAP8.1.3
```

4 Obtaining the ONTAP version from support.netapp.com

The required ONTAP software can be downloaded from http://now.netapp.com. Basically ONTAP versions can be downloaded based on the platforms. Please follow the below steps to download the software,



Go to http://now.netapp.com à downloadsà software, and then select the filer hardware model to download the ONTAP software

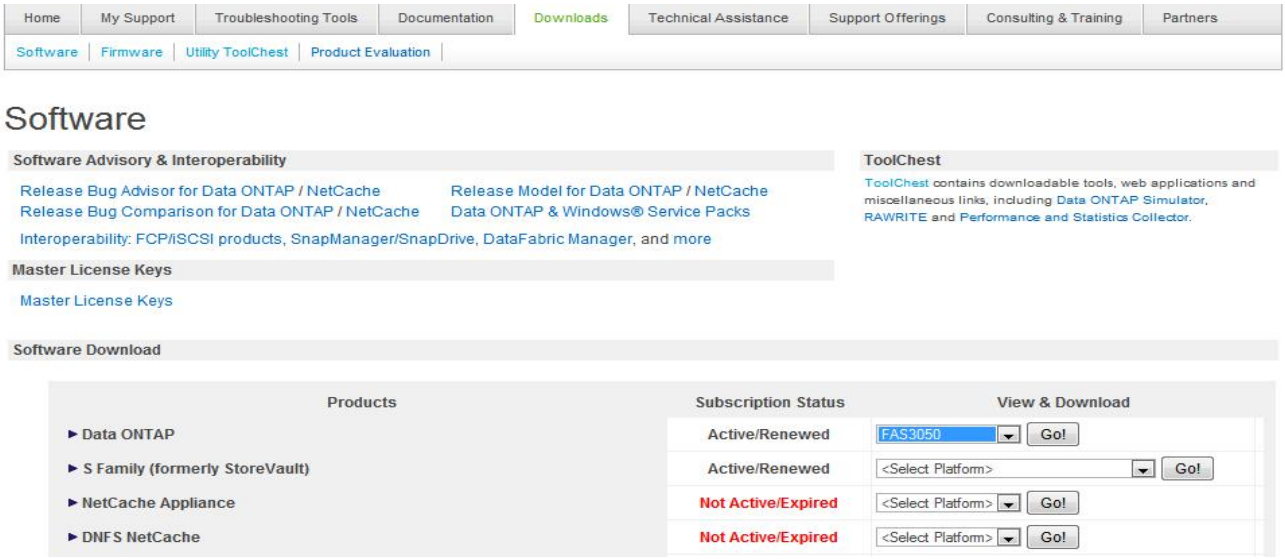


How to find the hardware model?

Use command: `ssh <filername> sysconfig -a |grep -i model`

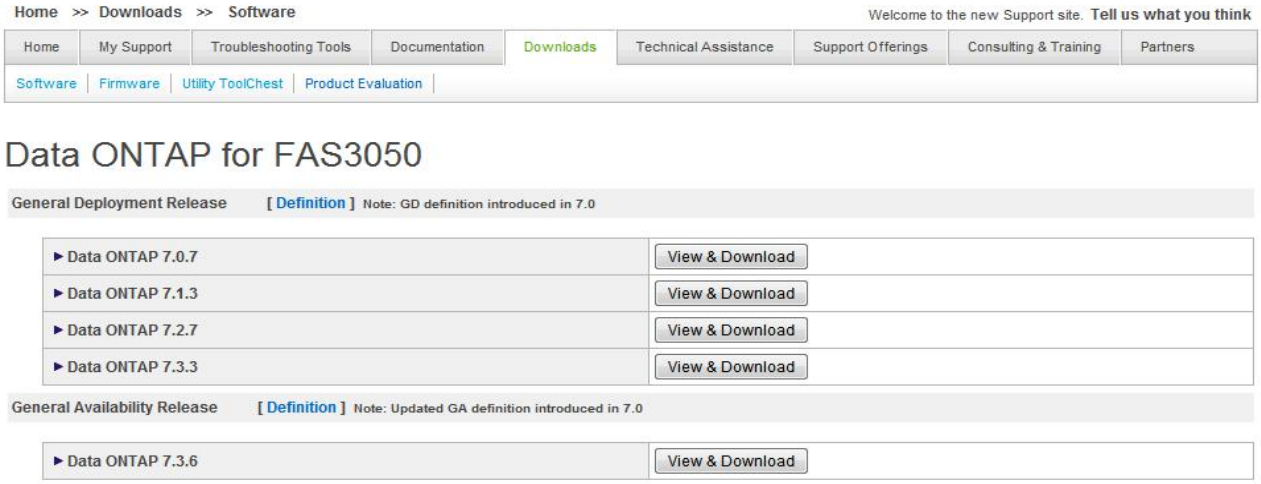
Above command will give the filer model.

```
cmp111cwq:~ # rsh eg-nasapp-a05 sysconfig -a |grep -i model
               Model Name:          FAS3050
cmp111cwq:~ # a
```



Then → GO!

This will show the available ONTAP versions for that filer model



Note: Most of the latest hardware filers support all the versions

Download the Ontap version to local desktop and later using SCP software we can copy it to DFM servers. Follow the below steps, Copy the Ontap version from dfm server to filer software folder

```
DFM#  CP 7311P2_setup_q.exe /filer/etc/software
```

4.1 MINOR VERSION NDU

1. Create an AutoSupport notification by entering the options autosupport.doit starting_NDU command at the console of each storage system controller. This creates a record of the system status just before upgrade and saves useful troubleshooting information in case there is a problem during the upgrade process.

   Command: `ssh <filername> options autosupport.doit starting_NDU`

2. Verify that controller failover is enabled on the HA pair partners by issuing the command cf status. If the command output lists Cluster disabled, determine the cause, address it, and then enable controller failover by issuing the cf enable command.

   Command: `ssh <filername> cf status`

   (if this shows as disabled),also need to verify why cluster was disabled. This could be due to interconnect issue, mailbox sync issue etc..

   Command: `ssh <filername> cf enable`

3. Determine whether automatic giveback is active by executing the command options cf.giveback.auto.enable. If enabled, disable it with the command options cf.giveback.auto.enable off.

   Command: `ssh <filername> options cf.giveback.auto.enable`

4. Verify that CPU utilization and disk utilization are both below 50%.
   a. Enter the command sysstat -c 10 -x 3 on each controller in the HA pair.
   b. Confirm that the values in the CPU and Disk Util columns remain below 50% for all 10 measurements reported.
   c. Make sure that no additional load is added to the system throughout the NDU process.

   Command: `ssh <filername> sysstat –c 10 –x 3  or  sysstat –x 5`

   Perform the software installation operation of the new version of Data ONTAP on both storage controllers.

5. Issue the download command on both controllers to update the compact flash boot media.
   a. You can also use the software update -r command instead of software install followed by the download command, but you must include the -r flag to control when the controller reboot occurs.

   Commands: `ssh <filername> software list` → this will list the uploaded latest software

   `ssh <filername> software update  –r` → this will extract and update the ONTAP software on compact flash card.

   (Or)

   `ssh <filername> software install` (this also does the same extraction)(above command is highly recommended)

Then ,

`ssh <filername> download` or do `ssh <filername>` and perform "`download`"

6. Confirm that controller failover is enabled and that CPU utilization and disk I/O do not exceed 50% per controller.

EG:

```
Netapp09> software update 7311P2_setup_q.exe -r

software: You can cancel this operation by hitting Ctrl- C in the next 6 seconds.
software: Depending on system load, it may take many minutes
software: to complete this operation. Until it finishes, you will software: not
be able to use the console.
software: installing software, this could take a few minutes...
software: Data ONTAP Package Manager Verifier 1
software: Validating metadata entries in /etc/boot/NPM_METADATA.txt
software: Checking sha1 checksum of file checksum file: /etc/boot/NPM_FCSUM-x86-
64.sha1.asc software: Checking sha1 file checksums in /etc/boot/NPM_FCSUM-x86-
64.sha1.asc
software: installation of 7311P2_setup_q.exe completed.
Fri Oct 23 22:42:18 CDT [adc15ntap09: rc:info]: software: installation of
7311P2_setup_q.exe completed.
```

Once ONTAP is installed this will gives a message as " software install completed successfully"

7. Choose the following option that describes your configuration.

If you have CIFS... Then...

If it's not in use in system B Go to the next step.

If it is in use in system B Enter the following command:

```
cifs terminate -t nn
```

nn is a notification period (in minutes) appropriate for your clients after which CIFS services are terminated. After that period of time, proceed to the next step. At the console of system A, enter the following command. Issue the cf takeover command on controller A (do not use the -f parameter).
Controller B shuts down cleanly and reboots.

Note: Before TO/GB, Check the following.

- Stop all active system jobs (dedup, snapmirror, snapvault, snapshots, etc).
- Don't perform additional management actions (such as deleting a lot of snapshots, volumes, etc).
- Ensure each node is under 50% usage. Reduce load if usage is high and ensure no additional workload starts during when all data is served on a single node.

Perform command: `cf takeover` (on primary)

8. When controller B displays Waiting for giveback, issue the cf giveback command on controller A to return controller B's data service.

   Command : Primary > cf status this should show as ("waiting for Giveback" status")

   Note: Before TO/GB , Check the following.

   - Stop all active system jobs (dedup, snapmirror, snapvault, snapshots, etc).
   - Don't perform additional management actions (such as deleting a lot of snapshots, volumes, etc).
   - Ensure each node is under 50% usage. Reduce load if usage is high and ensure no additional workload starts during when all data is served on a single node.

   Primary > `cf giveback`

9. Controller B is now running the new version of Data ONTAP and controller A the old version.

10. Issue the `cf takeover` command on controller B.

    Automatic BIOS system firmware updates

    Beginning with the Data ONTAP 7.3 release, the minimum BIOS release required to support Data ONTAP also enables automatic BIOS updates.After the minimum version is running, subsequent updates take place automatically during the boot sequence whenever Data ONTAP detects that a version resident on the boot device is more recent than the running version.

    However, to update firmware from an earlier version to the latest version available, you must run the update_flash command manually from the boot prompt on the system being upgraded. Subsequent system firmware updates are automatic.

    The following are the minimum BIOS system firmware versions required to support Data ONTAP.

    Note: For upgrading BIOS manually please refer steps at 7.0

11. When controller A displays the message —Waiting for giveback,ll issue the cf giveback command on controller B.

12. Verify that controller failover is enabled with the cf status command. Both controllers are now running the new version of Data ONTAP.

    Command: `ssh <filername> version -b` → to verify the latest Ontap version is upgraded or not.It should show like this,

    ```
    netapp> version -b
    1:/x86_64/kernel/primary.krn: OS 7.3.1.1P2→ This is the latest version just upgraded.
    ```

```
1:/backup/x86_64/kernel/primary.krn: OS 7.2.4P7 1:/x86_64/diag/diag.krn: 5.3.6
1:/x86_64/firmware/excelsio/firmware.img: Firmware 1.6.0
1:/x86_64/firmware/DrWho/firmware.img: Firmware 2.2.0 1:/boot/loader: Loader
1.6
```

Also check for the cluster status using command: `cf status`

13. Create another AutoSupport notification by entering the command options autosupport.doit finishing_NDU at the console of each storage system controller. This creates a record of the system status after upgrading. It saves useful troubleshooting information in case problems are being or have been encountered.

    Command: `ssh <filername> options autosupport.doit After_NDU`

14. Verify that all hosts previously connected to the storage controllers have not experienced I/O errors.

    Monitor the filer's log for any critical/warning messages (`tail -f /<filer>/etc/messages`).

    If any critical/warning message is been reported, please feel free to escalate to support team.

15. Verify the latest Ontap version by,

    Command: `ssh <filername> version -b`

    E.g.:

```
newnan:~ #
newnan:~ # rsh eg-nascorpbkp-f02 version -b
/cfcard/x86_64/freebsd/image1/kernel: OS 8.0.1P5
/cfcard/x86_64/freebsd/image2/kernel: OS 8.0.1
/cfcard/backup/x86_64/kernel/primary.krn: OS 7.3.3P3
/cfcard/x86_64/diag/diag.krn:  5.4.7
/cfcard/x86_64/firmware/excelsio/firmware.img: Firmware 1.9.0
/cfcard/x86_64/firmware/DrWho/firmware.img: Firmware 2.5.0
/cfcard/x86_64/firmware/SB_XV/firmware.img: Firmware 4.4.0
/cfcard/x86_64/firmware/SB_XVI/firmware.img: Firmware 5.1.0
/cfcard/x86_64/firmware/SB_XVIII/firmware.img: Firmware 7.0.1
/cfcard/boot/loader: Loader 1.7
/cfcard/common/firmware/zdi/zdi_fw.zpk: PAM II Firmware 1.10 (Build 0x201012200653)
/cfcard/common/firmware/zdi/zdi_fw.zpk: X1936A FPGA Configuration PROM 1.0 (Build 0x200706131558)
```

4.2 MAJOR VERSION NDU

After downloading ONTAP software from now.netapp.com (Refer section 5.0)

1. Create an AutoSupport notification by entering the options autosupport.doit starting_NDU command at the console of each storage system controller. This creates a record of the system status just before upgrade and saves useful troubleshooting information in case there is a problem during the upgrade process.

   Command: `ssh <filername> options autosupport.doit starting_NDU`

2. Verify that controller failover is enabled on the HA pair partners by issuing the command cf status. If the command output lists Cluster disabled, determine the cause, address it, and then enable controller failover by issuing the cf enable command.

   Command: `ssh <filername> cf status`

   (if this shows as disabled),also need to verify why cluster was disabled. This could be due to interconnect issue, mailbox sync issue etc.

   Command: `ssh <filername> cf enable`

3. Determine whether automatic giveback is active by executing the command options `cf.giveback.auto.enable`. If enabled, disable it with the command options cf.giveback.auto.`enable off`.

   Command: `ssh <filername> options cf.giveback.auto.enable`

4. Verify that CPU utilization and disk utilization are both below 50%.
   a. Enter the command sysstat -c 10 -x 3 on each controller in the HA pair.
   b. Confirm that the values in the CPU and Disk Util columns remain below 50% for all 10 measurements reported.
   c. Make sure that no additional load is added to the system throughout the NDU process.

   Command: `ssh <filername> sysstat –c 10 –x 3  or  sysstat –x 5`

   Perform the software installation operation of the new version of Data ONTAP on both storage controllers.

5. Issue the download command on both controllers to update the compact flash boot media.
   a. You can also use the `software update –r` command instead of software install followed by the download command, but you **must** include the -r flag to control when the controller reboot occurs.

   Commands: `ssh <filername> software list` → this will list the uploaded latest software

   `ssh <filername> software update  –r` → this will extract and update the Ontap software on compact flash card.

   (Or)

`ssh <filername> software install` (this also does the same extraction)(above command is highly recommended)

Then,

`ssh <filername> download` or do `ssh <filername> and perform "download"`

6. Confirm that controller failover is enabled and that CPU utilization and disk I/O do not exceed 50% per controller.

7. Issue the `cf takeover` command on controller A (do not use the -f parameter).

   Note: Before TO/GB , Check the following.

   - Stop all active system jobs (dedup, snapmirror, snapvault, snapshots, etc).
   - Don't perform additional management actions (such as deleting a lot of snapshots, volumes, etc).
   - Ensure each node is under 50% usage. Reduce load if usage is high and ensure no additional workload starts during when all data is served on a single node.

   Controller B shuts down cleanly and reboots.

   Once Ontap is installed this will gives a message as " software install completed successfully"

   EG:

```
Netapp09> software update 7311P2_setup_q.exe -r

software: You can cancel this operation by hitting Ctrl- C in the next 6
seconds. software: Depending on system load, it may take many minutes
software: to complete this operation. Until it finishes, you will software:
not be able to use the console.
software: installing software, this could take a few minutes...
software: Data ONTAP Package Manager Verifier 1
software: Validating metadata entries in /etc/boot/NPM_METADATA.txt
software: Checking sha1 checksum of file checksum file: /etc/boot/NPM_FCSUM-
x86-64.sha1.asc software: Checking sha1 file checksums in /etc/boot/NPM_FCSUM-
x86-64.sha1.asc
software: installation of 7311P2_setup_q.exe completed.
Fri Oct 23 22:42:18 CDT [adc15ntap09: rc:info]: software: installation of
7311P2_setup_q.exe completed.
```

   When you use the software update command without the -d option, the download command

   Then

   At the console of system B, enter the following command:
   Note: Before TO/GB , Check the following.

   - Stop all active system jobs (dedup, snapmirror, snapvault, snapshots, etc).

- Don’t perform additional management actions (such as deleting a lot of snapshots, volumes, etc).
- Ensure each node is under 50% usage. Reduce load if usage is high and ensure no additional workload starts during when all data is served on a single node.

```
cf takeover
```

This command causes system A to shut down gracefully and leaves system B in takeover mode.

8. To display the LOADER boot prompt at the system A console, press Ctrl-C at the system A console when instructed after the boot sequence starts.

   You can also display the LOADER prompt by pressing Ctrl-C at the system A console when the "Waiting for giveback" message appears at the console of system A. When prompted to halt the node rather than wait,

   enter y.

9. After halting the node, check the Boot Loader messages for a warning similar to the following:

   ```
   Warning: The CompactFlash contains newer firmware image (1.6.0). Please run
   'update_flash' at Loader prompt to update your system firmware (1.5X3).
   ```

   If you... Then...

   Do not see this warning. BIOS firmware is updated automatically if needed; go to Step 13.

   See this warning. You must update BIOS firmware manually; go to the next step.

   After the new BIOS system firmware is installed, future system firmware updates take place automatically.

   Attention: The version of BIOS system firmware that ships with Data ONTAP 8.0 and higher is the minimum requirement for running this Data ONTAP release. If your system is running a lower level of system firmware, you cannot boot Data ONTAP 8.0 and the upgrade fails.

10. At the boot prompt, enter the following command to reset the system: bye

11. Display the LOADER boot prompt again at the system A console by repeating Step 7.

12. Enter the following command:

    ```
    update_flash
    ```

    The system updates the firmware, displays several status messages, and displays the boot prompt.

13. Enter the following command to reboot the system using the new firmware and software:

    ```
    bye
    ```

14. Choose the option that describes your configuration.

    Then when the "`Waiting for giveback`" message appears on the console of system A...

    Attention: The `cf giveback` command can fail because of open client sessions (such as CIFS sessions), long-running operations, or operations that cannot be restarted (such as tape backup or SyncMirror resynchronization). Use force method if needed otherwise do the following

    - Stop all active system jobs (dedup, snapmirror, snapvault, snapshots, etc).
    - Don't perform additional management actions (such as deleting a lot of snapshots, volumes, etc).
    - Ensure each node is under 50% usage. Reduce load if usage is high and ensure no additional workload starts during when all data is served on a single node.

    ```
    cf giveback -f
    ```

    Note: At this point in the upgrade procedure—system A is running the new Data ONTAP version and system B is running an earlier Data ONTAP release family— the systems are in a state of "version mismatch." This means that normal high-availability functions such as NVRAM mirroring and automatic takeover are not in effect. You might see error messages indicating version mismatch and mailbox format problems. This is expected behavior; it represents a temporary state in a major nondisruptive upgrade and is not harmful. You should complete the upgrade procedure as quickly as possible; do not allow the two systems to remain in a state of version mismatch longer than necessary.

15. Choose the following option that describes your configuration.

    If you have CIFS... Then...

    If it is not in use in system B Go to the next step.

    If it is in use in system B Enter the following command?

    ```
    cifs terminate -t nn
    ```

    nn is a notification period (in minutes) appropriate for your clients after which CIFS services are terminated. After that period of time, proceed to the next step.

16. At the console of system A, enter the following command:

    Note: Before TO/GB , Check the following.

    - Stop all active system jobs (dedup, snapmirror, snapvault, snapshots, etc).
    - Don't perform additional management actions (such as deleting a lot of snapshots, volumes, etc).
    - Ensure each node is under 50% usage. Reduce load if usage is high and ensure no additional workload starts during when all data is served on a single node.

    ```
    cf takeover -n
    ```

    This command causes system B to shut down cleanly, flushing file-system information in memory to disk.

Note: The -n flag of the `cf takeover` command should only be used for major non-disruptive upgrades. If run during a minor non-disruptive upgrade or a non-upgrade takeover, it generates an error and the command terminates.

16. After the node halts, check the Boot Loader messages for a warning similar to the following:

    Warning: The CompactFlash contains newer firmware image (1.6.0). Please run `'update_flash'` at Loader prompt to update your system firmware (1.5X3).

    If... Then...

    You do not see this warning BIOS firmware is updated automatically if needed; go to Step 20.
    You see this warning You must update BIOS firmware manually; go to the next step.

    After the new BIOS system firmware is installed, future system firmware updates take place automatically.

17. At the boot prompt, enter the following command to reset the system:

    ```
    bye
    ```

18. To display the LOADER boot prompt at the system B console, press Ctrl-C at the system B console when instructed after the boot sequence starts.You can also display the LOADER prompt by pressing Ctrl-C at the system A console when the "Waiting for giveback" message appears at the console of system B. When prompted to halt the node rather than wait, enter y.

19. Enter the following command:

    ```
    update_flash
    ```

    The system updates the firmware, displays several status messages, and displays the boot prompt.

20. At the console of system B, enter the following command to reboot the system using the new system firmware (if it was installed) and software:

    ```
    bye
    ```

21. Choose the option that describes your configuration.

    Then when the "Waiting for giveback" message appears on the console of system B...

    Is not in use in system B Enter the following command at the console of system A:
    Note: Before TO/GB , Check the following.

    - Stop all active system jobs (dedup, snapmirror, snapvault, snapshots, etc).
    - Don’t perform additional management actions (such as deleting a lot of snapshots, volumes, etc).
    - Ensure each node is under 50% usage. Reduce load if usage is high and ensure no additional workload starts during when all data is served on a single node.

```
cf giveback
```

22. Verify that controller failover is enabled with the cf status command. Both controllers are now running the new version of Data ONTAP.

    Command: `ssh <filername> version -b` → to verify the latest Ontap version is upgraded or not. It should show like this,

```
netapp> version -b
1:/x86_64/kernel/primary.krn: OS 7.3.1.1P2      → This is the latest version
just upgraded.

1:/backup/x86_64/kernel/primary.krn: OS 7.2.4P7 1:/x86_64/diag/diag.krn: 5.3.6
1:/x86_64/firmware/excelsio/firmware.img: Firmware 1.6.0
1:/x86_64/firmware/DrWho/firmware.img: Firmware 2.2.0 1:/boot/loader: Loader
1.6
```

    Also check for the cluster status using command : `cf status`

23. Verify the latest Ontap version by,

    Command: `ssh <filername> version -b`
    E.g.:

```
newnan:~ #
newnan:~ # rsh eg-nascorpbkp-f02 version -b
/cfcard/x86_64/freebsd/image1/kernel: OS 8.0.1P5
/cfcard/x86_64/freebsd/image2/kernel: OS 8.0.1
/cfcard/backup/x86_64/kernel/primary.krn: OS 7.3.3P3
/cfcard/x86_64/diag/diag.krn:  5.4.7
/cfcard/x86_64/firmware/excelsio/firmware.img: Firmware 1.9.0
/cfcard/x86_64/firmware/DrWho/firmware.img: Firmware 2.5.0
/cfcard/x86_64/firmware/SB_XV/firmware.img: Firmware 4.4.0
/cfcard/x86_64/firmware/SB_XVI/firmware.img: Firmware 5.1.0
/cfcard/x86_64/firmware/SB_XVIII/firmware.img: Firmware 7.0.1
/cfcard/boot/loader: Loader 1.7
/cfcard/common/firmware/zdi/zdi_fw.zpk: PAM II Firmware 1.10 (Build 0x201012200653)
/cfcard/common/firmware/zdi/zdi_fw.zpk: X1936A FPGA Configuration PROM 1.0 (Build 0x200706131558)
newnan:~ #
```

5 Upgrading system BIOS manually:

Note: (This step is needed only when upgrading RLM/BMC/system BIOS Firmware) (step 12) if not continue to step 14,

E.g.: Upgrading System BIOS

Go to Item 10 on ONTAP Upgrade step, and then follow below

```
Phoenix TrustedCore(tm) Server
Copyright 1985-2004 Phoenix Technologies Ltd. All Rights Reserved
BIOS version: 2.2.0
Portions Copyright (c) 2006 Network Appliance, Inc. All Rights Reserved CPU= Dual
Core AMD Opteron(tm) Processor 265 X 2
Testing RAM 512MB RAM tested

8192MB RAM installed
Fixed Disk 0: NACF1GBJU-B11

System Configuration Data updated
Boot Loader version 1.6
Copyright (C) 2000-2003 Broadcom Corporation.
Portions Copyright (C) 2002-2008 NetApp

CPU Type: Dual Core AMD Opteron(tm) Processor 265

Starting AUTOBOOT press Ctrl-C to abort...      -→ Press Ctrl+C

Netapp > halt -f

Sat Sep 12 00:35:56 CDT [netapp: kern.shutdown:notice]: System shut down because :
"halt".
Sat Sep 12 00:36:00 CDT [netapp: pvif.allLinksDown:CRITICAL]: vifc-11: all links
down
Sat Sep 12 00:36:01 CDT [netapp: pvif.allLinksDown:CRITICAL]: vifa-11: all links
down
Sat Sep 12 00:36:01 CDT [netapp: pvif.allLinksDown:CRITICAL]: vifb-11: all links
down
Sat Sep 12 00:36:05 CDT [netapp: cf.fsm.firmwareStatus:info]: Cluster monitor:
partner halted

Phoenix TrustedCore(tm) Server
Copyright 1985-2004 Phoenix Technologies Ltd. All Rights Reserved
BIOS version: 2.1.0
Portions Copyright (c) 2006 Network Appliance, Inc. All Rights Reserved CPU= Dual
Core AMD Opteron(tm) Processor 265 X 2
Testing RAM 512MB RAM tested
```

```
8192MB RAM installed
Fixed Disk 0: NACF1GBJU-B11


Boot Loader version 1.2.3
Copyright (C) 2000,2001,2002,2003 Broadcom Corporation.
Portions Copyright (C) 2002-2006 Network Appliance Inc.

CPU Type: Dual Core AMD Opteron(tm) Processor 265

Warning: The CompactFlash contains newer firmware image (2.2.0). Please run
'update_flash' at Loader prompt to update your
system firmware (2.1.0).

LOADER> update_flash    → this will land in LOADER prompt and then use command:
update_flash

New BIOS Version: 2.2.0
New Loader Version: 1.6
Saving Primary Image to Secondary
Programming .+.+ .+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+.+ done.
2097152 bytes written Updating Primary Boot Flash
Programming .+.+.+.+.+.+.+.+.+.+.+.+.+.+.+ done. 917504 bytes written
LOADER> bye → This is to quit the loader prompt
```

Issue the halt command on controller A to shut it down cleanly.

When controller B detects that controller A is shut down cleanly, it initiates a takeover. System BIOS, RLM, or BMC firmware can be upgraded while controller A is down.

You can also use this opportunity to perform hardware maintenance or upgrades, if necessary. (follow Option 11 steps to upgrade FW)

When takeover and any additional maintenance operations are completed, issue the boot_ontap or bye command on controller A.

Next go to Item: 11 (ONTAP upgrade steps)

The –n (cf takeover –n) parameter applies only to major version NDU operations. The following message appears: ―Waiting for partner to be cleanly shutdown using the 'halt' command. Press Ctrl-C to abort wait...‖.

6 RLM upgrade

There are two ways to install RLM FW upgrades,

a. Using the Data ONTAP™ Command Line Interface (CLI)
b. Using the Remote LAN Module (RLM) Command Line Interface (CLI)

Procedure using method (a):: Which is the easy way of doing this.

Installation prerequisites

- You need to have access to a web server on a network accessible to your appliance OR
- You need to mount the root volume of the appliance as an NFS volume or CIFS share
- You need to have access to the Data ONTAP CLI
- You must use the Data ONTAP console or RLM “system console” session to update RLM firmware

Downloading and installing the firmware using the Data ONTAP CLI
Attention: Do not use a Data ONTAP telnet/ssh session to upgrade RLM firmware.

Step 1: At the Data ONTAP CLI, enter the following command to verify that the current RLM firmware version is older than the one you are planning to download and install:

Attention: Do not use a Data ONTAP telnet/rsh session to upgrade RLM firmware.

```
appliance_name> rlm status
```

Where appliance_name is the name you assigned to your appliance.

You will see the following system messages:

```
Remote LAN Module
Status: Online
Part Number: xxx-xxxxx
Revision: xx
Serial Number: xxxxxx
Firmware Version: x.x.x
```

If the RLM firmware version is older than what we are going to install then,

Step 2 : Click on link http://now.netapp.com/NOW/download/tools/rlm_fw/

The above link gives the list of available versions select the appropriate version, it takes you to next screen <accept> ,it goes to the below link (if version 3.1,it take to the below link)(http://now.netapp.com/NOW/download/tools/rlm_fw/3.1.0/ontap_cli.shtml)

From the above link on step 2,it gives the link to download the RLM_FW.zip option. Click on RLM_FW.zip to download the file from this NOW site

Step 3: Copy the downloaded RLM_FW.zip file to the root volume's /etc/software directory.

Step 4: At the filer console, enter the following command to list the available install packages:

```
appliance_name> software list
```

This should list the `RLM_FW.zip` file just copied to the `/etc/software` directory:

```
appliance_name> software list

RLM_FW.zip 71_setup_i.exe
```

Step 5: At the filer console, enter the following command to install the copied firmware file, ensuring that the file name is exactly as it was listed in the output from the preceding step:

```
appliance_name> software install RLM_FW.zip
```

You will see the following system messages:

```
software: installing software, this could take a few minutes...
software: installation of RLM_FW.zip completed.
```

Step 6: Enter the following command to update the RLM with the new firmware:

```
appliance_name> rlm update
```

You will see the following system messages:

```
Updating the RLM firmware.
DO NOT reset this system during this process.
New RLM version : x.x.x
Sending files to RLM...
Current RLM version : x.x.x
Installing package on RLM...
RLM: Firmware updated successfully!
```

Step 7: When the system prompts you to reboot the RLM, enter y to continue.
Note: Wait for 60 seconds to allow the RLM to reboot.

Step 8: At the filer console, enter the following command to verify that the RLM has been updated with the new firmware:

```
appliance_name> rlm status
```

You will see the following system messages:

```
Remote LAN Module
Status: Online
```

```
Part Number: xxx-xxxxx
Revision: xx
Serial Number: xxxxxx
Firmware Version: x.x.x
```

The firmware update process is complete.