

# STORAGE SUPPORT

PROCESS CONTROL MANUAL (PCM) - NAS

Document version 0.15  
Date of issue: TBD



THOMSON REUTERS™

## REVISION HISTORY

| Name                             | Date      | version | Summary of changes  |
|----------------------------------|-----------|---------|---|
| Fai Liu                          | 18MAY2016 | 0.1     | Initial   |
| Fai Liu                          | 12OCT2016 | 0.2     | NAS Host list gathering   |
| Fai Liu                          | 31OCT2016 | 0.3     | Added sections for WFA, Storage increase, exports edit and on NDU upgrade, Filer panic                              |
| Fai Liu                          | 22NOV2016 | 0.4     | Added Volume Offline, stale snapmirrors   |
| Shrinath Kurdekar                | 15DEC2016 | 0.5     | Reformatted document format   |
| Shrinath Kurdekar                | 22DEC2016 | 0.6     | Updated Section 1 and Added Section 2 & 3   |
| Shrinath Kurdekar                | 05JAN2017 | 0.7     | Updated Sections 4.1 to 4.4   |
| Shrinath Kurdekar                | 23JAN2017 | 0.8     | Completed sections till 4.14  |
| Shrinath Kurdekar                | 15Feb2017 | 0.9     | Added 7-mode cifs, technology refresh sections  |
| Shrinath Kurdekar                | 31MAR2017 | 0.10    | Updated with Feedback from Ian Daniels from Engineering, George, Nirmal, Renjith and Fai                            |
| Shrinath Kurdekar/Bharath Vedium | 21APR2017 | 0.11    | Separated Provisioning procedures into different document and added link.   |
| Shrinath Kurdekar                | 25APR2017 | 0.12    | Document Issued to support  |
| Shrinath Kurdekar                | 30JUN2017 | 0.12    | No version change to main PCM document. Cross site notes were added to storage provisioning procedures document     |
| Rajesh Reddy                     | 31AUG2017 | 0.13    | Added License keys update procedure post HW replacements  |
| Ramesh Kollimarla                | 09SEP2017 | 0.13    | Updated Archive log thin mitigation and 7-mode backup filer thin mitigation   |
| Shrinath Kurdekar                | 18SEP2017 | 0.13    | Updated delivery defect re-work process in section 4.4.5 and general guidelines for Thin mitigation process         |
| Navaneeth Mandala                | 18SEP2017 | 0.13    | Updated Vol move Process for c-DOT thin mitigation on shared filers   |
| Keerthi K M                      | 18SEP2017 | 0.13    | Added Reallocation procedures   |
| Fai Liu                          | 17JAN2018 | 0.14    | Added overcommit on dedicated Filers. TRP standard on Backup Filer. Expanded on PME script checker                  |
| Fai Liu                          | 09AUG2018 | 0.15    | Expanded Break locks, added CIFS management. Amended for TR and FR support groups. Added SSH Key Process, IAAS Grow |

## REVIEW HISTORY

| Reviewer Name     | Doc Version Reviewed | Date Sent for review | Date Review Filed | Approved/Rejected (with Reasons) |
|-------------------|----------------------|----------------------|-------------------|----------------------------------|
| DCO-STO-SUPP-NAS  | 0.12                 | 26APR2017            |                   |                                  |
| DCO-STO-SUPP-MGMT | 0.9                  |                      |                   | Approved                         |

|                            |      |           |  |  |
|----------------------------|------|-----------|--|--|
| DCO-STO-SUPP-MGMT, Authors | 0.13 | 13SEP2017 |  |  |
| Dco-sto-supp-mgmt, authors | 0.15 | 10AUG2018 |  |  |
|                            |      |           |  |  |
|                            |      |           |  |  |
|                            |      |           |  |  |

Note It is the author's responsibility to send this document out for review, making entries into columns 1-3

Note It is the reviewers' responsibility to complete columns 4-5 and return the reviewed document to the author

# CONTENTS

|   |    |
|---|----|
| PROCESS CONTROL MANUAL (PCM) - NAS  | 1  |
| About this document   | 7  |
| 1.1 Intended readership   | 7  |
| 1.2 In this guide   | 7  |
| 2 Roles and responsibilities  | 8  |
| 3 Infrastructure Overview   | 8  |
| 3.1 DC locations  | 8  |
| 3.2 BU classification   | 8  |
| 3.3 Team's Overview   | 8  |
| 4 NETAPP  | 12 |
| 4.1 Infrastructure overview   | 12 |
| 4.1.1 What is SIP and POD?  | 12 |
| 4.1.2 CPS (ECOM) and CIS(CORP):   | 12 |
| 4.1.3 What's a COLO?  | 13 |
| 4.1.4 What's a MGMT module?   | 13 |
| 4.1.5 Standard Stacks   | 13 |
| 4.2 Standards:  | 13 |
| 4.2.1 Architecture Standards  | 13 |
| 4.2.2 Engineering Standards   | 14 |
| 4.3 Access and Monitoring   | 16 |
| 4.3.1 DFM architecture:   | 16 |
| 4.3.2 DFM Scripts   | 16 |
| 4.3.3 Adding ssh keys to DFM  | 16 |
| 4.4 Builds and storage provisioning:  | 20 |
| 4.4.1 Infrastructure Builds:  | 20 |
| 4.4.2 BAU Storage Provisioning:   | 20 |
| 4.4.3 Emergency/Loaner Storage Provisioning:                                | 20 |
| 4.4.4 Decommissioning procedures  | 21 |
| 4.4.5 Delivery Re-Work process  | 22 |
| 4.5 Daily Checks and Reports  | 22 |
| 4.5.1 Capacity reports used for planning thin mitigation:                   | 22 |
| 4.5.2 Snapvault Lag Reports:  | 22 |
| 4.5.3 Audit Reports:  | 22 |
| 4.6 BAU Maintenance   | 23 |
| 4.6.1 Considerations while Executing changes and working on Major Incidents | 23 |
| 4.6.2 Maintenance Windows   | 23 |
| 4.6.3 Power Maintenance Event   | 23 |
| 4.6.4 What is a PAS and how to raise it?                                    | 28 |
| 4.6.5 Disk Failures   | 31 |

|        |  |     |
|--------|--|-----|
| 4.6.6  | Power supply Failures  | 31  |
| 4.6.7  | Bad FH   | 31  |
| 4.6.8  | Filer interface Down   | 35  |
| 4.6.9  | Adding protocols license to NetApp controller  | 39  |
| 4.6.10 | Snapvault Lags   | 41  |
| 4.6.11 | IAAS Growth – NFS and CIFS   | 41  |
| 4.6.12 | CDOT/7MODE Growth iSCSI  | 45  |
| 4.6.13 | CDOT/7MODE Instructions  | 45  |
| 4.7    | BU Environments  | 45  |
| 4.8    | capacity planning  | 45  |
| 4.8.1  | Guidelines to be strictly followed for all thin mitigation:                                  | 45  |
| 4.8.2  | Aggregate Utilization at 75% on Primary Shared Filers(7-mode):                               | 47  |
| 4.8.3  | Aggregate Utilization at 75% on Primary Shared Filers(c-DOT):                                | 49  |
| 4.8.4  | Aggregate Utilization at 75% on Archive Log Filers (7-mode and c-DOT):                       | 53  |
| 4.8.5  | Aggregate Utilization at 85% on Backup Filers(7-mode):                                       | 57  |
| 4.8.6  | Aggregate Utilization at 85% on Backup Filers(c-DOT): <Placeholder. TBA>                     | 60  |
| 4.8.7  | Aggregate Utilization at 75% or higher on Dedicated Filers(7-mode/c-DOT): <Placeholder. TBA> | 60  |
| 4.9    | Life cycle management  | 60  |
| 4.9.1  | 7-mode Ontap Upgrade process   | 61  |
| 4.10   | technology refresh   | 61  |
| 5      | Troubleshooting  | 65  |
| 5.1.1  | Single/Dual controller Panic   | 65  |
| 5.1.2  | Flexclone Issues   | 66  |
| 5.1.3  | How to gather host list when a filer node is down or when exports are deleted?               | 67  |
| 5.1.4  | Controller Down during PME event   | 67  |
| 5.1.5  | NFS locks and handling NFS lock issues   | 68  |
| 5.1.6  | Stale SnapMirrors  | 72  |
| 5.1.7  | Performance Troubleshooting  | 75  |
| 5.1.8  | CIFS Management  | 78  |
| 5.2    | Vendor Engagement  | 91  |
| 5.2.1  | How to raise a Netapp case?  | 91  |
| 5.2.2  | How to escalate issues to SAM?   | 92  |
| 5.2.3  | How to check if a EOSL system is under SMS support?  | 92  |
| 5.2.4  | How to manually log a case with SMS Support?   | 92  |
| 5.3    | Exception List   | 92  |
| 5.4    | Appendix   | 92  |
| 5.4.1  | How to configure a new Vlan?   | 92  |
| 5.4.2  | How to raise a PCA?  | 92  |
| 5.4.3  | Raising a Major Incident   | 95  |
| 5.4.4  | Bug Database and Key Known Bugs  | 95  |
| 5.4.5  | How to Open a Netapp case through Web  | 96  |
| 5.4.6  | Offline volumes (prior to deletion)  | 100 |
| 5.5    | Oracle ZFS   | 104 |

Document version 0.15  
Date of issue : TBD



## **ABOUT THIS DOCUMENT**

### **1.1 INTENDED READERSHIP**

This document is intended for use by Storage Support staff and also to limited usage by the Storage Altitude team at Thomson Reuters. This PCM should be used as a reference manual for any task being performed by every individual in the storage team as it clearly outlines all the Technical steps and processes to be followed. This will ensure we have a consistent way of performing changes to our infrastructure and avoid the following:

- Misconfigurations in the environment resulting from a missed execution step
- Reduce risk/impact to the infrastructure
- Human Errors

It is imperative the process and steps outlined in here are expected to be followed by every individual in the team. Any deviation to the processes outlined here will need email approval from DCO-STO-SUPP-MGMT.

### **1.2 IN THIS GUIDE**

This documents the core processes and procedures used by Storage Support Staff at Thomson Reuters. This will include but not limited to

- TR Storage Standards
- Life Cycle Management
- Capacity Planning
- Roles and Responsibilities
- Standard processes/procedures
- Interaction with DCIS teams
- BAU maintenance
- Troubleshooting guide

## 2 ROLES AND RESPONSIBILITIES

All employees are expected to adhere to the role and responsibilities as defined in the [Employee Handbook](#) and follow the guidelines per the handbook. The Employee Handbook also defines the roles and core functions of the support group which you should make yourself familiar with.

With the split with TR and F&R NewCo, there are also two sharepoint portal sites for each group. The F&R NewCo portal site is initially a copy of the TR site. Expect to see F&R NewCo specific data on this site in time.

TR: [https://theshare.thomsonreuters.com/sites/DCO\\_Storage/SitePages/Home.aspx](https://theshare.thomsonreuters.com/sites/DCO_Storage/SitePages/Home.aspx)

F&R NewCo: [https://theshare.thomsonreuters.com/sites/DCO\\_Storage\\_FR/SitePages/Home.aspx](https://theshare.thomsonreuters.com/sites/DCO_Storage_FR/SitePages/Home.aspx)

## 3 INFRASTRUCTURE OVERVIEW

### 3.1 DC LOCATIONS

A total of 10 datacenter locations worldwide are deemed Strategic and the remaining datacenters will be consolidated to strategic sites as part of the [Datacenter Rationalization program](#).

Full list of all Strategic and non-strategic sites managed by TR proximity services team refer to link [here](#)

In addition to this we have Standard Infrastructure deployed in some [small office locations](#) that are also managed by the Storage Support team. These locations include (Links reference to site specific documentation):

- Rochester
- [Ahmedabad](#)
- Santa Clara??
- Brazil
- Dubai
- Pampalona
- Cape Town
- Gydnia

With the TR/Blackstone F&R split the datacenter for each specific “company” has been specified on the hub page [here](#).

### 3.2 BU CLASSIFICATION

For Datacenter requirements including Storage, each business unit has an account team, including a business relationship manager (BRM), who will work directly with BU on projects requiring new infrastructure or changes to existing infrastructure. In addition to the BRM, BU architects will work with them on their requirements and own the high-level architectural design

List of All the Business Units at TR, their associated BRM and Solutions architect can be found [here](#)

Please note Each Business Unit listed in here will have sub BU's that support different applications. For Example, F&R has DataScope Select, Transactions, Investment Banking, T1 etc. which are all sub groups under F&R.

### 3.3 TEAM'S OVERVIEW

#### Storage Design and Engineering(D&E)

Responsible for Engineering standards in collaboration with Operational Readiness and Architecture. The team is responsible for designing standard/non-standard solutions, defining the storage roadmap in collaboration with Architecture, planning and designing our LCM roadmap and technology refresh. The teams under D&E structured as below:

- - Storage has been split between FR and TR groups and are relevant DL's
  - [Storage-engineering-TR@thomsonreuters.com](mailto:Storage-engineering-TR@thomsonreuters.com) – TR D&E Team
  - [Storage-engineering-FR@thomsonreuters.com](mailto:Storage-engineering-FR@thomsonreuters.com) – FR D&E Team

LifeCycle management <mailto:Thomson-DCO-STORAGE-LCM-ALL@Thomsonreuters.com>

- Responsible for keeping our code versions current. LCM team manages all BU communications related to Code upgrades. Once the new code standards are tested and published by D&E LCM team will work with Storage support resources and Vendor to complete the code upgrades.
- Separate TR/FR group is to be determined.

### How and When to Engage D&E?

Our D&E team can be engaged using the email DL's listed above. Some examples of when they should be engaged:

1. Questions related to Storage standards when not found in the Engineering standards document
2. Any requests from BU's for non-standard deployments
3. Vendor recommendations to implement non-standard configurations or code deployments
4. Encounter new bugs

### Storage Altitude

Storage Altitude team at TR is an extension of our Support team responsible for L1 Storage related activities. The scope of their services is outlined <here TBA>

Email: <mailto:DCO-Storage-Altitude@thomsonreuters.com>

The Altitude Distribution List is to be determined with the TR/FR split and will be announced in due course

### FLS SYSTEMS

First Level Support at TR provides the following services for Storage:

1. Handles all disk replacements for SAN, NAS and ZFS systems
2. Handles single PSU failures for SAN, NAS and ZFS systems
3. Inode Full alerts
4. Snapshot overflow Incident tickets for 7-mode only through [Automation](#)

Email (Legacy): [FLS-DCO-OPS-AND-CLOUD@thomsonreuters.com](mailto:FLS-DCO-OPS-AND-CLOUD@thomsonreuters.com)

Email (TR): [fls-dco-ops-and-cloud-tr@thomsonreuters.com](mailto:fls-dco-ops-and-cloud-tr@thomsonreuters.com)

Email (FR): [fls-dco-ops-and-cloud-fr@thomsonreuters.com](mailto:fls-dco-ops-and-cloud-fr@thomsonreuters.com)

SNOW Queue (TR): FLS-DCO-OPS-AND-CLOUD-TR

SNOW Queue (FR): FLS-DCO-OPS-AND-CLOUD-FR

## **Storage Delivery**

The Storage delivery team is responsible for handling new infrastructure builds, disk shelf adds and BAU Storage provisioning.

Delivery Infra team handles new Storage builds and capacity adds:

Email (Legacy): [Delivery.StorageInfra@thomsonreuters.com](mailto:Delivery.StorageInfra@thomsonreuters.com)

Email (TR): [Delivery.StorageInfra-TR@thomsonreuters.com](mailto:Delivery.StorageInfra-TR@thomsonreuters.com)

Email (FR): [Delivery.StorageInfra-FR@thomsonreuters.com](mailto:Delivery.StorageInfra-FR@thomsonreuters.com)

SNOW Groups

Legacy - DELIVERY-STORAGE-INFRA

TR - DELIVERY-STORAGE-INFRA-TR

FR - DELIVERY-STORAGE-INFRA-FR

BAU storage provisioning is handled by:

Email (Legacy): <mailto:delivery-storage@thomsonreuters.com>

Email (TR): <mailto:delivery-storage-tr@thomsonreuters.com>

Email (FR): <mailto:delivery-storage-fr@thomsonreuters.com>

SNOW Queue

Legacy: DELIVERY-STORAGE

TR: DELIVERY-STORAGE-TR

FR: DELIVERY-STORAGE-FR

**Other DCIS groups that we closely interact with:**

**SSSE (Systems Software Support and Engineering):**

- UNIX-SUPPORT-TR and UNIX-SUPPORT-FR - Provide support for UNIX systems
- WINDOWS-SUPPORT-TR and WINDOWS-SUPPORT-FR - Provide support for WINDOWS systems
- VIRTUAL-SUPPORT-TR and VIRTUAL-SUPPORT-FR - Provides support for ESX infrastructure within TR

Support assignment of hosts can be found in the asset details within the ITSM tool.

Escalation information for SSSE:

TR - <https://thehub.thomsonreuters.com/docs/DOC-2629090>

FR - <https://thehub.thomsonreuters.com/docs/DOC-2619760>

**ISSE (Infrastructure Software Support and Engineering):**

- MSSQL-SUPPORT-TR and MSSQL-SUPPORT-FR – SQL Support on Windows including MS SQL and MySQL.
- ORACLE-SUPPORT-TR and ORACLE-SUPPORT-FR – Oracle Support on UNIX.

Refer to their HUB site for more information [here](#)

**ENT-LAN (Enterprise Network Technology Team)**

- FLS-NETWORKS – First Level Network Support for Initial Triage.
- NETWORK-SUPPORT – Second Level Network Support. Engaged by FLS-Networks.
- NETWORK-CHANGE – Change Team responsible for Network changes.

Refer to Enterprise Network Technology hub site [here](#)

## 4 NETAPP

### 4.1 INFRASTRUCTURE OVERVIEW

Majority of the Netapp Infrastructure at TR is supported by the DCO Storage Support team. However, we do have few systems like Remote Office Filers, FXALL/Tradeweb filers, TAX professional filers that are managed by Remote office, FXALL/Tradeweb and DCO SSSE team respectively. Filers at TR fall in one of the below 3 categories:

#### ALL Flash Arrays (A700)

New infrastructure for CDOT with all Solid State disks. Will be utilised for both HT and LT requirements with QoS limiting the requirement

#### High Tier Filers

Intended for high IOPS utilisation with typically fast low capacity disks. Typical usage includes Virtual (ESX) Volumes/datastores, LION, WISP stacks.

#### Low Tier Filers

Intended for relatively low IOPS utilisation with high capacity slow disks. Typical usage includes single database servers, database log archiving where latency and IOPS is not a critical factor in the application

#### Backup Filers

Backup Filers typically consist of Filers with high capacity, low speed disks (i.e. 2TB SATA disks). Their intention is for snapvault backups only whereby high IOPS throughput is not a requirement.

#### 4.1.1 What is SIP and POD?

SIP stands for our Standard Infrastructure Platform. This includes the base technology for a Datacentre Module  
POD stands for platforms on demand. POD refers specifically to the compute footprint within SIP.

Netapp NAS and EMC Avamar are part of the Storage and Backup Standard Infrastructure Platform offerings managed by the Storage Support team.

For a high-level overview of POD refer [here](#)

For a detailed overview of POD including Network connectivity (on Slide 9) [here](#)

To learn how Filers are connected to network switches refer [here](#)

#### 4.1.2 CPS (ECOM) and CIS(CORP):

Its key to clearly understand the terms CPS (Customer Product systems) and CIS (Corporate and Internal Systems) as all infrastructure at TR is classified under one of these categories. A CIS or CPS environment is a component of our Strategic Infrastructure Platform (SIP) and contains all the services to support the products hosted within that environment.

A CIS or CPS module is comprised of networking, NAS storage, servers, and key services such as NTP, DNS, AD, load balancing, monitoring, and more

Refer to Architecture position paper here for detailed explanation of what systems classify as CPS and CIS [here](#)

Examples of our Netapp filers classified as CIS or CPS:

CPS: eg-nasecom-h09, ln-naslowep-d01(7-mode), pl-cps-clsp-p01(c-DOT)

CIS: eg-nasclnt-f01, eg-nascorp-h01(7-mode), pl-cis-clbk-p01(c-DOT)

You will learn more about NAS Filer naming standards for both 7-mode and c-DOT in section [Engineering Standards](#)

#### **4.1.3 What's a COLO?**

Colo module is a special module deployed in our strategic datacentres to facilitate migration of legacy infrastructure from non-strategic datacentres to Strategic sites. Colo is sometimes also referenced as transition space and the big rules for colo can be found [here](#). Colo Vlans can be found configured on some of our CPS Filers.

#### **4.1.4 What's a MGMT module?**

A management module is a secure, firewalled environment that hosts the applications necessary for administering our CIS and CPS environments. These applications include things like Splunk, HP Insight Manager, Application tools and Netapp OnCommand. There are two primary benefits we get from running these applications in their own module:

Security: Systems administrators and developers will access their tools in the management module instead of going all the way into the CIS/CPS modules where live data and products are kept.

Business Recovery: In the event of a datacentre outage, all of the critical administrative applications are consolidated in one place instead of scattered. Consequently, recovery is quicker

Please note a Key exception here to Full POD architecture is NO SnapVault. Services deployed in MGMT module will not have snapvault solution and use local snapshots with standard retention.

To learn more about the MGMT module refer [here](#)

*Note: The new 7-mode and c-DOT DFM infrastructure explained in section 4.4 is deployed in the MGMT module. Some of the services like c-DOT are still in the process of being migrated at the time of writing this PCM.*

#### **4.1.5 Standard Stacks**

While working on the NAS infrastructure you will continually come across the terms LION, WIP and WISP. These stacks represent the underlying compute, DB and Storage

LION – Linux Intel Oracle NAS. For more details on LION stack refer [here](#).

WISP - Windows ISCSI SQL Platform. For more details on WISP stack refer [here](#)

WIP – Windows ISCSI Platform – Used for ISCSI deployments for Flat files.

### **4.2 STANDARDS:**

#### **4.2.1 Architecture Standards**

The storage Architecture site can be accessed [here](#). Refer to the STORAGE section for Architecture standards for SAN, NAS and Backups.

Steward Bird is the primary Storage Architect responsible for evaluating and defining the TR Storage Architecture standards in partnership with Storage Engineering and Support.

The below architecture documents reference high level Architecture Standards and are also provide a useful insight into performance workload capabilities for the underlying HW models.

#### **7-mode Standard Architecture**

SIP (POD) Full Size (FAS 6220): [SIP \(POD\) Full Size](#)

Mini and Micro SIP (POD) (FAS 2240 and FAS 3250): [Mini and Micro SIP \(POD\)](#)

Cheap and Deep NAS (FAS 2240): [Low Cost HA NAS \(Cheap and Deep\)](#)

Legacy Standards (FAS 6210): [Legacy Standards](#)

#### **c-DOT Standard Architecture**

SIP (POD) Full Size (FAS 8040): [SIP \(POD\) Full Size](#)

Mini and Micro SIP (POD) (FAS255x): [Mini and Pea SIP \(POD\)](#)



Cheap and Deep NAS (FAS 2554): [Low Cost HA NAS \(Cheap and Deep\)](#)  
Archive Log Standards (FAS 8040): [Archive Log](#)

## Architecture Position Papers

Backup and Archival: [Backups, Archives, Retentions, and Offsite Storage](#)

Multiprotocol Shares on Netapp: [Multi-protocol shares on Netapp](#)

Accessing Netapp Arrays across Network Boundaries: [Accessing Netapp arrays across network boundaries](#)

NFS4 on Netapp for MQ only: [NFSv4 on NetApp](#)

### 4.2.2 Engineering Standards

The TR storage Design and Engineering Team works with Architecture through the Operational Readiness process to test and define the Engineering Standards for Storage:

#### 7-mode Standards

Consolidated Build Standards: [Consolidated Netapp 7-mode Build Standards](#)

7-mode Filer Naming Standards: [7-mode naming](#)

NFS4 and MQ: [NFSv4 7 Mode](#)

LION deployment guidelines: [Thomson Reuters Professional - Oracle on NetApp - Deployment Guidelines v5](#)

WIP and WISP guidelines: [Thomson Reuters - SQL Server and iSCSI on NetApp - Deployment Guidelines v6](#)

MySQL guidelines:<TBA>

ESX Deployment Guidelines: [Thomson Reuters Professional - VMware on NetApp - Deployment Guidelines v13](#) (Note: Some of the information in this document is obsolete and new builds should go to c-DOT. This document should be used as a reference for file restore mechanisms and old standards only.

7-mode Alert Standards: [7-mode Alert Standards](#)

#### c-DOT Standards

c-DOT Build Standards: [CDOT Consolidated Build Standards](#)

c-DOT Naming Standards: [CDOT naming](#)

NFS4 and MQ: [NFS And MQ](#)

LION Guidelines: [Oracle on NetApp cDOT - Deployment Guidelines](#)

WIP and WISP guidelines: [WIP and WISP Procedures on cDOT v1.9 \(2\)](#)

MySQL guidelines: [CDOT-MySQL Deployment Guide v6](#)

Multiprotocol: [Multi-Protocol cDOT](#)

ESX deployment Guidelines: [Thomson Reuters - VMware on NetApp cDOT - Deployment Guidelines v4 \(1\)](#)

c-DOT Alert Standards: [c-DOT Alert Standards](#)

Archive Log Standards: [Thomson Reuters - Log Backups - Deployment Guidelines v11](#)

AV Deployment Guide: [cDOT AV Deployment](#)

AV Standards: [cDOT AV](#)

#### Replication Standards

While Snapmirror replication is available on Netapp this is NOT a standard at TR. Snapmirror should only be used for data migrations only. Any new requirements for Storage based snapmirror replication would need to be granted an exception from Architecture. This exception should be stored on the sharepoint [here](#)

BU architecture should review the requirements and evaluate suitable host based replication mechanisms first. If snapmirror is deemed as the only feasible option, then they should engage the Storage architecture to get this exception documented and approved.

TIP: What to do when you received a request for snapmirror for permanent DR?

Engage Storage D&E and they will work with BU architecture and Storage Architecture to review the requirements.

## **Backup Standards**

Snapvault is the preferred backup mechanism and should be used without exception.

c-DOT: Refer to [section 8](#) for backup standards for c-DOT.

*Some Key points to remember once a snapvault relationship is created:*

- nosnap volumes should not have any snap policies configured.
- LION volumes are backed up using the DBA hotbackup script called “Run\_hotbackup\_netapp.sh”. snapvault is managed through schedule on the filer.
- WISP backups are managed by the DBA team through Snap Manager for SQL including vaulting to secondary/backup filer.
- ESX, non-LION NFS and CIFS backups are managed through the snapvault schedule on the Filer.

**7-mode:** Refer to [section 8](#) for Backup Standards for 7-mode

*Some Key points to remember once a snapvault relationship is created:*

- LION volumes are backed up using the DBA hotbackup script called “Run\_hotbackup\_netapp.sh”. snapvault is managed through schedule on the filer.
- WISP backups on primary are managed by the DBA team. The snapvault process is managed using the lun\_snapvault\_update.pl and lun\_snapvault\_cleanup.pl scripts run from our alarm standby DFMs.
- ESX, non-LION NFS and CIFS backups are managed through the snapvault schedule on the Filer.

## **QOS Standards for c-DOT**

Key things to note on QOS (Quality of Service) Policy on c-DOT:

- Our standard QoS Policy is based on IOPS, and set to 6000 IOPS per volume on **SHARED** filers only. **DO NOT** ENABLE QOS for volumes on dedicated filers unless approved as an exception by Engineering.
- If a customer is experiencing issues related to the 6000 IOPS policy, we should continue to investigate these on a case by case basis:
  - For now, we will not be asking customers to purchase more storage if they need more than 6000 IOPS
  - Engineering are reviewing the best approach and communication path to customers hitting QOS limits at the time of writing this document. Until we do, we should not be telling customers they should purchase more storage. We should evaluate the requirements, and adjust accordingly with approval from the Storage PCA Group.

## 4.3 ACCESS AND MONITORING

All systems should be accessed through [DCAG](#) and the following accounts should be used to manage the infrastructure:

- MGMT\M-account for managing CPS infrastructure and WFA
- TENNU-account for managing CIS infrastructure
- Generic shared accounts for Ex-Markets filers. Accessed through Global keychain.
- Legacy access mechanism through Citrix/VDI should NOT be used and will be phased out.

**Note:** Root account should not be used to administer the storage systems. Unauthorized use of root account for BAU activities without prior approval could result in disciplinary action.

### 4.3.1 DFM architecture:

The DFM servers at TR are classified as below:

1. Alerting DFM's – One primary/Standy DFM per CIS/CPS environment to handle alerting to EMAT/GMI
2. Performance DFM's
3. Jumpboxes – Should be used to connect to filers and for deployment for pre-approved scripts

#### 7-mode:

The 5.2.1 7-mode DFM architecture can be found [here](#). The link to the overall design plan can be found [here](#).

There are three strategic jump boxes located in Hong Kong, DTC and Eagan datacenters. Engineers should not access Filers directly for administration. All access should be undertaken via the jump boxes using your own account.

| DNS Name                                 | Location  | IP            | Host Name |
|--|-----------|---------------|-----------|
| dfm7-dco-jump-e01.int.thomsonreuters.com | Eagan E   | 159.42.128.16 | C152mad   |
| dfm7-dco-jump-d01.int.thomsonreuters.com | DTC       | 159.42.68.33  | C659xxa   |
| dfm7-dco-jump-k01.int.thomsonreuters.com | Hong Kong | 159.42.16.1   | C155fmj   |

#### c-DOT:

The current c-DOT infrastructure is managed through version 5.2.1 DFM server. [List here](#)

A new OCUM infrastructure is in the process of being deployed. The architecture diagram can be found [here](#). The link to the overall plan can be found [here](#).

### 4.3.2 DFM Scripts

The list of scripts running on our DFM infrastructure, their location and functionality can be found [here](#).

### 4.3.3 Adding ssh keys to DFM

Process to add ssh keys to the jumpbox and propagate to the infrastructure. This will allow single sign on once logged on to the jumpboxes.

EXIT SUDO BASH.

THIS MUST BE RUN FROM YOUR USER ACCOUNT.  
THIS MUST BE RUN FROM YOUR TEAMS JUMPBOX (c152mad TR or c659xxa FR)  
DO NOT RUN ACCESS FOR FR USER FROM TR JUMPBOX OR VICE VERSA OR ACCESS WILL BE  
WRONG!!!

Run ssh-keygen as your user from one of the jump boxes:

```
> ssh-keygen -t rsa -b 4096 -a 100
```

Press enter through all prompts, accepting the defaults:

```
Generating public/private rsa key pair.
```

```
Enter file in which to save the key (/home/u#####/.ssh/id_rsa):
```

```
Enter passphrase (empty for no passphrase):
```

```
Enter same passphrase again:
```

```
Your identification has been saved in /home/u#####/.ssh/id_rsa.
```

```
Your public key has been saved in /home/u#####/.ssh/id_rsa.pub.
```

```
The key fingerprint is:
```

```
b2:0e:e9:8c:ff:9c:5e:1f:ff:d3:63:92:ef:2e:ce u#####@c152mad
```

```
The key's randomart image is:
```

```
+--[ RSA 2048]----+
```

```
| |  
| |  
| |  
| |  
| . S |  
| .. o |  
| + .o+ |  
|o..=+B |
```

```
| ... +=.          |
+-----+
```

The keys will be saved to your home directory under a hidden folder called .ssh  
Your private key will be called id\_rsa  
Your public key will be called id\_rsa.pub  
You may see another file in .ssh called known\_hosts

## Moving your public key to the deployment folder

Make a directory for your public key:

```
> mkdir /filers/admin/scripts/conf/pub_keys/m#####
```

Copy your public key to this directory:

```
> cp ~/.ssh/id_rsa.pub /filers/admin/scripts/conf/pub_keys/m#####
```

## Moving keys (public/private) to other machines

To move your SSH keys to the other jump/script boxes, from the server without keys run:

**NOTE: Your private key (id\_rsa) should reside *only* on the 3 jump boxes. Never give out your private key**

```
> scp -r $remotejump:~/ssh ~
```

## Scripted public key deployment

This needs to be done by an engineer who already has keys deployed on the filers and requires the filer root volume be exported to the server where run.

## 7MODE

```
> for i in `cat /etc/dfm/filer.list`; do echo $i;
/filers/admin/scripts/support/adduser.pl -f $i -u m##### -k
/filers/admin/scripts/conf/pub_keys/m#####/id_rsa.pub; done;
```

## CDOT

```
> for i in `cat /etc/dfm/cfiler.list`; do echo $i;
/filers/admin/scripts/support/cdot_sshkey_deploy.pl -f $i -u m##### -k
/filers/admin/scripts/conf/pub_keys/m#####/id_rsa.pub; done;
```

## Test Access

### 7MODE

Test 7mode access - this will try to get the version for every 7mode filer:

```
for i in `cat /etc/dfm/filer.list`; do echo $i; ssh -o StrictHostKeyChecking=no -o ConnectTimeout=10 -o BatchMode=yes $i version; done;
```

## CDOT

Test CDOT access - this will try to get the version of every CDOT cluster:

```
for i in `cat /etc/dfm/cfiler.list`; do echo $i; ssh -o StrictHostKeyChecking=no -o ConnectTimeout=10 -o BatchMode=yes $i version; done;
```

## Manual public key deployment

### 7MODE

Create the user and add to the Administrators group. This is a local user on the filer, password does not refer to your domain password. Please input a STRONG password to keep the filer secure. No need to remember this password.

```
> ssh root@$filer useradmin user add $id -g Administrators -p '$password'  
Mount the filer root/vol0:
```

```
> mount $filer:/ /mnt/tmpmnt
```

Create directories for public key:

```
> mkdir -p /mnt/tmpmnt/etc/sshd/$id/.ssh
```

Copy public key to authorized\_keys file:

```
> cp /filers/admin/scripts/conf/pub_keys/$id/id_rsa.pub  
/mnt/tmpmnt/etc/sshd/$id/.ssh/authorized_keys
```

Set permissions:

```
> chmod -R 644 /mnt/tmpmnt/etc/sshd/$id/.ssh
```

## CDOT

Create the user, assign role, and set auth method:

```
> ssh admin@<cdot filer> login create -username <userid> -role admin -application ssh -  
authmethod publickey
```

Assign public key to users key index:

```
> ssh admin@<cdot filer> login publickey create -username <userid> -index 0 -publickey  
'“<key goes here>”'
```

## 4.4 BUILDS AND STORAGE PROVISIONING:

### 4.4.1 Infrastructure Builds:

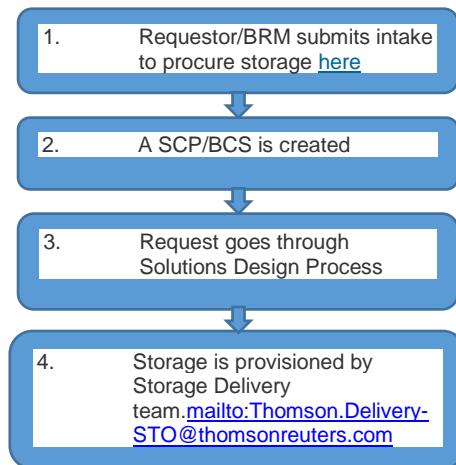
New Infrastructure builds at TR are handled by the Storage delivery Infrastructure team. This involves the following:

- Build of new Netapp cluster
- Hardware upgrades to existing cluster. Ex: Disk shelf additions

Once a new cluster is built and QA per standards storage delivery team will notify Netapp and Storage support on production readiness of the newly built cluster.

### 4.4.2 BAU Storage Provisioning:

All BAU storage provisioning requests are handled by the TR Storage-delivery team. Occasionally we may get requests for additional storage space. Unless the request is an Emergency request or temporary loaner please guide the requestor to the process outlined below:



If a requestor is new to intake process they should work with their Business Relationship Manager(BRM). The BRM mapping by BU can be found [here](#)

### 4.4.3 Emergency/Loaner Storage Provisioning:

What is considered as an emergency request?

Requests that cannot wait for the standard delivery timelines (typically 2 weeks) and can lead to application impact if not actioned immediately are classified as Emergency requests. This would typically be filesystems where utilization is at 95% or higher. Exception to this is Virtual team VMWare ESX volumes where 85% is considered as emergency

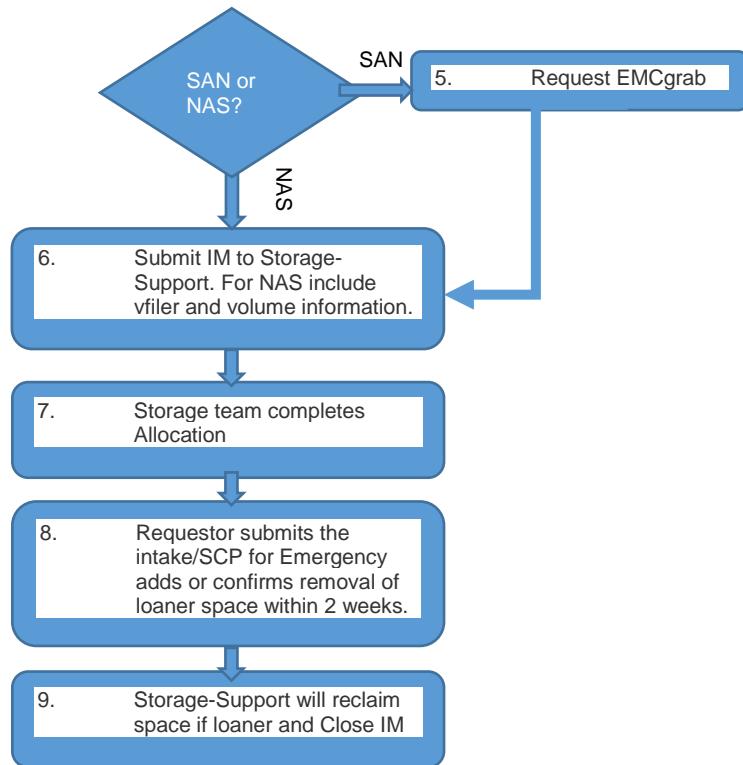
What is considered as a loaner request?

Space add request where the underlying filesystem is at critical utilization levels (95% or above) and loaner space is needed to clean up the filesystem. Notify the requestor that the space should be returned within 2 weeks or an intake/SCP should be submitted to make the space permanent.

All other loaner space requests that are not emergency and high capacity should be reviewed and approved by Storage D&E.

Requests that do not fall in either of the two categories but are still an emergency and cannot wait for Standard delivery process will require a Business Justification and BU director approval.

Process for a request an Emergency/Temporary Loaner space:



## Provisioning Guidelines?

All Storage provisioning should be done through ICO Automation/ServiceNow Workflows where available or using WFA. These workflows take care of end to end configuration and eliminates human errors.

Use of CLI for any of the tasks outline below is strictly prohibited.

A CR should be created for all emergency and loaner Storage add and reclaim requests. Refer section [Storage Provisioning Procedures](#) for step by step instructions on how to provision storage. This should be any storage provisioning activities including activities like thin mitigation, migrations etc.

### 4.4.4 Decommissioning procedures

Infrastructure decommission at TR is handled by DELIVERY-DECOMISSION team. For any Storage infrastructure that needs to be decommissioned an intake request need to be submitted.

Individual servers undergoing decom will have their storage and backup decommissioned as part of this decom process.

To learn more about the process and how to submit the decom intake for any storage infrastructure refer [here](#).

Storage support should not perform any decommissions with the exception of below:

- Removal of older vfiler/volume that were:
  - offline as part of thin mitigation.
  - offline as part of migrations done to address performance issues.

#### **4.4.5 Delivery Re-Work process**

At times, we may run into build issues where in a storage build was NOT completed as per the standards or best practices. In such cases, we may need to work with delivery team and invoke the re-work process to audit and fix such build issue.

Upon encountering a build issue Support engineers should work with their leadership team to determine if the re-work process needs to be invoked. Any immediate risk to the service that needs to be resolved immediately should be taken care by support and subsequently partner with delivery to audit and re-work older builds.

The rework process and tool are documented below:

[Defect Process](#)

[Rework Tool](#)

### **4.5 DAILY CHECKS AND REPORTS**

Below reports are send to dco-sto-supp-nas and should be reviewed upon receipt every day. Click on the link to review the email sent for each report and ensure these are not being filtered from your inbox.

#### **4.5.1 Capacity reports used for planning thin mitigation:**

[c-DOT Aggregate Capacity Report](#)

[7-mode thin report](#)

[7-mode Backup Filer Capacity Report](#)

[7-mode Backup Filer Capacity Alert Report](#)

#### **4.5.2 Snapvault Lag Reports:**

7-mode Snapvault Lag Report

7-mode Snapvault Miss Report

[c-DOT snapvault Lag Report](#)

[c-DOT snapvault Miss Report](#)

[ScholarOne snapvault Lag report](#)

[ScholarOne snapmirror Lag Report](#)

[Ex-Market Lag Report](#)

[TAX GoSystems snapvault report](#)

#### **4.5.3 Audit Reports:**

[BAD FH report](#)

[Broken Interface Report](#)

[Filer Standards Report](#)

[Vfiler Standards Report](#)

[Stale snapmirror Report](#)

## 4.6 BAU MAINTENANCE

### 4.6.1 Considerations while Executing changes and working on Major Incidents

- DO NOT execute any changes to the infrastructure without a valid CR. If a change needs to be implemented to mitigate an ongoing Major Incident this should be done through a PCA. Following the escalation process outlined in the Employee handbook will ensure senior management is aware of ongoing Incident and potential need to implement a change through PCA.
- Do NOT wait until last minute to review a CR assigned to you. Take time to review the CR details and ensure the CR has clear details about the change being performed, link to documentation related to the change, Justification, validation and backout plan. If the details are NOT clear DO NOT proceed with the change and follow-up with your lead or Storage IO.
- Focus on mitigating the incident vs troubleshooting.
- No matter how many times you have executed a change before always reference the PCM. Escalate to DCO-STO-SUPP-MGMT if there is no reference document available.

### 4.6.2 Maintenance Windows

Note the following considerations while scheduling changes during maintenance window:

- All Production changes should be scheduled after Business hours local datacentre time.
- All critical high Risk Storage changes should be scheduled on weekends.
- Certain Global products (Ex: Eikon, Collaboration) have specific low usage window during which the change should be scheduled.
- The only exception to above rules are:
  - Emergency PCA to resolve an on-going business impact that cannot wait for change to be done after business hours.
  - Emergency PCA's for Break-fix Activities scheduled after business hours.
  - Backup changes that need to be scheduled during the standard backup maintenance window 06:00-18:00 Local datacentre time on Wednesdays and Thursdays.

Certain Global Products have specific Low Usage window during which the change should be scheduled. Key Products include:

- **Eikon and Collab Low Usage Window:** Fri 23:00 - Sat 07:00 + Sat 14:00 - Sun 04:00 GMT
- **DSS (DataScope Select) Low usage Window:** Sunday 00:00 GMT - 18:00 GMT
- **DSE/NDA Low Usage window:** Sunday 12:00 GMT - 18:00 GMT
- **World Check One:** Friday and Saturday 23:00 GMT – 03:00 GMT
- **AMS NOVUS:** Sunday 03:00 GMT – 11:00 GMT

### 4.6.3 Power Maintenance Event

Power Maintenance Events (PMEs) are driven by the need to perform essential maintenance on the Mechanical and Electrical plant that supports the TR Data Centers to ensure continued integrity of the infrastructure. Events can

consist of Partial Power Down or Full Power Down and are usually planned to occur over a weekend during agreed maintenance. Each Data Center Power Path will undergo maintenance at least every 3 years.

For a full list of maintenances for the current year refer to the schedule [here](#)

Below is the sequence of events that shape the PME:

1. Publicizing the PME (addition to KeyEvents Calendar and attendance at Inter Service & DCO CABs) – PM/PS team
2. Review of impacted assets to ascertain the impact of the PME to infrastructure/products. – PM/PS Team
3. Assign Support Key Contact(s) for PME and attend PME related meetings – Storage Team Leads
4. The assigned Storage Support should review the asset list shared as part of the kick off meeting to understand:
  - o List of impacted assets (assets which will lose full power)
  - o List of affected/touched assets (assets that will lose only one power path. Asset will stay online on redundant power during the PME).
5. Advise Proximity Services of any additional audits or remediation requirements in advance of the PME. This could include moving power to other path for single power devices or replacing any failed power supplies.
6. Perform Remediation activities pre-PME.
7. Raise Vendor heightened awareness.
8. Complete pre-checks prior to start of PME.
9. Complete post checks after completion of PME.

### **PME Pre-checks:**

The PSU's on the filer need to be verified prior to any PME activitiy. If any issues are found on the precheck then a case should be raised to NetApp to resolve the issue prior to the PME

There is a script to perform the pre-checks on the filers:

### **Prerequisites:**

The script makes a few assumptions. If these statements below aren't met the script will fail to make the SSH connections and no auditing will be performed.

1. Script is being run from a current unix/linux environment. It is a self-contained shell script and doesn't rely on any additional modules/SDKs/etc.
2. User running the script has shared SSH keys on every filer, or access to a user account that does
3. DNS A or CNAME records exist for every controller/cluster entered into the CSV file
4. Every node in a cDOT cluster also has an appropriate A or CNAME record along
5. Every node in a cDOT cluster has a node-mgmt LIF accepting SSH connections

### **Script Usage:**

Please transfer the .zip file to a linux server first and then unzip the file to avoid any Windows formatting or conversion issues.

In order to use the script a user will need to create a file of controller and/or cluster hostnames in CSV format, and then pass that file to the script as the first argument.

The second argument should be one of two states

1. 'pme' – specify 'pme' as the second argument while one of the power legs is down. The script will verify that exactly half of the PSUs are faulted for all nodes & shelves, and report anything outside of this condition.

2. empty/blank – leave it blank after the \*first\* leg has been brought down and restored. The script will report on \*any\* faulted PSUs.
3. If a PSU shows a fault after the first power leg has been brought down, then the PSU state and cabling should be investigated to ensure it won't be the only PSU left when the second power leg is brought down.
4. Alternatively, the second argument can be left blank and the script can be used at any time to verify PSU health on controller(s)

Below is the instructions into the script and a warning will appear if no file is specified.

```
./psu_health.sh <INPUT_FILE> <PME_ARG>(optional param)
```

<INPUT\_FILE> should be the name of CSV file containing controllers or clusters to check PSU status.

<PME\_ARG> - specify 'pme' if testing during a PME where a power leg is down, otherwise leave blank.

*example:*

*Version 1 script:*

```
./psu_health.sh /home/m6036149/input.csv      ##Expects no PSUs to be offline and will report *any* bad PSU found.
```

or

```
./psu_health.sh /home/m6036149/input.csv pme    ##Expects exactly half of total PSUs to be offline and will report any variances.
```

*Version 2 script:*

```
./psu_health_v2.sh /home/m6036149/pme_test.csv
```

**Expected output during a non-PME window:**

```
./psu_health.sh test.csv
```

```
+++++
```

Reading input file test.csv...

gathering information from host 10.209.41.170

cluster-mode node hive-01 found on 10.209.41.170

cluster-mode node hive-02 found on 10.209.41.170

..finished.

```
+++++
```

Gathering PSU status from nodes...

checking node PSU status on node hive-01

checking shelf PSU status on node hive-01

checking node PSU status on node hive-02

checking shelf PSU status on node hive-02

..finished.

```
+++++
```

Checking all node PSU output now...

..finished.

Checking all shelf PSU output now...



...finished.

+++++

**Expected output if the ‘pme’ argument is applied during a non-PME window (no PSUs down when half of them should be):**

```
./psu_health.sh test.csv pme
```

+++++

Reading input file test.csv...

gathering information from host 10.209.41.170

cluster-mode node hive-01 found on 10.209.41.170

cluster-mode node hive-02 found on 10.209.41.170

...finished.

+++++

Gathering PSU status from nodes...

checking node PSU status on node hive-01

checking shelf PSU status on node hive-01

checking node PSU status on node hive-02

checking shelf PSU status on node hive-02

...finished.

+++++

Checking all node PSU output now...

No node PSUs faulted for node hive-01 - possible power cabling problem found.

No node PSUs faulted for node hive-02 - possible power cabling problem found.

...finished.

Checking all shelf PSU output now...

No shelf PSUs faulted for shelf Shelf:\_40|SHJ00000000002E on node hive-01 - possible power cabling problem found.

No shelf PSUs faulted for shelf Shelf:\_41|SHJ00000000002B7 on node hive-01 - possible power cabling problem found.

No shelf PSUs faulted for shelf Shelf:\_10|7000007814 on node hive-01 - possible power cabling problem found.

No shelf PSUs faulted for shelf Shelf:\_11|7000007711 on node hive-01 - possible power cabling problem found.

No shelf PSUs faulted for shelf Shelf:\_40|SHJ00000000002E on node hive-02 - possible power cabling problem found.

No shelf PSUs faulted for shelf Shelf:\_41|SHJ00000000002B7 on node hive-02 - possible power cabling problem found.

No shelf PSUs faulted for shelf Shelf:\_10|7000007814 on node hive-02 - possible power cabling problem found.

No shelf PSUs faulted for shelf Shelf:\_11|7000007711 on node hive-02 - possible power cabling problem found.

...finished.

## **Supported Models & ONTAP Versions:**



Lastly, below are the filer models & ONTAP versions supported in the script (this is also included as a comment in the header of the script). As additional models & ONTAP releases are used in the environment there will need to be slight logic additions in one of the script functions.

| Filer_Model | ONTAP_Version | OS     |
|-------------|---------------|--------|
| FAS2240-2   | 8.1.2         | 7-Mode |
| FAS2240-2   | 8.1.3P1       | 7-Mode |
| FAS2240-2   | 8.2.3P5       | 7-Mode |
| FAS2240-2   | 8.2.4         | 7-Mode |
| FAS2240-4   | 8.1.3P1       | 7-Mode |
| FAS2240-4   | 8.2.3P5       | 7-Mode |
| FAS2554     | 8.2.3P5       | cDOT   |
| FAS3250     | 8.1.3         | 7-Mode |
| FAS3250     | 8.1.3P1       | 7-Mode |
| FAS3250     | 8.2.3P5       | 7-Mode |
| FAS3250     | 8.2.3P5       | cDOT   |
| FAS3250     | 8.3.2P4       | cDOT   |
| FAS6080     | 8.1.3P1       | 7-Mode |
| FAS6080     | 8.2.3P5       | 7-Mode |
| FAS6210     | 8.1.3P1       | 7-Mode |
| FAS6210     | 8.2.3P5       | 7-Mode |
| FAS6220     | 8.1.3P1       | 7-Mode |
| FAS6220     | 8.2.3P5       | 7-Mode |
| FAS8040     | 8.2.3P5       | cDOT   |

Script Location:

```
m6036149@c152mad:/filers/admin/scripts/support> ls -l psu*
-r-xr-xr-x 1 u0135425 g0135425 19902 Oct 29 15:24 psu_health.sh
-r-xr-xr-x 1 u0173152 g0173152 20995 Feb 7 12:38 psu_health_v2.sh
```

Create a CSV file under your home folder and list the filers in it:

```
m6036149@c152mad:~> pwd
/home/m6036149
m6036149@c152mad:~> vi pme_test.csv
```

Need to list all the filer under the file pme\_test.csv

```
eg-nascorpbkp-f03
eg-nascorpbkp-e06
hz-nascorpbkp-a01
ln-nascorpbkp-d01
```

Executing the script:

```
m6036149@c152mad:/filers/admin/scripts/support> ./psu_health_v2.sh /home/m6036149/pme_test.csv
```

Output:

```
m6036149@c152mad:/filers/admin/scripts/support> ./psu_health_v2.sh /home/m6036149/pme_test.csv
+++++
Reading input file /home/m6036149/pme_test.csv...
...finished.
+++++
Gathering PSU status from nodes...
...finished.
+++++
Checking all node PSU output now...
...finished.
Checking all shelf PSU output now...
...finished.
+++++
m6036149@c152mad:/filers/admin/scripts/support>
```

Once we execute the script we will get the above output. If any filer had issue it will list the filer name which had issue.

### Auto support:

Prior before the PME we need to trigger the autosupport on the filer:

```
m6036149@c152mad:/filers/admin/scripts/support> ssh eg-nascorpbkp-f03 options autosupport.doit PME
```

#### 4.6.4 What is a PAS and how to raise it?

**Physical Access Service(PAS)** provides Access Control in all DCS datacenters Globally, ensuring only authorized personnel are granted entry. A PAS needs to be submitted while scheduling vendor customer Engineer(CE)/Field engineer(FE) is required to be onsite to perform hardware replacements or other scheduled activities that require them to be onsite.

##### How to raise a PAS request to proximity services

Web Link: <http://pas.int.thomsonreuters.com/pas/user/RequestServlet>

Process:

1. Open the above link → Login via SAFE Account
2. Select the Data Centre from the drop down & select **Next**

**WHAT DOES IT DO?**

Please Select Datecentre

BANGALORE  
BANGALORE GCC  
BOSTON  
BROOKFIELD  
DOCKLANDS  
EAGAN-E  
EAGAN-F  
EAGAN-H  
FAREHAM (UK1)  
GENEVA  
GOSWELL ROAD (UK2)  
HARTLAND (US1)  
HAUPPAUGE  
HAZELWOOD (US2)  
HONG KONG (HK1)  
HYDERABAD  
LIMERICK  
NUTLEY

**HOW CAN I FILE A REQUEST?**

Request for Access can be made through the Service Portal. This submission and then on the portal.

For Emergency access Where the requirement permission of the Data Centre Manager.

**ACCESS REQUEST**

Datacentre: Please Select Datecentre

**INSTRUCTIONS:**

To create a request/ticket, please follow the steps below:

- Firstly, select a site or data centre from the drop-down list and click next.
- Enter the request details:
- Requester Information
- Access Information (Request Type / Room / Area)
- Visitor Information
- Access Date & Time
- Then, click submit.

3. Select Type of Access from the drop-down list (Temporary for short period of access to the Field Engineer)

## ACCESS

Type \*

Please Select Type of Access  
Please Select Type of Access  
Temporary  
Extended Temporary  
Permanent

You have 100 characters left.

Please choose the type of access according to the access criteria:  
• Temporary (1 to 5 days access)  
• Extended Temporary (6 days to 3 months access)  
• Permanent (subject to review)

4. Choose the Business Justification relevant to the work based on IM/CR  
Note:

- i. Justification is mandatory for temporary access
- ii. Incident Number or Change Number is mandatory
- iii. Provide the CR/IM number below Justification dialogue box

Justification \*

Other  
Please Select Justification  
Incident  
**Change**  
Other

Escort Required  
Enter name of individual or group providing escort.

You have 100 characters left.

Justification is mandatory for temporary access request  
• A valid SM7 IMXXXXXXXXXX for incident related access request.  
• A valid SM7 CXXXXXXXXXX for change related access request.  
• For any "other" justification type, please detail in the following field.

5. Check & enter the **Escort Required** field with the Proximity services engineer that will escort the Field Engineer into the DC or Just specify the Proximity services group name.  
Ex: DC-PS-EAGAN

Escort Required  
Enter name of individual or group providing escort.  
**DC-PS-EAGAN**

You have 89 characters left.

6. Fill the required fields under Person(s) Requiring Access. This will be the details of the vendor CE/FE that needs to be onsite.  
Ex: Access given to Robert Wedell from Dell-EMC with 83948702 as external reference (Vendor Change record)

## PERSON REQUIRING ACCESS

Click [] to add yourself or [] to add or [] to remove record

 Request access for yourself? Please provide your name and card ID in this section.

Unknown Visitor(s)

|            |                  |              |             |                      |
|------------|------------------|--------------|-------------|----------------------|
| Company: * | Other Company: * | First Name * | Last Name * | External Reference * |
| Other      | Dell-EMC         | Robert       | Wedell      | 83948702             |

7. Select Date & Time for the scheduled CE/FE visit.  
Note: The Date &Time will reflect the selected DC timezone.

## DATE(S) & TIME(S)

| Date: *  | Time: * |
|--|---------|
| Start: 15-Jan-17   | 07 : 00 |
| End: 15-Jan-17     | 10 : 00 |

8. Complete the Comments field with reason for FE visit

## COMMENT

Robert **Wedell** from Dell-EMC will reach DC-PS-Eagan to replace the failed disk in EG-SANVMAXCIS-F01 VMAX array.

You have 88 characters left.

9. Select the Computer Room where the asset is located, Location information is available at Service Manager 9 under Location tab.

## EAGAN-E

### COMPUTER ROOM

- D LAN Rooms
- Dock Access
- Mainframe / Network
- OCC
- S012
- S101
- Telcom

### OTHER(S)

- DC Tour

### CSE AREAS

- CRAC/CRAH Galleries
- Court Yard
- Elec / Mech Rooms
- Maintenance Shop
- West Ramp Door

### How to find the location of the Asset or Configuration Item (CI):

- a) Select the Computer Room where the asset is located, Location information is available at ServiceNow under Location tab.
- b) Open [https://thomsonreuters.service-now.com/nav\\_to.do](https://thomsonreuters.service-now.com/nav_to.do)  
(or) <http://gotmon.int.thomsonreuters.com/> to find the location of Asset
- c) IN ServiceNow select Configuration Management → Enter CI to Search and hit <Enter>

The screenshot shows the ServiceNow CMDB interface. On the left, there is a sidebar with a navigation menu. The 'Configuration Items' section is expanded, showing 'All', 'CMDB Groups', 'CMDB Query Builder', 'Hardware' (which is expanded to show 'All'), and 'CMDB Dashboard'. Below these are 'CMDB View', 'Service View', and 'Group View'. A red box highlights the 'Configuration' button in the top bar, and a red arrow points from it to the 'Configuration Items' section in the sidebar. On the right, the main pane displays a list of configuration items. At the top of this list, there is a search bar containing the text 'In-nasecom-d01'. A red box highlights this search bar, and a red arrow points from it to the search bar. The list itself contains 15 entries, each with a checkbox, an info icon, '(empty)', and a date column. The columns are labeled 'Name', 'Asset', 'Customer', 'Operational status', 'Asset tag', and 'Last modified'.

| Name    | Asset | Customer | Operational status | Asset tag | Last modified |
|---------|-------|----------|--------------------|-----------|---------------|
| (empty) |       |          | Decommissioned     | 202243    | (empty)       |
| (empty) |       |          | Decommissioned     | 200333    | (empty)       |
| (empty) |       |          | Decommissioned     | 202669    | (empty)       |
| (empty) |       |          | Decommissioned     | 204591    | (empty)       |
| (empty) |       |          | Decommissioned     | 201703    | (empty)       |
| (empty) |       |          | Decommissioned     | 204463    | (empty)       |
| (empty) |       |          | Decommissioned     | 200050    | (empty)       |
| (empty) |       |          | Decommissioned     | 202641    | (empty)       |
| (empty) |       |          | Decommissioned     | 200205    | (empty)       |
| (empty) |       |          | Decommissioned     | 202892    | (empty)       |
| (empty) |       |          | Decommissioned     | 204236    | (empty)       |
| (empty) |       |          | Decommissioned     | 200362    | (empty)       |

- d) Select the asset and the location details will be listed

In-nasecom-d01

|               |  |
|---------------|--|
| Name          | In-nasecom-d01   |
| Asset tag     | RFID25396  |
| Asset         | RFID25396 - NetApp FAS6210   |
| * Device type | NAS Controller   |
| Serial number | 800000113178   |
| Model ID      | NetApp FAS6210   |
| Manufacturer  | NetApp   |
| Provision ID  |  |
| Reference ID  | SNCI05851429   |
| Installed     |  |
| DCIM Managed  | No   |
| Location      | GB - DTC/London-DTC  |
| Comments      | Rack : dtc_dh04 ag073 Rack Unit : 41<br>Slot : N/A Grid Location : AG073<br>Power Path : N/A |

10. Accept the terms & conditions and submit the request.
11. Once the PAS request is submitted, requestor will receive a mail notification with PAS ID & email on status of PAS.
12. Submit the PAS details to DC-PS team and work with vendor to schedule the CE/FE visit.

#### 4.6.5 Disk Failures

Disk failures trigger a autosupport to Netapp through which a case is automatically created. Netapp Support will work with FLS-SYSTEMS to schedule the disk replacement. FLS-SYSTEMS make use of a TR internal script called "OPER MENU" to validate the disk failure and subsequently raise a CR/PAS to schedule the replacement.

All replacements should be done after business hours. Occasionally FLS-SYSTEMS may not be able to validate the disk failure and reached out to storage support team to confirm the disk replacement prior to scheduling it with Netapp.

#### 4.6.6 Power supply Failures

PSU failures trigger a autosupport to Netapp through which a case is automatically created. Netapp Support will work with FLS-SYSTEMS to schedule the PSU replacement. FLS-SYSTEMS will schedule the failed PSU replacement with Netapp and raise a CR/PAS.

All replacements should be done after business hours. FLS-SYSTEMS handle single PSU replacements only. If multiple PSU's have failed, this will be handled by the Storage support team.

#### 4.6.7 Bad FH

A Bad FH on any file system may cause an outage to the servers that are mounted to that volume while performing the TO/GB and needs to be remediated.

A Bad FH is reported during:

1. Pre-Checks carried out for TO/GB operations (Ontap upgrades, Switch migrations, HW maintenance etc.)
2. Consolidated Monthly report for Bad FH through schedule script on our DFM infrastructure. Example output can be seen [here](#)

[How to manually check for BAD FH during pre-checks?](#)

- a. Connect to the one of the jumpboxes (Ex: c152mad.int.thomsonreuters.com)
- b. The script is located here: /filers/admin/scripts/support/nfs\_export\_debug.pl
- c. Execute the script as shown below redirecting the output to a text file  

```
/filers/admin/scripts/support/nfs_export_debug.pl <Filname> >
/home/svcstg_scriptuser/<Filname>_prework_output.txt
```

*Ex: /filers/admin/scripts/support/nfs\_export\_debug.pl eg-naslowcc-h03 > /home/svcstg\_scriptuser/eg-naslowcc-h03\_prework\_output.txt*

```
-bash-3.2$ /filers/admin/scripts/support/nfs_export_debug.pl eg-naslowcc-h03 > /home/svcstg_scriptuser/eg-naslowcc-h03_prework_output.txt
Gathering NFS exports in memory.
Finding vfile export file paths.
Running rdfile commands for vfile export files.
Running export tbl_dump commands.
Running showfh commands.
```
- d. grep for Bad FH as shown below  

```
-bash-3.2$ cat /home/svcstg_scriptuser/eg-naslowcc-h03_prework_output.txt |grep -i "bad"
/vol/trs_lifesciences_nfsdataqa_snap/nonprod_db () [online]: fh=0 0 0 60 4a8ee32e 332bad9: fh_hash=28: name_hash=98:
/vol/trs_lifesciences_nfsdataqa_snap/nonprod_db () [online]: fh=0 0 0 60 4a8ee32e 332bad9: fh_hash=28: name_hash=98:
flags=0x00 snapid=0 fileid=0x000060 gen=0x4a8ee32e fsid=0x332bad9
```
- e. Identify the hosts exported to the volume with Bad FH by checking the export permissions for the volume in /etc/exports file
- f. Schedule a remediation CR to fix the Bad FH

#### How to check consolidated Monthly report for Bad FH?

- a. A consolidated BAD FH report emails is sent to DCO-STO-SUPP-NAS from “**svcstg\_scriptuser - Storage Group [svcstg\_scriptuser@nerstrand.int.westgroup.net]**” every month for all the physical filers.
- b. Ignore the following output from the report as are volumes undergoing migrations or decom
  - i. volumes with expiry date  
*Ex:at\_cobalt265p\_n01ora1\_nosnap\_EXP20161027\_CR07850942*
  - ii. Volumes which are offline  
*Ex: /vol/test\_ico\_vol\_snap\_001b () [offline]*
  - iii. Volumes that do not have any mounts
  - iv. Volumes which are named as TEST (Confirm if this test volume belongs to STORAGE)
- c. The rest of the volumes are Bad FH candidates
- d. Identify the hosts exported to the volume with Bad FH by checking the export permissions for the volume in /etc/exports file
- e. Schedule a remediation CR to fix the Bad FH

#### Process to fix BAD FH

- a. You should have identified the Volume and Exported Hosts as outlined earlier.
- b. Find the support group, Change group and Config admin group via. (SM9 DL)
  - o [https://thomsonreuters.service-now.com/nav\\_to.do](https://thomsonreuters.service-now.com/nav_to.do) (or)
  - o <http://gotmon.int.thomsonreuters.com/index.php>

*Example: Host- c371vqqjend05.int.thomsonreuters.com*

The screenshot shows the ServiceNow CMDB Configuration Item detail view for item 'c371vuhrtlws'. A red arrow points to a group of configuration items under the 'Support group L3' field, which are highlighted with a red border. The highlighted items are:

- Config admin group: UNIX-SUPPORT-FR
- Support group L1: APP-SRE-KYC
- Support group L2: APP-OPS-RISK-GLOB
- Support group L3: APP-OPS-RISK-GLOB
- Change approval groups: APP-OPS-ORGID, CHANGE-MGMT-EIKON-REALTIME

The rest of the configuration item details are as follows:

- Name: c371vuhrtlws
- Is Virtual: checked
- Asset: SMAT079493 - Virtual Virtual Server
- Asset tag: SMAT079493
- Serial number: VMware-42 2c 96 fe a4 05 53 77-0c 9b
- Model ID: Virtual Virtual Server
- Manufacturer: Virtual
- Provision ID:
- Reference ID: CI929315
- Installed: 2013-11-29 09:00:53
- DCIM Managed: No
- Operational status: Commissioned
- Environment: Production
- Customer facing: Customer
- DR: No
- Service tier: Managed
- Location: GB - DTC/London-DTC/DH04
- Comments: Rack: NA Rack Unit: NA Grid: NA Slot: NA Power Path: NA Comments: Logical Image
- Divestiture Status: King
- TSA Stage:
- Config managed: Yes

*In the above example APP-SRE-AYC, APP-OPS-RISJ-GLOB are the Application team/BU and UNIX-SUPPORT-MANAGED is the config admin group*

- Use the below web link to find the Outlook DL for the respective ServiceNow group detail
- [https://thomsonreuters.servicenow.com/sys\\_report\\_template.do?jvar\\_report\\_id=cb3e4900130c0784a6b576d66144b044](https://thomsonreuters.servicenow.com/sys_report_template.do?jvar_report_id=cb3e4900130c0784a6b576d66144b044)  
(or <http://gotmon.int.thomsonreuters.com/index.php> (Click on support group to get the Outlook DL))

*Example: APP-SRE-KYC*

*Click on the ServiceNow link above, add a filter condition and add the ServiceNow Group. Click <Run>*

The screenshot shows the ServiceNow Group Detail page for ADM007B. At the top, there are dropdowns for Data (Table), Type (List), and Group by (None). To the right, there are two columns: 'Available' and 'Selected'. The 'Available' column lists various fields like Director-Ref, Manager, Team lead-Ref, etc. The 'Selected' column contains Name, Description, Active, Created, Updated, Director-Ref, Director escalation, Manager, Manager escalation, and Team lead-Ref. A red arrow points from the 'Run' button at the top right to the 'Selected' column. Another red arrow points from the 'Available' column to the 'Selected' column.

e. From the above click the group and you will find the group Distribution list as below:

The screenshot shows the distribution details for the APP-SRE-KYC group. It includes fields for Team lead escalation, Manager escalation, Director escalation, Department, Stakeholder escalation, Managed incident control group, Problem management group, Change management group, ECAB group, Schedule, Pillar plus1, Pillar minus1, Type, and Description. On the right side, there are sections for Manager, Group phone, Group email (highlighted with a red box), SMS Address, Tier, Ticket destination, Hourly rate, and Active status. A red arrow points from the 'Group email' field to the 'Group email' field in the distribution details.

f. Send an email to Platforms, BU/App Team and DB Team (if applicable for DB volumes) notifying the need to mitigate the Bad FH issue. The email should include:

- Volumes and Hosts in scope
- High level action plan as below:

**Action Plan:**

- Application team to shutdown the applications.
- DBA team will shutdown the Database
- UNIX team will umount the impacted volume
- Storage team will perform an export refresh
  - Verify if the un-mount task is done from the platform team
  - Run the below command to refresh the exports from storage end

```
"vfiler run <vfilername> exportfs <volume/Qtree path>
```

```
-bash-3.2$ ssh fr-nasecom-u03 vfiler run prod-ecom-u0138 exportfs /vol/cb0101_tcmdataproduk102_snap/images002
```

5. UNIX team will perform remount of the remediated volume
6. Database/application teams will start the DB/Apps.
7. Storage will perform a post check and confirm the bad fh status
  - a. Re-run the Bad FH script manually and verify if the BAD FH is cleared (Refer to Manual Script run section)
  - c. Request for downtime/maintenance window
- g. Schedule a Q1 Change Request during the approved downtime window. Add clear action plan and CT's for Platform for Un-Mount & Mount task, DB (If applicable) for DB shutdown, App Team (If Applicable) for Application Shutdown and Storage-support for exports refresh/post checks
- h. Send a Kick off email with the Action Plan prior to start of Change
- i. Implement the Action plan as outlined in the CR.
- j. Perform post checks by executing the script again and confirm Bad FH no longer exists

#### 4.6.8 Filer interface Down

An interface/port down alert will be reported in one of the following ways:

- Automated IM triggered through Filer monitoring
- Broken Interface down email report from svcstg\_scriptuser@nerstrand.int.westgroup.net
- An alert received by FLS-networks team

##### How to check if a network port is down:

1. Check messages from the filer end, if there are any and grep with interface/ port. Etc...

Commands:

7-Mode: `ssh <physical filer> rdfile /etc/messages | grep -i interface`

```
-bash-3.2$ ssh pl-nasecom-p05 rdfile /etc/messages | grep -i interface
```

C-Dot: connect to the physical filer and run “event log show \*interface”

```
pl-cis-claa-p01::> event log show *interface
```

Example messages:

*Wed Nov 9 07:35:39 GMT [In-nasecom-d01:snmp.link.down: info]: Interface 5 is down.*

*Wed Nov 9 07:35:39 GMT [In-nasecom-d01:netif.linkDown: info]: Ethernet e0e: Link down, check cable.*

2. Run the ifgrp status command

7-mode: `ssh <physical filer> vif status (or) ssh <physical filer> ifgrp status`

*Ex: ssh eg-nassecom-h03 vif status (or) ssh eg-nassecom-h03 ifgrp status*

c-Dot: connect to filer and run “system node run -node <node> ifgrp status“

*Ex: eg-cps-clsp-h01::> system node run -node eg-cps-clsp-h01-h01 ifgrp status*



```

c152mad:~ # ssh pl-nasecom-p05 vif status
root@pl-nasecom-p05's password:
ifgrp: command "vif" is deprecated in favor of command "ifgrp"
default: transmit 'IP Load balancing', Ifgrp Type 'multi_mode', fail 'log'
ecomvif0: 2 links, transmit 'IP Load balancing', Ifgrp Type 'lacp' fail 'default'
    Ifgrp Status   Up      Addr_set
    up:
    e0e: state up, since 18Nov2016 21:21:14 (53+10:31:02)
        mediatype: auto-10g_sr-fd-up
        flags: enabled
        active aggr, aggr port: e0c
        input packets 45219746223, input bytes 122879606623730
        input lACP packets 1322153, output lACP packets 1322388
        output packets 18745473706, output bytes 141027408782155
        up indications 13, broken indications 8
        drops (if) 0, drops (link) 9
        indication: up at 18Nov2016 21:21:14
            consecutive 0, transitions 21
    e0c: state up, since 21Oct2016 21:55:08 (81+10:57:08)
        mediatype: auto-10g_sr-fd-up
        flags: enabled
        active aggr, aggr port: e0c
        input packets 53167115687, input bytes 122276404802572
        input lACP packets 1322151, output lACP packets 1322384
        output packets 52047906739, output bytes 257757123766203
        up indications 10, broken indications 6
        drops (if) 0, drops (link) 0
        indication: up at 21Oct2016 21:55:08
            consecutive 0, transitions 16

```

3. Check the Ifgrp Type.

- a. If the Ifgrp Type is listed as 'multi\_mode' or 'lacp' then both ports should be up. If either one of the interface is down this is considered loss of resiliency and decrease in throughput. Engage the PS team and network team to troubleshoot this further.
- b. If the Ifgrp Type is listed as 'single\_mode' only one port will be up and other will be down. If the active port fails, the standby interface will be up and take over traffic. This will result in loss of resiliency. Engage the PS team and network team to troubleshoot this further.
- c. The timestamp next to the interface status shows when the interface entered the given state.

Below screenshot shows ecomvif0 which is a multi\_mode/lacp vif and dprodvif0 which is a single mode vif.



```

default: transmit 'IP Load balancing', Ifgrp Type 'multi_mode', fail 'log'
ecomvif0: 2 links, transmit 'IP Load balancing', Ifgrp Type 'lacp' fail 'default'
    Ifgrp Status     Up      Addr_set
    up:
    e0c: state up, since 23Oct2016 00:29:01 (80+14:24:56)
        mediatype: auto-10g_sr-fd-up
        flags: enabled
        active agrgr, agrgr port: e0e
        input packets 150409854024, input bytes 254157154864000
        input lACP packets 232110, output lACP packets 232124
        output packets 84668614337, output bytes 711110550684783
        up indications 2, broken indications 0
        drops (if) 0, drops (link) 0
        indication: up at 23Oct2016 00:29:01
                    consecutive 0, transitions 2
    e0e: state up, since 23Oct2016 00:28:58 (80+14:24:59)
        mediatype: auto-10g_sr-fd-up
        flags: enabled
        active agrgr, agrgr port: e0e
        input packets 205272545924, input bytes 217348497221057
        input lACP packets 232112, output lACP packets 232123
        output packets 181522819999, output bytes 1899062114730099
        up indications 2, broken indications 0
        drops (if) 0, drops (link) 0
        indication: up at 23Oct2016 00:28:58
                    consecutive 0, transitions 2
dprodvif0: 1 link, transmit 'none', Ifgrp Type 'single_mode' fail 'default'
    Ifgrp Status     Up      Addr_set
    up:
    e4a: state up, since 23Oct2016 00:28:57 (80+14:25:00)
        mediatype: auto-10g_sr-fd-up
        flags: enabled favored
        input packets 6343553419, input bytes 16137177359381
        output packets 4602669465, output bytes 10623895830496
        output probe packets 0, input probe packets 0
        strike count: 0 of 10
        up indications 2, broken indications 1
        drops (if) 0, drops (link) 3
        indication: up at 23Oct2016 00:28:57
                    consecutive 6963528, transitions 3
    down:
    e0d: state down, since 23Oct2016 00:29:28 (80+14:24:29)
        mediatype: auto-10g_sr-fd-up
        flags: enabled
        input packets 1348626, input bytes 120346854
        output packets 124600, output bytes 23186908
        output probe packets 0, input probe packets 0
        strike count: 0 of 10
        up indications 2, broken indications 1
        drops (if) 0, drops (link) 0
        indication: up at 23Oct2016 00:28:56
                    consecutive 6963529, transitions 3

```

4. If you received the alert but find the interfaces up check for port flapping messages in the filer logs and also check for any CRC errors as outlined below:

- Run the ifstat command for the port and see if there are any CRC errors  
7-mode: ssh <physical filer> ifstat e0P ("ifstat -a" for all interfaces)  
*Ex: ssh eg-nassecom-h03 ifstat e0P ("ifstat -a" for all interfaces)*



```
c152mad:~ # ssh eg-nassecom-h03 ifstat e0P
root@eg-nassecom-h03's password:

-- interface e0P (36 days, 19 hours, 14 minutes, 2 seconds) --

RECEIVE
Frames/second: 2 | Bytes/second: 368 | Errors/minute: 0
Discards/minute: 0 | Total frames: 5330k | Total bytes: 557m
Total errors: 0 | Total discards: 0 | Multi/broadcast: 671k
No buffers: 0 | Non-primary u/c: 0 | Tag drop: 0
Vlan tag drop: 0 | Vlan untag drop: 0 | Vlan forwards: 0
Vlan broadcasts: 0 | Vlan unicasts: 0 | CRC errors: 0
Runt frames: 0 | Fragment: 0 | Long frames: 0
Jabber: 0 | Alignment errors: 0 | Bus overruns: 0
Queue overflows: 0 | Xon: 0 | Xoff: 0
Jumbo: 0 | Reset: 0 | Reset1: 0
Reset2: 0

TRANSMIT
Frames/second: 2 | Bytes/second: 161 | Errors/minute: 0
Discards/minute: 0 | Total frames: 5302k | Total bytes: 420m
Total errors: 0 | Total discards: 0 | Multi/broadcast: 0
Queue overflows: 0 | No buffers: 0 | Max collisions: 0
Single collision: 0 | Multi collisions: 0 | Late collisions: 0
Timeout: 0 | Xon: 0 | Xoff: 0
Jumbo: 0

LINK_INFO
Current state: up | Up to downs: 1 | Auto: off
Speed: 100m | Duplex: full | Flowcontrol: full
```

c-DOT: Connect to the cluster and run “system node run -node eg-cps-clsp-h01-h01 ifstat e0M” (“ifstat -a” for all interfaces)

*Ex: system node run -node eg-cps-clsp-h01-h01 ifstat e0M (“ifstat -a” for all interfaces)*

```
eg-cps-clsp-h01::> system node run -node eg-cps-clsp-h01-h01 ifstat e0M

-- interface e0M (1 day, 15 hours, 52 minutes, 47 seconds) --

RECEIVE
Frames/second: 1 | Bytes/second: 85 | Errors/minute: 0
Discards/minute: 0 | Total frames: 141k | Total bytes: 9906k
Total errors: 0 | Total discards: 0 | Multi/broadcast: 141k
No buffers: 0 | Non-primary u/c: 0 | L2 terminate: 138k
Tag drop: 0 | Vlan tag drop: 0 | Vlan untag drop: 0
Vlan forwards: 0 | Vlan broadcasts: 0 | Vlan unicasts: 0
CRC errors: 0 | Runt frames: 0 | Fragment: 0
Long frames: 0 | Jabber: 0 | Alignment errors: 0
Bus overruns: 0 | Queue overflows: 0 | Xon: 0
Xoff: 0 | Jumbo: 0 | Reset: 0
Reset1: 0 | Reset2: 0

TRANSMIT
Frames/second: 0 | Bytes/second: 0 | Errors/minute: 0
Discards/minute: 0 | Total frames: 2393 | Total bytes: 344k
Total errors: 0 | Total discards: 0 | Multi/broadcast: 2393
Queue overflows: 0 | No buffers: 0 | Max collisions: 0
Single collision: 0 | Multi collisions: 0 | Late collisions: 0
Timeout: 0 | Xon: 0 | Xoff: 0
Jumbo: 0

LINK_INFO
Current state: up | Up to downs: 1 | Auto: on
Speed: 1000m | Duplex: full | Flowcontrol: full
```

- b. If there are any errors reported under CRC clear the counters by using ifstat -z and rerun the refresh command again to see if the CRC errors are increasing,

7-Mode

```
-bash-3.2$ ssh pl-nasecom-p05 ifstat -z e0e
```

```
-bash-3.2$ ssh pl-nasecom-p05 ifstat e0e
```

C-Dot

```
pl-cis-claa-p01::> system node run -node pl-cis-claa-p01-n01 -command ifstat -z e4b
pl-cis-claa-p01::> system node run -node pl-cis-claa-p01-n01 -command ifstat e4b
```

- c. If the CRC errors are increasing, we should engage the PS team along with the network to do a physical verification to see if there are any faulty cable or SFP



## **Follow the below steps for interface down and high CRC errors:**

1. Raise a P3 Major incident to FLS-Networks for Loss of Resiliency to investigate the port that is down or showing high CRC errors
2. Raise a p2 Netapp case in parallel to investigate if the issue is on the filer or external to the filer.
3. FLS-SYSTEM should have opened a TRT Call. Request PS team to do a physical check on the network switch port
4. If confirmed by NetApp and Network team to replace Cable/SFP, Network support will raise a PCA to replace cable/SFP on the switch port. A CT should be assigned to Storage to do the post checks.
5. Validate and confirm the changes are non-disruptive. All changes should be scheduled after business hours. Storage team will perform the post checks (Re-run the commands in Step 1 to 4 and check the status)
6. If the issue persists arrange NetApp engineer to be onsite to replace the SFP on the switch

### **4.6.9 Adding protocols license to NetApp controller**

The following is a list of scenarios where new license keys are commonly required:

- **Controller or Motherboard Replacements** - With Data ONTAP 8.2 and 8.3, these always require new license keys due to the change in the Controller (System) Serial Number (8.2 and 8.3 license keys are locked to the Controller Serial Number). If you require new license keys for a HW Replacement scenario, contact CSS.

This table identifies Data ONTAP license key formats and the version and mode each belongs to:

| Version and Mode                    | License Key Format  |
|-------------------------------------|---|
| Data ONTAP 8.0/8.1 7-Mode           | 7-character, all uppercase alpha (example: ABCDEFG)                       |
| Clustered Data ONTAP 8.0/8.1        | 14-character, all uppercase alpha (example: ABCDEFGHJKLMNP)               |
| Data ONTAP 8.2 (both modes) and 8.3 | 28-character, all uppercase alpha (example: ABCDEFGHJKLMNPQRSTUVWXYZABCD) |

#### **Note:**

- *In Data ONTAP 8.2 and higher versions, License Keys are locked ("node-locked") to the Controller Serial Number they are issued. Replacement Controllers require new License Keys that must be installed within 90 days.*
- *The Data ONTAP 8.2 and 8.3 Evaluation ('Eval') License Keys have explicit expiration dates. An Eval key is typically issued for a 90-day period. To extend a software evaluation after an Eval key expires, obtain and install a new Eval key. Work with a NetApp representative to obtain Eval license keys.*

#### **Steps to obtain license keys:**

1. After a Controller or Motherboard replacement new license keys must be applied to enable value-add features (such as protocols, Snap Mirror, etc.).
2. Post replacement of controller or motherboard, license keys will be updated on [NetApp support site](#) (Products→Software Licenses)within 7 days period or should receive an e-mail from "NetApp - Service Entitlement Specialist team" for the new serial number.
3. If not received in 7-days, Contact NetApp customer service (CSS) to receive the protocol licenses.

#### **Steps to raise a change:**

1. Post motherboard replacement, new licenses keys can be applied to new serial number, with a Service-Now change.
2. Raise a Normal change in [Service-Now](#) with 2-day lead time
3. Fill all required fields & add information such as (Old Serial, new Serial, Filer Name, etc.)

## Steps to apply Licensing for each protocol:

### 1. Command to check license

➤ 7Mode:

```
>ssh <Filer_Name> license show (7Mode)
```

```
svcstg_scriptuser@c152mad:~> ssh pl-nascorp-p03 license show
```

```
Warning: License grace period active. Showing entries associated with the original system serial number.  
There are 85 days and 20 hours left in the grace period.
```

| Original Serial Number: | 701435002490   |                     |            |
|-------------------------|----------------|---------------------|------------|
| Owner:                  | pl-nascorp-p03 |                     |            |
| Package                 | Type           | Description         | Expiration |
| NFS                     | license        | NFS License         | -          |
| CIFS                    | license        | CIFS License        | -          |
| iSCSI                   | license        | iSCSI License       | -          |
| SnapRestore             | license        | SnapRestore License | -          |
| SnapMirror              | license        | SnapMirror License  | -          |
| SnapVault               | license        | SnapVault License   | -          |

➤ CDOT:

```
Cluster::> license show -serial-number <Node Serial Number>
```

```
eg-cps-claa-f01::> license show -serial-number 1-81-0000000000000000700002249096  
(system license show)
```

```
Serial Number: 1-81-0000000000000000700002249096
```

```
Owner: eg-cps-claa-f01-n01
```

| Package | Type    | Description  | Expiration |
|---------|---------|--------------|------------|
| NFS     | license | NFS License  | -          |
| CIFS    | license | CIFS License | -          |

Here before applying license keys “license show” command shows a warning!!

*“Warning: License grace period active. Showing entries associated with the original system serial number.*

*There are 85 days and 20 hours left in the grace period.”*

This indicates with the grace period & old serial number as “Original Serial Number”.

### 2. To add license keys

➤ 7Mode:

```
>ssh <Filer_Name> license add <License_Code>
```

```
svcstg_scriptuser@c152mad:~> ssh pl-nascorp-p03 license add ITDWTQERYVHXCFSATBAAAAAAA  
license add: successfully added license key "ITDWTQERYVHXCFSATBAAAAAAA".
```

➤ CDOT:

```
Cluster::> license add --license-code <License_Code_V2>
```

```
eg-cps-claa-f01::> license add --license-code <License Code V2>
```

### 3. Once all the license added re verify with the “license show”

➤ 7Mode:

```
svcstg_scriptuser@c152mad:~> ssh pl-nascorp-p03 license show
```

```
Warning: License update grace period validation active. Showing licenses associated with both the original and all updated system serial numbers.  
There are 24 hours left in the grace validation period.
```

```
Current Serial Number: 791412000123  
Owner: pl-nascorp-p03
```

Note: Above ‘warning’ will be automatically cleared in 24Hrs.

➤ CDOT:



```

Cluster ::> license show -serial-number <Node Serial Number>
eg-cps-claa-f01::> license show -serial-number 1-81-0000000000000700002249096
  (system license show)

Serial Number: 1-81-0000000000000700002249096
Owner: eg-cps-claa-f01-n01
Package      Type    Description          Expiration
-----      -----
NFS          license  NFS License          -
CIFS         license  CIFS License          -

```

4. Trigger autosupport from the controller to get confirmation on license add from NetApp.

➤ **7Mode:**

```
>ssh <Filer_Name> options autosupport.doit <case_number>
```

➤ **CDOT:**

```
Cluster ::> autosupport invoke -node <Node_Name>
```

**Additional References:**

5. For additional information regarding Data ONTAP Licensing, see article [3013749](#): Data ONTAP 8.2 and 8.3 Licensing Overview and References.
6. For details about how license keys are sold and handled in Data ONTAP 8.2, see article [3013742](#): What are the licensing and packaging requirements for Data ONTAP 8.2 and 8.3.
7. [Knowledge Base](#) on protocol Licensing.

#### 4.6.10 Snapvault Lags

<Placeholder TBA in next version>

#### 4.6.11 IAAS Growth – NFS and CIFS

Action needed to be taken from storage support when RITM comes to queue from IAAS.

**What is IAAS?**

IAAS (formerly known as Unify), is our self-service offering for ordering infrastructure- which is then built through automated workflows. There is no Solution Design phase or Delivery queue, so as long as your requirements fit with our IAAS offerings, you are able to order your requests and have they handed over to you in about 6 days or less.

**IAAS offering in Storage**

Currently IAAS developed automation FORM for space growth. As of now it covers growth request for the below volume only.

- FLAT Volume
- LION Volume (DB- Oracle)
- ESX Volume
- CIFS Volume

ISCSCI space growth is still in development stage.

## Who is using the Form for space growth?

The Form has been developed for BU's to grow the space without help of Delivery team. BU's doesn't have awareness of the standards what we follow for storage allocation, In order to avoid that currently the form was used by DCIS-Solution-Consulting team for the growth request from BU's

They will be verifying the aggregate over commitment & utilization is below threshold prior to grow the volume.

Point of contact from DCIS-Solution-Consulting team

- Vinoth Ezhumalai
- Blomer, Rachael D

## Expected issues/failure

Below are the failure/Errors will be seeing based on scenarios.

SF1, SF2 & SF3 doesn't require any storage intervention. SF4 & SF5 will be our part

## Success and Failure Scenarios

|     | Scenario                           | Description  | Action  |
|-----|------------------------------------|--|---|
| SF1 | Full success                       | The additional requested space will be allocated to the requested volume.                    | The ServiceNow request will be updated throughout the process with the specifics as they are completed and the Request is updated as "Closed Complete".   |
| SF2 | Invalid export path or mount point | The export/share path or mount point provided cannot be parsed                               | <ul style="list-style-type: none"><li>• The catalog item will report the following error message<ul style="list-style-type: none"><li>◦ "Please enter a valid mount point or share path"</li></ul></li></ul>  |
| SF3 | NAS resources cannot be resolved   | The catalog item back-end script is unable to determine one or more of the NAS resource IDs. | <ul style="list-style-type: none"><li>• The catalog item will report one of the following error messages<ul style="list-style-type: none"><li>◦ "Please enter a valid mount point or share path"</li><li>◦ "Unable to parse volume info"</li><li>◦ "NasVolume.id {nasVolumeld} has no CIFS Shares associated with it."</li><li>◦ "NasVolume.id {nasVolumeld} has no qtrees associated with it."</li></ul></li></ul> |

|     |                                 |   |
|-----|---------------------------------|---|
| SF4 | Aggregate check failure         | <p>Two aggregate checks (backup [if required] and primary) are performed prior to invoking the resize service.</p> <ul style="list-style-type: none"> <li>Message returned to Comments and Work Notes section of RITM. Budget is refunded.</li> <li>Task generated to STORAGE-SUPPORT to investigate</li> <li><b>Task must be saved as <i>Closed Complete</i> to advance workflow</b></li> <li>Drop-down list options: <ul style="list-style-type: none"> <li><u>Grow in-place</u>: Workflow continues to next step along happy path</li> <li><u>Grow request rejected</u>: Workflow updates and closes RITM Work Notes with message "The Shared Storage Grow process has completed unsuccessfully. The grow request has been rejected."</li> <li><u>Volume must be migrated</u>: Workflow updates and closes RITM Work Notes with message 'The Shared Storage Grow process has completed unsuccessfully. The volume must be migrated to an alternative filer and virtual filer.'</li> </ul> </li> </ul>  |
| SF5 | ICO workflow invocation failure | <p>There are a total of three SOAP calls within the workflow: Backup Aggregate Checks, Primary Aggregate Checks, Shared Storage Grow.</p> <ul style="list-style-type: none"> <li>Message returned to Comments and Work Notes section of RITM. Budget is refunded.</li> <li>Retry SOAP call and allow workflow to progress. If SOAP call fails, task generated to DELIVERY-STORAGE to investigate and/or complete request manually.</li> <li><b>Task must be saved as <i>Closed Complete</i> to advance workflow</b></li> <li>Drop-down list options: <ul style="list-style-type: none"> <li><u>Capacity problem</u>: Workflow updates RITM Work Notes and assigns task to Storage Support to investigate</li> <li><u>Growth completed manually</u>: Workflow updates and closes RITM Work Notes with message 'The Shared Storage Grow process has completed successfully with manual intervention. Please see work notes for full details.'</li> <li><u>Unable to grow manually</u>: Workflow updates and closes RITM Work Notes with message "The Shared Storage Grow process has completed unsuccessfully. The grow request cannot be grown manually."</li> </ul> </li> </ul> |

### SF5: (ICO Workflow Invocation Failure)

This scenario of failure will be moved to Delivery-Storage as per the Form. This failure occurs when Form not able to reach the controller. Delivery-Team will be manually growing the space and close the RITM.

## SF4 (Aggregate check Failure)

This scenario of failure will come to storage support. If aggregate is over utilized or over committed automatic RITM has been raised to storage-support for migration. Once the migration completed we have to close the RITM and then the allocation will be done automatically. As of now DCIS-Solution-Consulting team will be checking the threshold prior the growth.

### Failure RITM received

Currently we have received couple of scenario's SF4

#### Scenario 1:

**Error: Problem while executing workflow(NAME=7Mode\_NAS\_Volume\_Resize v1.0), WFA(status=Failed), Error: Volume has the fixed file system size option set.**

When we get the above error please disable fs\_size\_fixed=off and grow the space. It's one time fix when we disable this option we won't get the above error on this volume in future.

Below is the command to disable the option

```
m6036149@c152mad:~> ssh ln-naslowcp-d06 vol options cb0538_fnr_eciborgappqa_nosnap fs_size_fixed off
```

Reference RITM - RITM0395617

#### Scenario 2:

**Error: Aggregate capacity checks against backup volume sv\_07\_cps\_vm\_grp01 have failed. The Unify Shared Storage Grow process cannot continue. A manual task will be assigned to Storage Support.**

This growth form has been created as when we grow for primary it will grow the backup volume automatically. When the Form tries to grow backup volume it will be checking the backup aggregate & over commitment. As per standard we won't set over commitment threshold on back aggregate. The form was set as 200% threshold which causes failures.

As per standard while creating backup volume we will set auto grow option where volume can grow up to 14TB automatically . So it is not dependent on primary volume growth.

If we get the above two scenario's we can proceed with space growth and close the RITMs. No BCS is required for this space growth.

#### Note:

We started using the Form recently, as of now we had seen couple of scenario's this document will be incrementally updated when we see new scenarios. In the mean development team will be working to bring down the scenario of failures. As of now scenario 2 will be fixed soon.

#### **4.6.12 CDOT/7MODE Growth iSCSI**

#### **4.6.13 CDOT/7MODE Instructions**

CDOT Capacity/Performance calculations

7MODE Capacity/Performance calculations

### **4.7 BU ENVIRONMENTS**

<This is a placeholder for some of the critical BU specific documentation and where to find them>

Scholar one

TAX and Accounting

- TRUST OTT/OTIR
- TAX provision
- TAX Gosystems and OIT

F&R collab

F&R DSS

### **4.8 CAPACITY PLANNING**

Capacity and Inventory management process is handled as outlined [here](#)

The NAS capacity Planning meeting is held every 2 weeks on Tuesday by Jonathan Stocks and represented by Storage Support and D&E teams. The NAS capacity Planning heatmap can be found [here](#). During this meeting, new HW orders, New file build status and Shelf Adds to meet capacity constraints are reviewed.

The storage support staff play an active role in working with capacity Planning to manage capacity on our storage infrastructure.

When any aggregate reaches its utilization threshold the procedures outlined below should be followed:

1. Plan a thin mitigation as per the outlined process.
2. Create two separate CRs one for Pre-migration (storage only) and one for cutover (including the post-migration CTs. The post migration tasks should include steps for clean-up).
3. Ensure a CR has been raised for clean-up task (reclaim offline/expired volumes etc.)
4. The cutover CR should have the relevant BU/Platform/DB team tasks and approvals and should be planned as per the BU maintenance window.
5. If there is no room to migrate to any available shared primary filer work with Capacity Planning team on shelf adds to grow available capacity.

#### **4.8.1 Guidelines to be strictly followed for all thin mitigation:**

- a. Ensure the Filer Aggregate utilization is below standard thresholds (standard thresholds are 75% for shared and 85% for backup filers) post migration. Ideally the utilization should not exceed 65% for shared filers.
- b. Ensure the Aggregate Overcommit is below thresholds (200%) for all filers except Backup filers. Ideally this should be ~190% for all filers except backup filers. Dedicated Filers do not have any overcommit levels and should be at 1:1.
- c. Ensure the performance checks are on the filers.



- i. Validate the physical Filer has sufficient room to accommodate the IOPS and throughput for new vfiler/volume. IOPS and throughput requirements should be available from requester or existing source vfiler if this is part of a migration.
- ii. For 7-Mode, ensure the TRP load script (perfinfo.pl) along with NMC is checked to determine if the filer has room to accommodate the new request.
- iii. For c-DOT use OPM/Grafana to review the performance on the target filer.
- iv. Performance metrics are not relevant for Backup filers and do not form part of review under usage such as deployments, backup and restores.
- d. DO NOT combine Different BU data in the same vfiler. Escalate if we are closer to hitting vfiler limits.**
- e. Review the performance on Source Vfiler/volume and ensure destination has room to accommodate this workload. For c-DOT ensure the IOPS are within standard 6k QOS values. If exceeding then review with D&E for exceptions.**
- f. Ensure the vfiler count is as per Standard thresholds. Standard thresholds are <65 for 7-mode and 128 for c-DOT.**
- g. Ensure volume counts are as per standards.**
- h. Ensure the destination/target Filer is from same Site, Module, Environment and Tier type and has same VLAN as source.**

#### 4.8.2 Aggregate Utilization at 75% on Primary Shared Filers(7-mode):

A thin mitigation (migration to alternate destination within same module) should be planned when capacity is available. The destination could be another 7-mode filer or c-DOT filer that has sufficient space and performance to accommodate the source vfile or volume being migrated. Outlined below is the process to perform thin mitigation from 7-mode source to a 7-mode target or c-DOT destination

| #                          | Checks  | Command to Run  | Comments  |
|----------------------------|---|---|---|
| <b><u>Source:</u></b>      |   |   |   |
| 1                          | Identify if the filer is CIS/CPS  | Based on the filer Name Refer to 7-mode and c-DOT Naming Standards. | ecom/lowep - CPS<br>corp/lowcp/lowcc - CIS<br>check if the filer is part of Tech Refresh (If the filer is part of Tech refresh plan for migration to C-MODE filer).<br>In C-Mode<br>DD is dedicated filer,<br>AA Archive,<br>SN - Shared Non-Prod<br>SP - Shared Prod |
| 2                          | Identify the Tier of the source filer.  | vol status -s   | If the disk RPM is 10K,15K its considered HT(High Tier).<br>7200K RPM drives are LT (Low Tier).   |
| 3                          | Check the current aggr utilization  | df -Ag  | Note the current utilization, and calculate how much capacity should be made available to keep the aggr below 65% utilization.  |
| 4                          | Identify volumes with in the aggr, that are good candidates for migration   | aggr show_space -g <>aggr_name>>                                    | identify the volumes which are most space consuming   |
| 5                          | Check the containing vfile of the volume identified for migration.  | vfile status -r   | check the vfile to which the volume belongs   |
| 6                          | Check the total usage on the vfile that's being targeted for migration and determine if you need to move entire vfile or a particular volume to bring down the usage. | vfile run <>vfile name>> df -h                                      | check the overall utilization on the vfile.   |
| 7                          | Check the number of IOPS the vfile/volume doing   | check using NMC   |   |
| 8                          | if moving a single volume check if it has CIFS or iSCSI   | CIFS shares/LUN show/ lgroup show                                   | Note down the igroup/LUN/Share details.   |
| 9                          | Check if the volumes has any SM/SV relation.  | 1) snapmirror/Snapvault status.                                     | Note the schedules and destination filer details; the same need to be reconfigured accordingly. Source cannot be migrated alone if there is a active SM relation to a 7-MODE destination filer. Choose only a 7-Mode filer as destination if source has active SM.    |
| 10                         | Check the vlan for the source vfile   | Lookup vlan information in zipper                                   | The destination filer and source filer should be in the same network and destination filer have the Vlan of the source vfile in which we are migrating.   |
| <b><u>Destination:</u></b> |   |   |   |
| 11                         | Login to DFM that hosts the source filer.   |   |   |

|    |  |   |  |
|----|--|---|--|
| 12 | Based on what's determined in step 1 & 2, find a filer of same type in the given DFM | dfm controller list   grep ecom/corp/low/   | determine the available filers of same class (CIS/CPS) and Tier.<br>If none of the filers are 7-Mode check for Shared C-MODE filers in the location and plan for 7MTT migration.<br>2) if the source filer is not part of Tech Refresh; recommend to use filer which are shared only (Name having SN/SP).  |
| 13 | Narrow down the filers based on capacity, over all allocation and performance.       | <b>For 7-MODE:</b><br>1) df -Ag.<br>2) aggr show-space -g<br><b>For C-MODE:</b><br>1) aggr show -aggregate * -fields root,availspace,percent-used,size  | 1) check the current utilization, aggr over commitment and calculate what would be final values post completion of migration.<br>2) utilization shouldn't be above 65% post migration.<br>3) Overcommitment shouldn't go above 200% post migration.  |
| 14 | Check the number of Vfilers on the destination.                                      | 1) vfiler limit - 7-MODE<br>2)vserver show -aggregate <>Aggr name>> - you need to run it for each data aggr on the node to get the count. - C-MODE  | 1) Do not use a filer which is already running >= 55 vfilers<br>2) C-DOT doesn't have this requirement; however ensure that the vservers are well spread between the cluster nodes when provisioning via WFA.  |
| 15 | Check the performance on the filer   | 1) Run /filers/admin/scripts/support/perfinfo script and select option 6 to see a week statistics. - 7-MODE<br>2) qos statistics performance show -iterations 0 -rows 10 -refresh-display false -node <<node name>> - C-MODE<br>3) dashboard performance show -node <<node name>> - C-MODE  | 1)the perfinfo output should show the load under warning/critical level for the filer. If the output shows these levels, identify another filer with similar characteristics as per steps 10-14.<br>2) Run sysstat to see the filer overall performance on 7-Mode check for CPU & disk utilization columns of sysstat -c 10 -s output to determine the average usage.<br>3) In NMC check that the filer overall read and write latencies are below 20ms and 5ms respectively |
| 16 | schedule for migration   | <b>For ESX volumes:</b><br>1) VI team will perform vmotion for ESX volumes. Rise a CR with 2-day lead time to create a new vfilier and volume using WFA.<br>2) Submit a SR to virtual team and provide new storage details which they will use to perform v-motion<br><b>For 7-MODE:</b><br>1) Do datamotion if entire vfilier can be migrated.<br>2) Perform Snapmirror migration if only a single volume need to be moved.<br><b>For C-MODE:</b><br>1) Create new vserver via the WFA and ensure that you chose the right template for NAS/CIFS/iSCSI etc if migrating to C-MODE.<br>2) Use 7MTT to perform the data copy if the destination is C-MODE filer. Refer to the 7MTT documentation for complete details. | Always use NMC for Datamotion if moving to 7-Mode. DO NOT perform manual migration.<br>For c-DOT, Once the new vserver is created using the right WFA template ensure the desired protocols are enabled.<br>>> net interface show -vserver <<vserver name>> -lif <<lif name>> -fields data-protocol<br>>> vserver show -vserver <<vserver name>> -fields allowed-protocols   |



|    |  |  |                                     |
|----|--|--|-------------------------------------|
|    |  | <u>For 7-MODE:</u><br>1) CIFS shares<br>2) LUN show<br>3) iscsi enable<br><u>For C-MODE:</u><br>4) Create the Vserver by choosing the right template in WFA for CIFS/iSCSI<br>5) cifs share show -vserver <<vserver name>> - to validate the CIFS shares<br>6) export-policy rule show -vserver <<Vserver name>> - To validate the NFS host access.<br>7) vol show -vserver <<vserver name>> -volume <<vol name>> -fileds junction-path,policy - to check the mountpoint and export policy associated. |                                     |
| 17 | For CIFS/iSCSI volume ensure the destination vfiler has the required licenses and enable (CIFS/iSCSI). | 1) CIFS setup<br>2) Refer to the CIFS/ISCSI C-MODE documentation for complete details.   |                                     |
| 18 | Configure SM and SV as required for the volumes post migration and do the necessary cleanup            | Check the SV and SM relations are still intact post successful migration.<br>1) Snapmirror status<br>2) Snapvault status<br>3) For c-DOT,Refer to the 7MTT document for complete set of commands to be run to configure SV.  | Compare the setting with the source |
| 19 | Ensure proper post mitigation clean ups are completed.   | 1) If migrated to C-MODE, cleanup the SM snapshots and any additional snap reserver allocated,<br>2) offline the vfiler/volume and rename it. Submit a CR to destroy it after 2 weeks.<br>3) Reclaim the vfiler IP by submitting a request in Zipper after 2 weeks.  |                                     |

#### 4.8.3 Aggregate Utilization at 75% on Primary Shared Filers(c-DOT):

##### Data Motion for Volumes (NFS protocol Only)

DataMotion for Volumes (often referred to as vol move) lets you move a volume within an SVM from one aggregate (the source) to another aggregate (the destination). The destination can be on the same node or any other node in the cluster.

There are four phases in the volume move process. Once the volume move is initiated, the progression of stages is automatic.

1. **Validation phase:** Verifies that the requested vol move is possible by checking available capacity on the destination aggregate as well as other requirements.
2. **Setup phase:** A new volume is created on the destination aggregate.
3. **Iterative phase:** Data is replicated from the source volume to the destination volume by replicating groups of Snapshot™ copies over the cluster network. After each iteration, the delta between the source and destination is checked to see if it is small enough that a final replication can be completed in the time defined for the cutover phase. I/O from clients and hosts to the source volume is not affected during this phase.
4. **Cutover phase:** All I/O access is queued and requests to the source volume are blocked. The final replication transfer is completed and the volume database is updated with the new volume information. Queued I/O is then resumed on the volume at the new location. The cutover completes in a defined "cutover period" that is within an acceptable window of time for the client/host application.

## Pre-requisites

1. Ensure you have reviewed all the guidelines outlined [here](#). Screenshots and examples specific to c-DOT are shown below:

- 1.1. Check the aggregate utilization on the destination aggregate on the (Utilization should be less than 65%).

| Aggregate      | Size    | Available | Used% | State  | #Vols | Nodes | RAID     | Status |
|----------------|---------|-----------|-------|--------|-------|-------|----------|--------|
| aggr1_data_h01 | 57.20TB | 12.10TB   | 79%   | online | 14    | h01   | raid_dp, | normal |
| aggr1_data_h01 | 57.20TB | 43.22TB   | 24%   | online | 21    | h02   | hybrid,  | normal |
| aggr1_data_101 | 81.49TB | 51.91TB   | 36%   | online | 26    | 101   | raid_dp, | normal |
| aggr1_data_102 | 81.49TB | 79.66TB   | 2%    | online | 27    | 102   | raid_dp, | normal |

- 1.2. Check the Overcommit on the aggregate (threshold is less than 200% and should not exceed 190% post migration ).Below is the reference screenshot. Calculate the total space and derive the overcommit value.

| Filesystem                                      | total  | used   | avail  | capacity | Mounted on  | Vserver           |
|---|--------|--------|--------|----------|---|-------------------|
| /vol/avtest/                                    | 972MB  | 3044KB | 9725MB | 0%       | /avtest   | av-cpssp01-d01    |
| /vol/avtest/.snapshot                           | 512MB  | 3456KB | 509MB  | 1%       | /avtest/.snapshot                                 | av-cpssp01-d01    |
| /vol/cb0392_at_fsp487p_n01oral_nosnap/          | 206GB  | 161GB  | 44GB   | 78%      | /cb0392_at_fsp487p_n01oral1_nosnap                | cpsprod-d0001     |
| /vol/cb0392_at_fsp487p_n01oral/.snapshot        | 0B     | 0B     | 0B     | 0%       | /cb0392_at_fsp487p_n01oral_nosnap/.snapshot       | cpsprod-d0001     |
| /vol/cb0392_at_fsp487p_s01oral/                 | 9358GB | 54%    | 4834GB | 54%      | /cb0392_at_fsp487p_s01oral_snap                   | cpsprod-d0001     |
| /vol/cb0392_at_fsp487p_s01oral/.snapshot        | 19TB   | 10TB   | 9TB    | 38%      | /cb0392_at_fsp487p_s01oral1_snap/.snapshot        | cpsprod-d0001     |
| /vol/cb0392_at_fsp487p_s01oral1/                | 5059GB | 1866GB | 3193GB | 37%      | /cb0392_at_fsp487p_s01oral_snap/.snapshot         | cpsprod-d0001     |
| /vol/cb0392_at_fsp487p_s01oral1/.snapshot       | 10GB   | 3047MB | 7192MB | 30%      | /cb0392_at_fsp487p_s01oraladml_snap/.snapshot     | cpsprod-d0001     |
| /vol/cb0392_at_fsp487p_s01oraladml/             | 2560MB | 1618MB | 941MB  | 63%      | /cb0392_at_fsp487p_s01oraladml1_snap/.snapshot    | cpsprod-d0001     |
| /vol/cb0392_at_fsp487p_s01oraladml1/            | 2560MB | 1618MB | 941MB  | 63%      | /cb0392_at_fsp487p_s01oraladml1/.snapshot         | cpsprod-d0001     |
| /vol/cpsprod_d0001_root/                        | 972MB  | 384KB  | 972MB  | 0%       | ---   | cpsprod-d0001     |
| /vol/cpsprod_d0001_root/.snapshot               | 51MB   | 1584KB | 49MB   | 3%       | ---   | cpsprod-d0001     |
| /vol/cb0295_trta_ftpdataproddtc1_nosnap/        | 48GB   | 9068KB | 47GB   | 0%       | /cb0295_trta_ftpdataproddtc1_nosnap               | cpsprod-d0005     |
| /vol/cb0295_trta_ftpdataproddtc1/.snapshot      | 9438GB | 5080GB | 4358GB | 54%      | /cb0295_trta_ftpdataproddtc11_nosnap/.snapshot    | cpsprod-d0005     |
| /vol/cb0295_trta_ftpdataproddtc11_nosnap/       | 9438GB | 5080GB | 4358GB | 54%      | /cb0295_trta_ftpdataproddtc11/.snapshot           | cpsprod-d0005     |
| /vol/cpsprod_d0005_root/                        | 972MB  | 392KB  | 972MB  | 0%       | ---   | cpsprod-d0005     |
| /vol/cpsprod_d0005_root/.snapshot               | 51MB   | 1696KB | 49MB   | 3%       | ---   | cpsprod-d0005     |
| /vol/cpsprod_d0006_root/                        | 972MB  | 396KB  | 972MB  | 0%       | ---   | cpsprod-d0006     |
| /vol/cpsprod_d0006_root/.snapshot               | 51MB   | 1516KB | 49MB   | 3%       | ---   | cpsprod-d0006     |
| /vol/cpsprod_d0014_root/                        | 972MB  | 388KB  | 972MB  | 0%       | ---   | cpsprod-d0014     |
| /vol/cpsprod_d0014_root/.snapshot               | 51MB   | 1556KB | 49MB   | 3%       | ---   | cpsprod-d0014     |
| /vol/cb0584_fnr_pccdbdtcp_n01oral_nosnap/       | 1858GB | 896GB  | 961GB  | 48%      | /cb0584_fnr_pccdbdtcp_n01oral_nosnap              | cpsprod-d0017     |
| /vol/cb0584_fnr_pccdbdtcp_n01oral/.snapshot     | 0B     | 0B     | 0B     | 0%       | /cb0584_fnr_pccdbdtcp_n01oral_nosnap/.snapshot    | cpsprod-d0017     |
| /vol/cb0584_fnr_pccdbdtcp_s01oral_snap/         | 18TB   | 16TB   | 2020GB | 89%      | /cb0584_fnr_pccdbdtcp_s01oral_snap                | cpsprod-d0017     |
| /vol/cb0584_fnr_pccdbdtcp_s01oral/.snapshot     | 4608GB | 2298GB | 2308GB | 50%      | /cb0584_fnr_pccdbdtcp_s01oral1_snap/.snapshot     | cpsprod-d0017     |
| /vol/cb0584_fnr_pccdbdtcp_s01oraladml_snap/     | 25GB   | 947MB  | 24GB   | 4%       | /cb0584_fnr_pccdbdtcp_s01oraladml_snap            | cpsprod-d0017     |
| /vol/cb0584_fnr_pccdbdtcp_s01oraladml/.snapshot | 6400MB | 797MB  | 5602MB | 12%      | /cb0584_fnr_pccdbdtcp_s01oraladml1_snap/.snapshot | cpsprod-d0017     |
| /vol/cpsprod_d0017_root/                        | 972MB  | 396KB  | 972MB  | 0%       | ---   | cpsprod-d0017     |
| /vol/cpsprod_d0017_root/.snapshot               | 51MB   | 1612KB | 49MB   | 3%       | ---   | cpsprod-d0017     |
| /vol/reserve_h01_d0002_root/                    | 972MB  | 376KB  | 972MB  | 0%       | ---   | reserve_h01_d0002 |
| /vol/reserve_h01_d0002_root/.snapshot           | 51MB   | 1568KB | 49MB   | 3%       | ---   | reserve_h01_d0002 |

- 1.3. Check if the Vlan exists on destination Cluster.

| (network port vlan show) |          |      |      |                   |         |             |
|--------------------------|----------|------|------|-------------------|---------|-------------|
| Node                     | VLAN     | Name | Port | Network           | Network | MAC Address |
|                          |          |      |      | VLAN ID           |         |             |
| ln-cps-clsp-d01-h01      | a0a-2004 | a0a  | 2004 | 02:a0:98:a5:db:8d |         |             |
|                          | a0a-2006 | a0a  | 2006 | 02:a0:98:a5:db:8d |         |             |
|                          | a0b-2004 | a0b  | 2004 | 02:a0:98:a5:db:8e |         |             |
| ln-cps-clsp-d01-h02      | a0a-2004 | a0a  | 2004 | 02:a0:98:a5:53:4c |         |             |
|                          | a0a-2006 | a0a  | 2006 | 02:a0:98:a5:53:4c |         |             |
|                          | a0b-2004 | a0b  | 2004 | 02:a0:98:a5:53:4d |         |             |

- 1.4. Validate the target Filer is from same Site(Datacenter), Module(ecom, corp, colo), Environment (shared, dedicated, backup, mgmt etc. ) and Tier type(Tier1, Tier )**

```
ln-cps-clsp-d01::> node run -node ln-cps-clsp-d01-h02 aggr status -s

Spare disks

RAID Disk      Device      HA SHELF BAY CHAN Pool Type   RPM  Used (MB/blks)  Phys (MB/blks)
-----  -----
Spare disks for block checksum
spare        0b.33.23    0b    33  23  SA:A   -    SAS 10000 560000/1146880000 572325/1172123568
spare        0b.34.22    0b    34  22  SA:A   -    SAS 10000 560000/1146880000 572325/1172123568
spare        0b.34.23    0b    34  23  SA:A   -    SAS 10000 560000/1146880000 572325/1172123568
spare        0b.35.22    0b    35  22  SA:A   -    SAS 10000 560000/1146880000 572325/1172123568
spare        0b.35.23    0b    35  23  SA:A   -    SAS 10000 560000/1146880000 572325/1172123568
spare        3c.30.23    3c    30  23  SA:B   -    SAS 10000 560000/1146880000 572325/1172123568
spare        3c.31.23    3c    31  23  SA:B   -    SAS 10000 560000/1146880000 572325/1172123568
spare        3c.32.23    3c    32  23  SA:B   -    SAS 10000 560000/1146880000 572325/1172123568
spare        3a.10.23    3a    10  23  SA:B   -    SSD  N/A   381304/780910592  381554/781422768
```

- 1.5. Check for any snap mirror relationships**

```
ln-cps-clsp-d01::> snapmirror show -source-vserver cpsprod-d0017
There are no entries matching your query.
```

- 1.6. Review the performance on Source Vfiler/volume. For c-DOT ensure the IOPS are within standard 6k QOS values. If exceeding then review with D&E for exception and approvals.**

- 1.7. Check the performance of target filer (system utilization for one month in grafana/OPM tool). Reference screenshot from grafana shown below. Ensure the target filer has sufficient room to accommodate the source workload.**



- 1.8. Ensure the vfiler count is as per Standard thresholds.**

- 1.9. Ensure volume counts are as per standards.**

## High level steps for volume move to perform without downtime (Automatic Cutover)

1. Raise a normal change with BU teams as approvers. Notify the BU and initiate a kick off email. Attach the pre-check document to the change, commads in the below txt file.



Pre-checks.txt

2. Move all the volumes in vserver including root volume of vserver one by one from source to target aggregate without any downtime.
3. Migrate the LIF from node Source node to target node & change the home node/port.

## Step by Step process for performing automatic cutover

1. Command to perform volume move and automatic cutover :

```
➤ volume move start -vserver vserver_name -volume volume_name -destination-aggregate  
aggr_name -cutover-window 45 -cutover-attempts 3 -cutover-action defer_on_failure -perform-  
validation-only false -foreground false  
m6037398@c152mad:~> volume move start -vserver cpsprod-f0046 -volume cb0234_tsh_endnote_prod1_nosnap -destination-aggregate  
aggr1_data_h02 cutover-window 45 -cutover-attempts 3 -cutover-action defer_on_failure -perform-validation-only false -for  
eground false
```

2. Command to check the volume move status: (shows us how much percent of data copy completed)

```
➤ Vol move show -vserver vservername
```

```
volume move show -vserver cpsprod-f0046
```

Output as follows -

| Vserver | Volume | State | Move Phase | Percent-Complete | Time-To-Complete |
|---------|--------|-------|------------|------------------|------------------|
|---------|--------|-------|------------|------------------|------------------|

```
-----  
cpsprod-f0046 cb0234_tsh_endnote_prod1_nosnap done completed 100% -  
cpsprod-f0046 cb0234_tsh_endnote_prod2_nosnap done completed 100% -  
cpsprod-f0046 cb0234_tsh_endnote_prod3_nosnap done completed 100% -  
cpsprod-f0046 cb0234_tsh_endnote_prod4_nosnap done completed 100% -  
cpsprod-f0046 cb0234_tsh_endnote_web1_snap done completed 100% -  
cpsprod-f0046 cb0234_tsh_endnote_web2_snap done completed 100% -  
cpsprod-f0046 cb0234_tsh_endnote_web3_snap done completed 100% -  
cpsprod-f0046 cb0234_tsh_endnote_web4_snap healthy replicating 30% Mon Jul 03 13:14:34 2017
```

3. Command to migrate LIF & changing the home node/port:

```
➤ net int migrate -vserver vservername -lif lif_name -destination-node dest_nodename -destination-  
port port_name
```

```
m6037398@c152mad:~> net int migrate -vserver cpsprod-f0046 -lif cpsprod-f0046-lif01 -destination-node eg-cps-clsp-f01-101 -  
destination-port a0a-3022
```



➤ net int modify -vserver vservername -lif lif\_name -home-node nodename -home-port port\_name

```
m6037398@c152mad:~> net int modify -vserver cpsprod-f0046 -lif cpsprod-f0046-lif01 -home-node eg-cps-clsp-f01-101 -home-port a0a-3022
```

## Post checks to be completed post migration

4. Command to see if it's migrated to desired aggregate

➤ vserver show -vserver cpsprod-d0017 -fields aggregate

```
ln-cps-clsp-d01::> vserver show -vserver cpsprod-d0017 -fields aggregate
vserver      aggregate
-----
cpsprod-d0017 aggr1_data_h01
```

5. Command to check lif migration and home port.

➤ net int show -vserver cpsprod-f0046

```
m6037398@c152mad:~> ssh eg-cps-clsp-f01 net int show -vserver cpsprod-f0046
(network interface show)
      Logical      Status      Network      Current      Current  Is
Vserver     Interface   Admin/Oper Address/Mask    Node       Port   Home
-----
cpsprod-f0046
      cpsprod-f0046-lif01 up/up 10.215.126.43/23 eg-cps-clsp-f01-101 a0a-3022 true
```

6. Ensure DBA/BU checkouts are completed and CR/CT closed on time

7. Monitor the Aggregate utilization on both Source and Target

### 4.8.4 Aggregate Utilization at 75% on Archive Log Filers (7-mode and c-DOT):

#### Overview:

Please follow the procedure below when you encounter aggregate utilization thresholds breaching on Archive log filers or when shared Archive log volumes are becoming full.

Per design Database archives are configured with Primary and Secondary Archive log location. The primary location is a configured to hold archive logs as per the desired retention days. The secondary archive log location is a qtree with limited amount of storage to hold archives temporarily and should only be used in the event of emergency situation or during migrations.

The primary archive log in most cases would be the c-DOT archive log filers. However, some primary archive log destinations exist on 7-mode filers and are in the process of being migrated to c-DOT filers in strategic datacentres.

The secondary archive log location is a qtree created on shared volume and could be located on either 7-mode or c-DOT filer.

Archive logs are backed up based on the retention. In our environment, we have 7days, 14days, 30days and 45days retention available. We are using scripts to clean up the old or expired volumes. The archive log clean-up scripts are maintained by storage D&E team.

#### How does Archiving on NAS work:

Each DB has both primary and secondary archive log volume/qtree mounted by default. In case, of any issues on primary the archive log will failover to secondary. If we get alerts notifying archive logs are writing on secondary, then we need to check from storage and confirm with unix that primary mounts are available and followup with respective

DB team to failback the archlogs to primary. The arch log failover can be triggered when the primary mounts are not available or DB team has ran script to failover to secondary.

In the event that this primary log backup storage is unavailable due to a planned or unplanned outage, database switches to writing the archive logs to a Secondary log backup storage (7 Mode NetApp NFS mountpoint). secondary is configured as a single thin provisioned volume per datacenter module named infra\_nosnap, with each instance of Oracle having it's own qtree for archive log storage.

If the archive logs continue to run on secondary due to issues on primary, we need to monitor the storage space on the secondary volume and filer until it gets failed back to primary as it's a shared volume/storage and there are chances of it becoming full. We need to notify the DBA team and work with unix and DB teams to redirect the archive logs to primary.

### **Archive log(archlog) 7-mode cleanup scripts:**

The 7-Mode below CIS and CPS scripts configured for the archive log cleanup on dfm jumpbox **c152mad.int.thomsonreuters.com**.

```
#Archive prune script
30 20 * * * root /filers/admin/scripts/support/Archlog_delete_cps_Netapp.sh
30 20 * * * root /filers/admin/scripts/support/Archlog_delete_cps_Netapp_Newnan.sh
30 9 * * * root /filers/admin/scripts/support/Archlog_delete_cis_Netapp.sh
```

The working process of script can be viewed from each script. The script targets both primary and secondary archive log vfilers and cleans up old or expired archlogs.

In 7-mode filers we have primary and secondary archlogs available for all sites and buildings. In C-DoT we have dedicated filers for the archlog.

### **Archlog C-dot cleanup scripts:**

The C-DOT archive log pruning script is available at below location on each SITE CDOT dfm servers.

```
##Archlog pruning script
0 9 * * *      root /filers/admin/scripts/support/cdot_archivelog_pruning.sh
```

### **Troubleshooting Steps:**

We need to check whether the script is running or NOT by verifying any of the archive log mounts. If the archive logs are getting cleaned up correctly then the archive log volumes/qtree will have archive log files as per retention and we can consider the script is not working. Check the archive mounts have proper permissions to the respective DFM to cleanup the archlogs. If all mounts are working and there is issue with script itself then we need to reach out or escalate to storage D&E and work with them in fixing the issue.

### **Mitigation steps to reduce Utilization**

1. In cases where the aggregate utilization reaches above threshold and pruning script does not properly, request DBA team to do manual clean up first and if they are unable to do so then perform it from storage end with a proper change and BU approvals.
2. Check for expired volumes on the filer for clean-up  
we can run `ssh <filer_name> aggr show_space` which gives the list of volumes in the aggregate with status including offline volumes. We can cross-check the offline volumes and can cleanup eligible volumes to reclaim the space.

3. If it's a critical situation then check if there are any space disks on the filer, can consider adding them to increase the capacity of the filer aggregate.
4. For manual cleanup follow the below steps:

- a. need to mount the archive log volume to one of dfm's temp directory.

```
c152mad:~ # mount ded-ecom-d0001:/vol/infra_oraarchpri_cps_TCM_nosnap /mnt/ram
c152mad:~ # cd /mnt/ram
```

- b. List out the directories available

- c. Find the biggest directory using the below script and check if there are any old or expired archive logs.

```
/filers/admin/scripts/support/findbig.sh <volume mount>
```

```
u0159922@cl52mad:/filers/admin/scripts/support> ./findbig.sh /filers/prod-corp-k0001-arch
This Script will find the Top 10 biggest directories and Top 10 biggest files on LOCAL filesystem
#####
Here Comes the biggest directories on /filers/prod-corp-k0001-arch
#####
du: cannot read directory '/filers/prod-corp-k0001-arch/wlasia_7_anazq_n01mysqlarch1/performance_schema': Permission denied
du: cannot read directory '/filers/prod-corp-k0001-arch/wlasia_7_anazq_n01mysqlarch1/MYWAQ02A': Permission denied
du: cannot read directory '/filers/prod-corp-k0001-arch/wlasia_7_anazq_n01mysqlarch1/mysql': Permission denied
    3.5 G *****/filers/prod-corp-k0001-arch
    1.8 G *****/filers/prod-corp-k0001-arch/infra_14_emat754p_n0loraarch1
    1.8 G *****/filers/prod-corp-k0001-arch/infra_14_emat754p_n0loraarch1/orp754a
    1.7 G *****/filers/prod-corp-k0001-arch/infra_14_emat755p_n0loraarch1
    1.7 G *****/filers/prod-corp-k0001-arch/infra_14_emat755p_n0loraarch1/orp755a
    44.0 K *****/filers/prod-corp-k0001-arch/wlasia_7_anazq_n01mysqlarch1
    36.00 K *****/filers/prod-corp-k0001-arch/infra_7_cc114p_n0loraarch1
    8.00 K ****/filers/prod-corp-k0001-arch/wlasia_7_anazq_n01mysqlarch1/mysql
    4.00 K ***/filers/prod-corp-k0001-arch/wlasia_7_anazq_n01mysqlarch1/performance_schema
    4.00 K ***/filers/prod-corp-k0001-arch/wlasia_7_anazq_n01mysqlarch1/MYWAQ02A

Here Comes the biggest files on /filers/prod-corp-k0001-arch
#####
find: '/filers/prod-corp-k0001-arch/wlasia_7_anazq_n01mysqlarch1/performance_schema': Permission denied
find: '/filers/prod-corp-k0001-arch/wlasia_7_anazq_n01mysqlarch1/MYWAQ02A': Permission denied
find: '/filers/prod-corp-k0001-arch/wlasia_7_anazq_n01mysqlarch1/mysql': Permission denied
    57028 KB /filers/prod-corp-k0001-arch/infra_14_emat754p_n0loraarch1/orp754a/LOG_863429750_39805 1.ARC
    38932 KB /filers/prod-corp-k0001-arch/infra_14_emat755p_n0loraarch1/orp755a/LOG_863362134_39887 1.ARC
    38476 KB /filers/prod-corp-k0001-arch/infra_14_emat754p_n0loraarch1/orp754a/LOG_863429750_39708 1.ARC
    37768 KB /filers/prod-corp-k0001-arch/infra_14_emat754p_n0loraarch1/orp754a/LOG_863429750_39372 1.ARC
    35016 KB /filers/prod-corp-k0001-arch/infra_14_emat755p_n0loraarch1/orp755a/LOG_863362134_39599 1.ARC
    34656 KB /filers/prod-corp-k0001-arch/infra_14_emat755p_n0loraarch1/orp755a/LOG_863362134_39455 1.ARC
    34276 KB /filers/prod-corp-k0001-arch/infra_14_emat755p_n0loraarch1/orp755a/LOG_863362134_39791 1.ARC
    34084 KB /filers/prod-corp-k0001-arch/infra_14_emat755p_n0loraarch1/orp755a/LOG_863362134_39743 1.ARC
    34044 KB /filers/prod-corp-k0001-arch/infra_14_emat755p_n0loraarch1/orp755a/LOG_863362134_39935 1.ARC
    34036 KB /filers/prod-corp-k0001-arch/infra_14_emat755p_n0loraarch1/orp755a/LOG_863362134_39551 1.ARC
u0159922@cl52mad:/filers/admin/scripts/support>
```

- d. If find any old or expired archive logs, please proceed with cleaning up with them manually.

5. If no clean-up/space add is possible then we need to plan a migration to dedicated c-DOT archive log filers using the standard process for the migration. If the archive log is already on a c-DOT filer and there is no other node available for migration then reach out to D&E/Capacity Planning for shelf add/node add on the c-DOT cluster.

*Oracle archive logs will be written to a NFS mountpoint served by a different Vserver that resides on a dedicated cDOT log backup storage system. The dedicated cDOT log backup storage system will have one volume per Oracle instance with no qtrees being used, and it will be configured with post-process compression. The volume name will have \_<ret#>\_ in it, where <ret#> is the number of days that the logs are retained, with the possible values being 7, 14, 30, or 45.*

High level steps for migrating to c-DOT are as below:

- a. Ensure you have reviewed all the guidelines outlined [here](#).

- b. NFS mount points are used by the database for archive log storage. These volumes should be created by using WFA as documented in the Provisioning procedures.

Ex: Sample archive log volumes in C-DoT filer shown below.

| eg-cis-claa-f01::> vol show<br>(volume show) |   |                         |        |      |         |           |       |
|--|---|-------------------------|--------|------|---------|-----------|-------|
| Vserver                                      | Volume  | Aggregate               | State  | Type | Size    | Available | Used% |
| cisdb2-f0030                                 | cb0182_sap_pocf01_45_n01db2_nosnap            | aggr1_data_sata2000_n02 | online | RW   | 68.36TB | 55.26TB   | 19%   |
| cisdb2-f0030                                 | cisdb2_f0030_root                             | aggr1_data_sata2000_n02 | online | RW   | 1GB     | 972.4MB   | 5%    |
| cismssql-f0001                               | cb0008_tasql1qa_7_sqlarch1_nosnap             | aggr1_data_sata2000_n01 | online | RW   | 68.36TB | 45.49TB   | 33%   |
| cismssql-f0001                               | cb0037_servicemanagerdev_45_sqlarch1_nosnap   | aggr1_data_sata2000_n01 | online | RW   | 68.36TB | 45.49TB   | 33%   |
| cismssql-f0001                               | cb0037_vcdprod_14_sqlarch1_nosnap             | aggr1_data_sata2000_n01 | online | RW   | 68.36TB | 45.49TB   | 33%   |
| cismssql-f0001                               | cb0109_mytimeproddbe2_14_sqlarch1_nosnap      | aggr1_data_sata2000_n01 | online | RW   | 68.36TB | 45.49TB   | 33%   |
| cismssql-f0001                               | cb0111_anovercontinuumprod_14_sqlarch1_nosnap | aggr1_data_sata2000_n01 | online | RW   | 68.36TB | 45.49TB   | 33%   |
| cismssql-f0001                               | cb0111_ccuresat2sqlprod_7_sqlarch1_nosnap     | aggr1_data_sata2000_n01 | online | RW   | 68.36TB | 45.49TB   | 33%   |

- c. Once the volumes are created schedule a cutover with DBA team and perform the following action plan.
- Initiate a kick off mail.
  - DBA team will fail over to arch log generation from primary to secondary location mounts on the respective servers.
  - Unix team will perform unmount and mount oraarch1 FS's with mentioned mount point names. Check and set permissions similar to previous mountpoint  
/n01/oraarch1 to /n01/oraarch1\_old  
/n01/oraarch1\_new to /n01/oraarch1
  - DB team will fail over to arch log generation from secondary to primary location mounts on the respective servers and do the final post checks.

- v. Storage team will complete the rename and offline of the primary volume/qtree and mark it for expiry and raise a CR to reclaim after expiry date.
- d. The old archive logs will be available to application/oracle team till they get expired on the old mounts.

#### 4.8.5 Aggregate Utilization at 85% on Backup Filers(7-mode):

Follow the steps outlined below when an aggregate on our backup filer reaches >=85% utilization.

##### 1. Mitigation checks to do before the migration:

- 1.1. Check if there are any unused/expired volumes. On the Filer whose aggregate utilization is >85% check if there are any unused/expired volumes to bring down the utilization.

```
u0159922@c152mad:~> ssh eg-nascorpbkp-h02 df -Ah
Aggregate          total        used      avail capacity
agrgr_h250_64       87TB       74TB      12TB     85%
agrgr_h250_64/.snapshot    0TB       0TB      0TB      0%
agrgr_h251_64_FULL     87TB       63TB      23TB     73%
agrgr_h251_64_FULL/.snapshot 0TB       0TB      0TB      0%
agrgr_h252_64_FULL     87TB       62TB      24TB     71%
agrgr_h252_64_FULL/.snapshot 0TB       0TB      0TB      0%
agrgr_root_FULL       744GB      101GB     643GB    14%
agrgr_root_FULL/.snapshot 0TB       0TB      0TB      0%
u0159922@c152mad:~>
```

If there are any such volumes check the snapshots and confirm the expiry date based on volume retention. If the snapshots on the volume retention are expired we can consider the cleanup of the volume or can rename it with expiry date so that it can be cleaned up later.

Before cleaning up expired volume confirm that there is no active snapvault relationship exist for the volume. (For ora volumes we might have disabled snapvault upon request from DB team)

Ex:

```
u0159922@c152mad:~> ssh mp-nascorpbkp-x01 snap list sv_14_ct_pcats2p_s01oraadml_snap_CR08071885_EXP_Nov132016
Volume sv_14_ct_pcats2p_s01oraadml_snap_CR08071885_EXP_Nov132016
working...
-----
```

| %/used    | %/total  | date         | name  |
|-----------|----------|--------------|---|
| 0% ( 0%)  | 0% ( 0%) | Oct 30 02:05 | sv_ct_pcats2p_s01oraadml_snap.0   |
| 0% ( 0%)  | 0% ( 0%) | Oct 30 02:05 | cis-cs-bkp-x01(0118075043)_sv_14_ct_pcats2p_s01oraadml_snap-base.1 (busy,snapvault) |
| 0% ( 0%)  | 0% ( 0%) | Oct 29 02:05 | sv_ct_pcats2p_s01oraadml_snap.1   |
| 8% ( 8%)  | 0% ( 0%) | Oct 28 02:06 | sv_ct_pcats2p_s01oraadml_snap.2   |
| 11% ( 4%) | 0% ( 0%) | Oct 27 02:06 | sv_ct_pcats2p_s01oraadml_snap.3   |
| 18% ( 8%) | 1% ( 0%) | Oct 26 02:05 | sv_ct_pcats2p_s01oraadml_snap.4   |
| 22% ( 6%) | 1% ( 0%) | Oct 25 02:06 | sv_ct_pcats2p_s01oraadml_snap.5   |
| 24% ( 3%) | 1% ( 0%) | Oct 24 02:07 | sv_ct_pcats2p_s01oraadml_snap.6   |
| 27% ( 6%) | 1% ( 0%) | Oct 23 02:06 | sv_ct_pcats2p_s01oraadml_snap.7   |
| 32% ( 9%) | 2% ( 0%) | Oct 22 02:06 | sv_ct_pcats2p_s01oraadml_snap.8   |
| 35% ( 6%) | 2% ( 0%) | Oct 21 02:06 | sv_ct_pcats2p_s01oraadml_snap.9   |
| 37% ( 6%) | 2% ( 0%) | Oct 20 02:06 | sv_ct_pcats2p_s01oraadml_snap.10  |
| 39% ( 6%) | 2% ( 0%) | Oct 19 02:05 | sv_ct_pcats2p_s01oraadml_snap.11  |
| 40% ( 3%) | 2% ( 0%) | Oct 18 02:06 | sv_ct_pcats2p_s01oraadml_snap.12  |
| 43% ( 8%) | 3% ( 0%) | Oct 17 02:06 | sv_ct_pcats2p_s01oraadml_snap.13  |
| 64% (50%) | 6% ( 3%) | Jul 31 02:10 | sv_ct_pcats2p_s01oraadml_snap_s01oradata1.0   |
| 64% ( 0%) | 6% ( 0%) | Jul 30 02:09 | sv_ct_pcats2p_s01oraadml_snap_s01oradata1.1   |
| 64% ( 0%) | 6% ( 0%) | Jul 29 02:10 | sv_ct_pcats2p_s01oraadml_snap_s01oradata1.2   |
| 64% ( 0%) | 6% ( 0%) | Jul 28 02:11 | sv_ct_pcats2p_s01oraadml_snap_s01oradata1.3   |
| 64% ( 0%) | 6% ( 0%) | Jul 27 02:12 | sv_ct_pcats2p_s01oraadml_snap_s01oradata1.4   |
| 64% ( 0%) | 6% ( 0%) | Jul 26 02:11 | sv_ct_pcats2p_s01oraadml_snap_s01oradata1.5   |
| 64% ( 0%) | 6% ( 0%) | Jul 25 02:10 | sv_ct_pcats2p_s01oraadml_snap_s01oradata1.6   |
| 64% ( 0%) | 6% ( 0%) | Jul 24 02:10 | sv_ct_pcats2p_s01oraadml_snap_s01oradata1.7   |
| 64% ( 0%) | 6% ( 0%) | Jul 23 02:11 | sv_ct_pcats2p_s01oraadml_snap_s01oradata1.8   |
| 64% ( 0%) | 6% ( 0%) | Jul 22 02:12 | sv_ct_pcats2p_s01oraadml_snap_s01oradata1.9   |
| 64% ( 0%) | 6% ( 0%) | Jul 21 02:12 | sv_ct_pcats2p_s01oraadml_snap_s01oradata1.10  |
| 64% ( 0%) | 6% ( 0%) | Jul 20 02:12 | sv_ct_pcats2p_s01oraadml_snap_s01oradata1.11  |
| 64% ( 0%) | 6% ( 0%) | Jul 19 02:11 | sv_ct_pcats2p_s01oraadml_snap_s01oradata1.12  |
| 64% ( 0%) | 6% ( 0%) | Jul 18 02:13 | sv_ct_pcats2p_s01oraadml_snap_s01oradata1.13  |

In the above example, the volume retention is 14 days and last snapshot was taken on Oct 30 so the volume will expire on 13<sup>th</sup> Nov. We can follow the change process and clean-up this expired volume.

- 1.2. Check if there are any duplicate snapvault relations for a volume.
  - This needs to be verified manually for each volume. If we find any duplicate relationships then the volume with highest lag relation should be cleaned up using steps outlined in step 1.1 above.
- 1.3. Check for any spare disk capacity. This is unlikely and should only be added after approval from D&E.

## 2. Identify the volume/volumes and backup destination filer for the migration.

- 2.1. Ensure you have reviewed all the guidelines outlined [here](#).
  - Check the VLAN being used and ensure the destination backup filer has the required VLAN. If not additional network connectivity may be needed. Take note of special VLANs for colo, TTA, CLEAR etc.

```
u0159922@c152mad:~> ssh eg-nascorpbkp-h02 vfiler status
vfiler0                         running
cis-cs-bkp-h02                  running
cis-ss-bkp-h02                  running
corph2                           running
cps-cs-bkp-h02                  running
cps-ss-bkp-h02                  running
cps-ttabkp-2503                 running
cps-ttabkp-2900                 running
cps-ttabkp-3702                 running
cps-ttatzbkp-2524               running
cps-ttatzbkp-2528               running
cps-ttatzbkp-2536               running
ecomh2                           running
eg-nascorpbkp-h02-corpvsip     running
eg-nascorpbkp-h02-ecomvsip     running
eg-nascorpbkp-h02-ttavsip-2503 running
eg-nascorpbkp-h02-ttavsip-2524 running
eg-nascorpbkp-h02-ttavsip-2900 running
eg-nascorpbkp-h02-ttavsip-3702 running
eg-nascorpbkp-h02-ttazvsip-2536 running
u0159922@c152mad:~>
```

Above example shows a mix of VLANs including special TTA VLAN. If selecting vfiler/volume in special VLAN like TTA ensure this exists on target backup filer.

Note: In some cases the vlan may be available on a c-DOT filer in which case a migration of both Primary and backup volume may need to be considered.

Same is the case with below COLO and CLEAR vlan's

```
u0159922@c152mad:~> ssh eg-nascorpbkp-f03 vfiler status
vfiler0                         running
cis-colo-bkp-f03                running
cis-cs-bkp-f03                  running
cis-ss-bkp-f03                  running
cps colo-bkp_f03                running
cps-cs-bkp-f03                  running
cps-ss-bkp-f03                  running
eg-nascorpbkp-f03-colovsip-3001 running
eg-nascorpbkp-f03-colovsip-3003 running
eg-nascorpbkp-f03-corpvsip-3053 running
eg-nascorpbkp-f03-corpvsip     running
eg-nascorpbkp-f03-ecomvsip     running
u0159922@c152mad:~>
```

- Cross site backups should NOT be configured. All backups should go to the same site and module backup Filers. Destination aggregate and filer should be from same site (Eagan->Eagan, Plano->Plano) and module ( corp->corp, ecom->ecom)

Ex: Do NOT configure cross-site snapvault from Eagan Site E to Eagan Site F

- 2.2. Identify the Source volume for migration.
  - We can select single or multiple volumes based on size to bring down the aggregate utilization to < 85%

For example, below we have selected a volume in corp network in Eagan.

```
u0159922@c152mad:~> ssh eg-nascorpbkp-h02 vfile run cis-cs-bkp-h02 vol status sv_14_infra_emat558p_s0lora1_snap
===== cis-cs-bkp-h02
      Volume State          Status           Options
      sv_14_infra_emat558p_s0lora1_snap online      raid_dp, flex
                                         sis           nosnap=on, guarantee=none, fractional_reserve=0
                                         64-bit
      Volume UUID: 2d4da7b1-0eeb-11e3-9157-123478563412
      Containing aggregate: 'aggr_h250_64'
u0159922@c152mad:~>
```

```
u0159922@c152mad:~> ssh eg-nascorpbkp-h02 vfile status -a cis-cs-bkp-h02 |head -10
cis-cs-bkp-h02                         running
  ipspace: corp-2502
  IP address: 10.206.122.67 [corpvinf-2502]
  Path: /vol/cis_cis_bkp_h02_root [/etc]
```

As per the related vfile naming convention this is a CIS vfile. So, we have to move this volume on new destinations CIS vfile.

- Check the volume size.

```
-----.
u0159922@c152mad:~> ssh eg-nascorpbkp-h02 vol size sv_14_infra_emat558p_s0lora1_snap
vol size: Flexible volume 'sv_14_infra_emat558p_s0lora1_snap' has size 100g.
u0159922@c152mad:~>
```

- Check and make note of the snapvault status of the volume

```
u0159922@c152mad:~> ssh eg-nascorpbkp-h02 vfile run cis-cs-bkp-h02 snapvault status /vol/sv_14_infra_emat558p_s0lora1_snap/1
===== cis-cs-bkp-h02
Snapvault is ON.
Source                               Destination
prod-corp-f0314:/vol/infra_emat558p_s0lora1_snap  cis-cs-bkp-h02:/vol/sv_14_infra_emat558p_s0lora1_snap/1  State   Lag    Status
                                                Snapvaulted   08:47:14  Idle
```

### 2.3. Identify the destination Filer and Aggregate from belonging to same site and module with same vlan connectivity.

- Validate the aggregate utilization stays below 85% if the source volume is migrated to this filer.
  - ssh <filernname> df -Ah
  - Select less utilized aggregate for the migration.
- Check volume count of the destination filer. If the volume count is full and can't accommodate any more volumes need to follow above steps (1.1) for the cleanup.

If no cleanup is possible then we can select another filer or perform grouping.

- ssh <filernname> vol status | egrep "sv\_|\_root" | wc -l

### 2.4. Create new volume on the destination filer. Before creating new volume in destination, check and confirm that there is no volume with the same name.

```
u0159922@c152mad:~> ssh eg-nascorpbkp-f04 vol status sv_14_infra_emat558p_s0lora1_snap
vol status: No volume named 'sv_14_infra_emat558p_s0lora1_snap' exists.
u0159922@c152mad:~>
```

### 2.5. Create a new destination filer with same size and properties and associate with respective vfile

#### 2.6. Intialize snapmirror and monitor the transfer status.

- >ssh <destination filer> vfile run <destination vfile> snapmirror initialize -S <source vfile:source volume> <destination volume>

- And monitor the status
  - >ssh <destination filer> vfiler run <destination vfiler> snapmirror status <destination volume>
- 2.7. Perform cutover. Once the baseline transfer is completed verify that all source volume snapshots are copied to the new destination. If any discrepancy, perform snapmirror update and confirm all backup snapshots are available on new destination volume.
- 2.7..1. Compare the old & new backup snapshots:
- >ssh <Source filer> vfiler run <Source vfiler> snap list <source volume>
  - >ssh <destination filer> vfiler run <destination vfiler> snap list <destination volume>
- 2.7..2. Once all snapshots are available, do final update and perform cutover.
- >ssh <destination filer> vfiler run <destination vfiler> snapmirror quiesce <destination volume>
  - >ssh <destination filer> vfiler run <destination vfiler> snapmirror break <destination volume>
  - >ssh <destination filer> vfiler run <destination vfiler> snapmirror status <destination volume>
- 2.8. Re-configure snapvault with new destination. Now the snapvault relationship needs to be reestablished with the primary volume and vfiler.
- >ssh <destination filer> vfiler run <destination vfiler> snapvault start -r -S <primary vfiler:primary volume> <destination volume>

While attempting to re-configure, the relation may go for quiescing for some time. Wait till it comes to idle and perform re-configuration.

- 2.9. Once SV is re-configured, configure snapvault snapshots on the new backup volume, update snapvault and confirm that new relation is working.

```
u0159922@c152mad:~> ssh eg-nascorpbkp-f04 vfiler run cis-ss-bkp-f04 snapvault snap sched sv_14_infra_emat558p_s01oral1_snap
===== cis-ss-bkp-f04
xfer   sv_14_infra_emat558p_s01oral1_snap sv_infra_emat558p_s01oral1_snap_s01oradata1 14@sun-sat@2 preserve=default,warn=0
u0159922@c152mad:~>
```

- 2.10. Offline and rename the old backup volume. Now the snapvault source will have two relations, release old backup destination volume relation.
- 2.11. Offline and rename the old backup volume either as part of the post clean up task or raise a new CR. Usually old backup volume will be cleaned up once the relation is monitored for couple of days and cleaned up as all the retention snapshots are available in new destination volume.
- 2.12. Monitor the new relation over next 2 days. Monitor the new snapvault relation and fix if there are any configuration issues or see lag >24hours. Once everything is fixed proceed with the cleaning up the old destination volume and monitor the respective aggregate for the space release.

#### **4.8.6 Aggregate Utilization at 85% on Backup Filers(c-DOT): <Placeholder. TBA>**

#### **4.8.7 Aggregate Utilization at 75% or higher on Dedicated Filers(7-mode/c-DOT): <Placeholder. TBA>**

### **4.9 LIFE CYCLE MANAGEMENT**

The current approved code version for Ontap/DFM/OCUM etc. can be referenced [here](#)

#### **4.9.1 7-mode Ontap Upgrade process**

1. Storage support team should provide the existing SnapMirror(SM) relationship details to LCM. This will enable them to identify the SM destination filers to be upgraded before the source filers.
2. LCM team will schedule downtime with the Business Units and confirm the CR's for upgrade at least 2 week ahead of schedule.
3. Storage Altitude team will create the required CR's.
4. Storage Support team will complete the pre-checks at-least 1 week ahead of scheduled upgrade. The pre-check script gathers all required information prior to the upgrade and should be executed from the jumpboxes as below:  
`/filers/admin/scripts/support/precheck.pl`
5. Complete all checks as outlined in the TO/GB checklist and document the results. Checklist can be found [here](#)
6. The completed checklist should be uploaded to the sharepoint [here](#) and email sent to the storage support team and LCM team notifying completion of pre-checks.
7. Schedule any remediation required prior the upgrade using our standard change process. Notify LCM team about the need to remediate the issue prior to proceeding with the upgrade. If the remediation cannot be performed prior to the upgrade notify LCM team to reschedule the upgrade.
8. The engineer performing the upgrade should review the checklist well ahead of the scheduled time. Do NOT proceed with the upgrade if there are concerns with the pre-checks that could result in an issue and notify your leads right away.
9. Engineer performing the upgrade should ensure the TO/GB scripts are executed for all TO/GB events during the upgrade to avoid the long CP and iscsi bugs. This is only applicable when upgrading from 8.1.3 to 8.2.3p5.
10. For a step by step upgrade process follow the upgrade guide [here](#)
11. Complete the post checks as outlined [here](#).

Note: Please take extra caution while working on x-Markets filers. Examples of xMarkets deviation from SIP Filers are:

- Missing default gateway information for vFilers
- Exports made to IP addresses (as opposed to host names)

## **4.10 TECHNOLOGY REFRESH**

### **Summary:**

NAS assets that are approaching End of Support Life(EOSL), already EOSL, or expiring lease/maintenance are planned for a technology refresh every year to keep the infrastructure current. Storage D&E team is responsible for reviewing such assets and structuring a tech refresh proposal. Upon approval, any infrastructure builds will be handled through standard delivery process.

PMO will request for Storage Support resources to be assigned to kick off the project. Storage support team will be responsible for handling all data migrations and storage activities in scope of the project as per the design guidelines published by Storage D&E.

For detailed documentation covering all tech refresh activities, refer to [7M2CDOT\\_TechRefresh.docx](#)

### **Migration procedures for 7Mode to CDOT on sharepoint:**

For CIFS, refer to [7mode\\_to\\_CDOT\\_Migration\\_for\\_SMB.pdf](#)

For NFS, refer to [7mode\\_to\\_CDOT\\_Migration\\_for\\_NFS.pdf](#)

For NFS LION, refer to [LION\\_7mode\\_to\\_CDOT\\_migration.docx](#)

For Multiprotocol Volumes, refer to [MP Runbook for 7mode to CDOT MTT Migrations.docx](#) and [Multiprotocol 7-mode to c-DOT WI](#)

For ISCSI: At the time of writing this document ISCSI migrations from 7-mode to c-DOT are by exception only. Any migrations should be done from 7-mode to 7-mode filer only due to SMSQL SI for 7.3 still being in progress.

### Runbooks:

Tech refresh migrations should follow standard process outlined in the runbook template. The runbook template was created by the PMO with help from Storage Support. The template steps are generalized to cover migrations for all protocols.

PMO creates and manages the weekly bundle runbooks from the template.

Runbook example: [NetApp\\_RUNBOOK\\_B-1056.xlsx](#)

### Mounts Sheets:

Using the runbook, Storage creates the mounts sheet. The mounts sheet contains the host information for NFS and ISCSI migrations and is used to complete the host re-audits and provide the Platform teams with the new storage information. The Unix team specifically uses the NewPath data to stage their tasks for each bundle event. PMO updates the runbook with the freshly audited host information from the mounts sheet.

Mounts sheet example: [1056mounts.xlsx](#)

### Standard Bundle timebox:

PMO is responsible for defining and scheduling migrations by creating runbooks, communicating with the BUs, and chasing CR approvals. Storage Support is responsible for completing audits, creating CRs, and performing other pre-migration activities. The following steps must be completed in order due to dependencies.

The following timebox assumes the initial audits and owner identifications were previously completed.

| Week1   | Week2  | Week3                              | Week4 - Cutover   |
|---|--|------------------------------------|---|
| PMO creates bundle runbook.   | Storage Support creates prework and cutover CRs based on host audit results.             | Storage support completes prework. | Storage Support works with platform to perform a minor host re-audit.           |
| Storage Support uses runbook to create the mounts sheet and works with platform teams to complete host re-audits. | Once CRs are created, PMO sends BU notification of prework and begins chasing approvals. |                                    | Cutover occurs, source volumes are offlined and renamed to expire in two weeks. |

### Migration timebox template:

PMO team uses a cutover timebox as needed, typically on larger bundles that span numerous BUs. PMO works with each involved team to identify how long pre-cutover, cutover, and post-cutover tasks will take for each team. The timebox is then used by PMO during cutover to ensure migration work stays on track.

Working example before and after:

[NetApp Refresh - Cutover Timeline - B-1052.xlsx](#)

[NetApp Refresh - Cutover Timeline - B-1052 Completed.xlsx](#)

### CR creation process:

Storage Support is responsible for CR creation.

### Prework CRs:

Prework CRs follow the Storage → NAS → Initial Sync categorization and are pre-approved and non-impactful. The prework CRs should be scheduled for up to two weeks long ending at cutover. Prework should be performed up to one week prior to the cutover. Snapmirrors cannot be initiated until PMO sends BU notification.

### Cutover CRs:



Cutover CRs are to be created following a generalized standard template for each CIFS, NFS, CIFS/NFS multiprotocol, or iSCSI volumes. If different protocols are scheduled during the same event, each one needs a separate cutover CR created. These CRs should be created after the host audits are completed, two to three weeks prior to the cutover date. All cutover CRs will be Q3/Q4 requiring a 7-day lead time following the Storage → NAS → Modify categorization.

Tasks should be added by Storage Support for the standard DCO groups involved. For database stop and start tasks, include CTs for ORACLE-SUPPORT (NFS LION), MSSQL-SUPPORT (iSCSI), or DBA-SUPP-NONSTD (NFS MYSQL). For server pre-cutover and post-cutover tasks, include CTs for WINDOWS-SUPPORT-MANAGED (iSCSI), WINDOWS-SUPPORT-CUSTOM (iSCSI), UNIX-SUPPORT-MANAGED (NFS), or UNIX-SUPPORT-CUSTOM (NFS). For storage cutover and post-configuration tasks, include CTs for STORAGE-SUPPORT.

For detailed documentation for CR creation and examples, refer to [7M2CDOT\\_TechRefresh.docx](#)

#### **BU notification process:**

PMO manages communications with the BUs and hosts meetings for each bundle event to discuss pre-cutover and post-cutover steps required by the businesses. Once CRs are in place, PMO will send prework notification and start collecting approvals.

#### **Prework activities:**

7MTT is used to set up the 7Mode to CDOT copy process, following the steps outlined in the migration procedure documents.

Links to the 7MTT tools: [CIS 7MTT](#) : [CPS 7MTT](#)

Cheat sheets are created using a cheat sheet creator, [Cheat Sheet Template V5](#), and then uploaded to the sharepoint.

Current upload location: [2015NR Cheat Sheet folder](#)

Snapmirror tracker sheets (aka SMTracker) are filled out to include snapvault configurations and track how much space is added to volumes during prework for each bundle. They are uploaded to sharepoint and eventually used to track cleanup and reclamation of the backup infrastructure.

Snapmirror Tracker template: [SMTrackerB-10xx-x.xlsx](#)

#### **Project Tracking documentation:**

PMO and Storage Support handle separate tracking documentation. There is some overlap, but they are used for different purposes. The PMO documentation is the primary master document for bundle scheduling and metrics tracking. The Storage documentation is updated based on the PMO bundling and is used for various tracking activities.

Current working examples: [2015NR Storage tracker](#) : [2015NR PMO Master Tracker](#)

Example Storage tracking document: [MigrationTrackerExample.xlsx](#)

#### **One-off 7Mode to CDOT migration Tracking:**

In the case of a one-off 7Mode to CDOT migration not included in a major tech refresh project and therefore no PM guidance, this [all-inclusive tracking sheet](#) can be used.

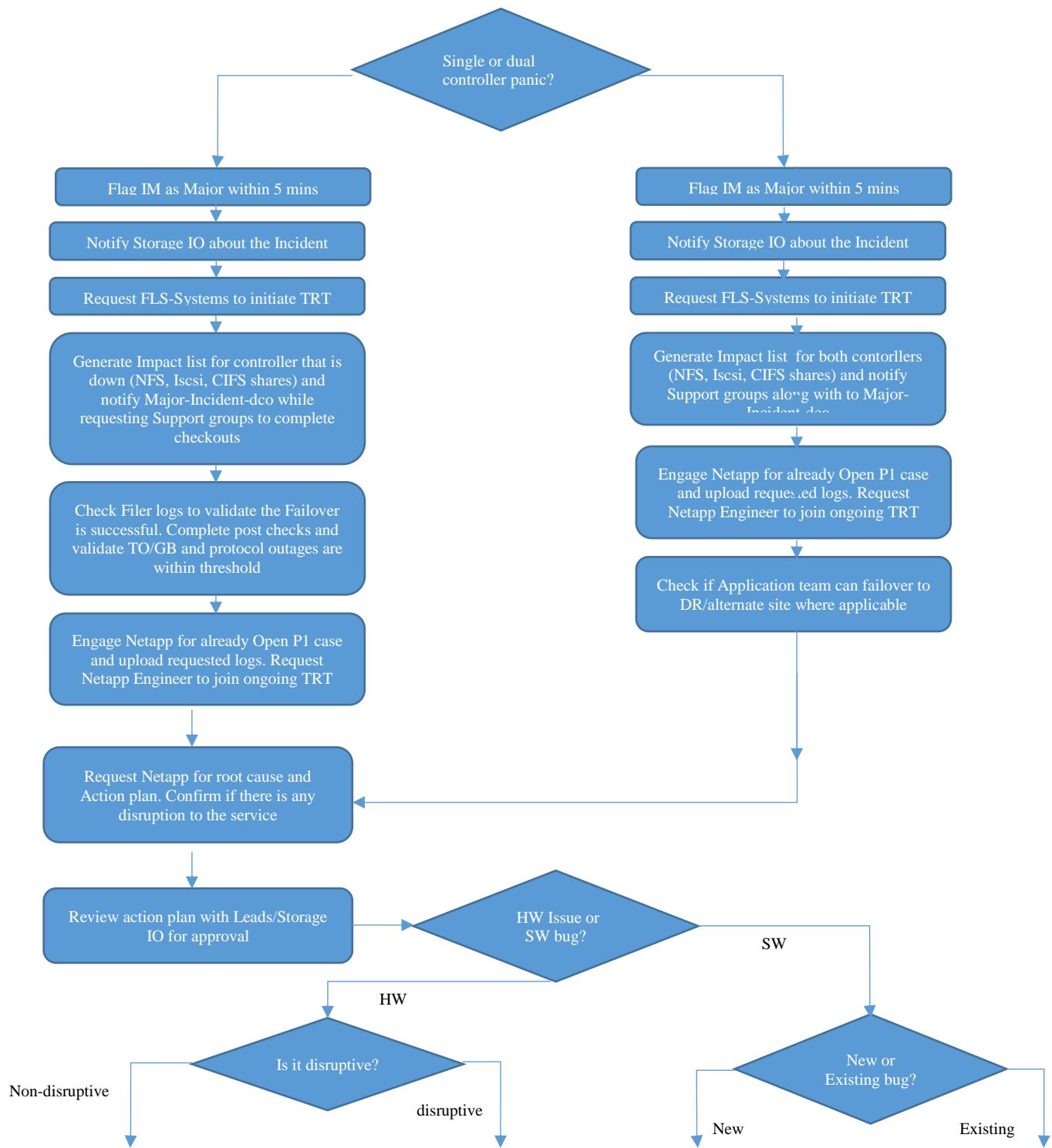
Create a folder within [MiniMigrations](#) to represent the one-off migration and be sure to add a date identifier. Within the newly created folder, upload the associated tracking sheet and any supporting documents, such as cheat sheets.

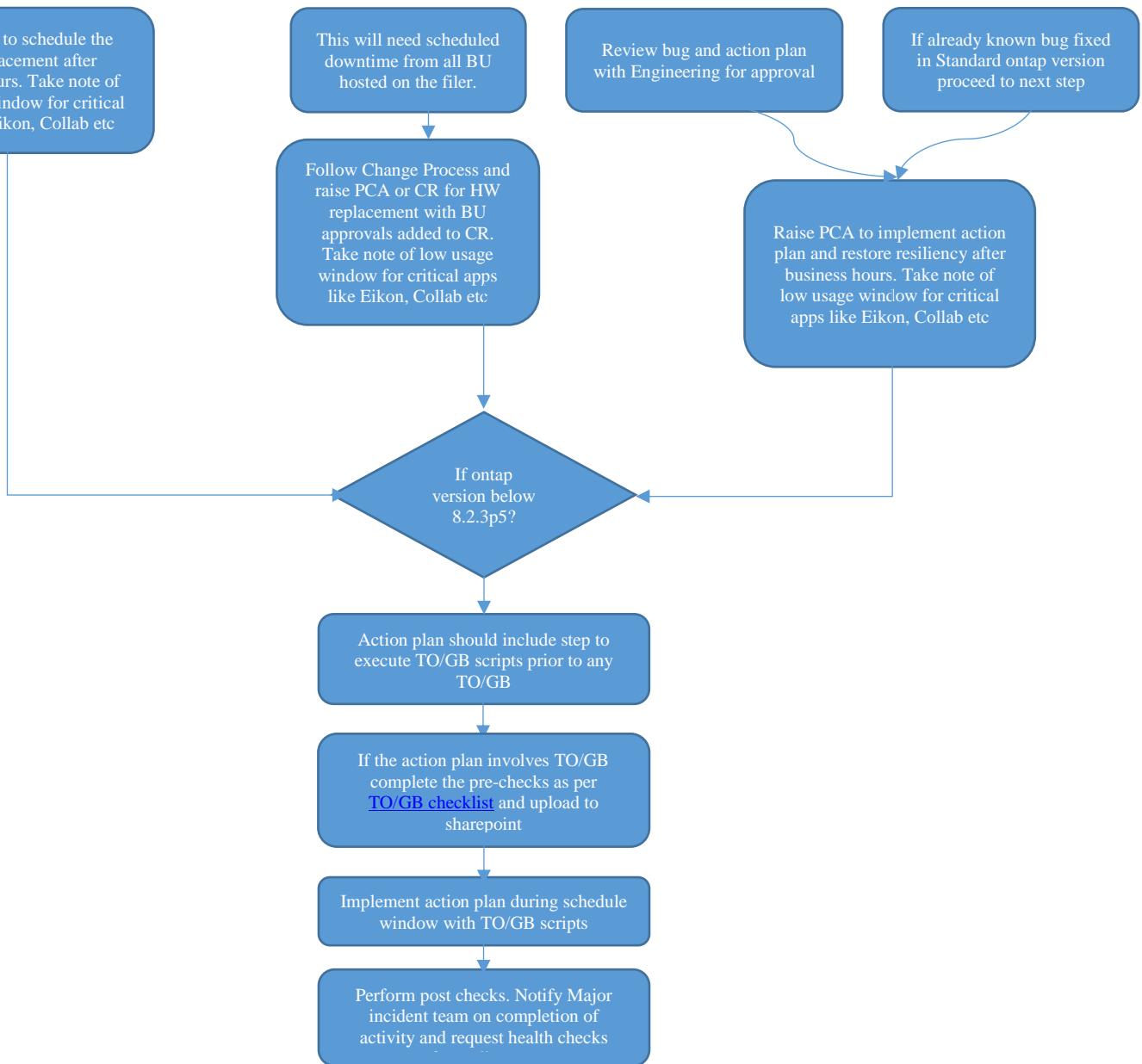
Document version 0.15  
Date of issue : TBD



## 5 TROUBLESHOOTING

### 5.1.1 Single/Dual controller Panic





### 5.1.2 Flexclone Issues

Flexclone is licensed only on our backup controllers and provides DBA team the ability to perform database restores during incidents and testing restore procedures.

There is no involvement of Storage team for the restores but occasionally the DBA team will reach out to storage support when they encounter errors. The document [here](#) covers the restore procedure used by the DBA team.

When a IM is submitted to us check the following:

- Ensure the DBA team are attempting the restore from Backup Filer as the primary filers are not licensed for Flexclone
- If the clones are getting mounted read-only make sure the DBA team are NOT using the latest snapshot. They should be using latest snapshot -1 as outlined in their documentation.

### 5.1.3 How to gather host list when a filer node is down or when exports are deleted?

We will need to gather host list on a filer during incidents (Filer Panic, Exports deletion etc.) and for planned maintenance activities (ontap upgrades, switch migrations etc.)

1. Login to the jumpbox server

```
ssh c152mad.int.thomsonreuters.com
```

2. cd to /filers/admin/scripts/support/
3. Execute the script ./ filerhostlist.py . Script usage shown below

Usage: filerhostlist.py [options]

Options:

-h, --help show this help message and exit

-f FILERNAME, --filer=FILERNAME

Collect host list for a single Filer

-d DATACENTER, --datacenter=DATACENTER

Enter Datacenter location Enter All for all Datacenters

4. A CSV file will be created with the input filer name as seen from the screenshot below.

```
U0156863 - u0156863@c152mad:/filers/admin/scripts/support - ssh  
u0156863@c152mad:/filers/admin/scripts/support> ./filerhostlist.py -f eg-nasapp-b11  
Creating output file eg-nasapp-b11.csv  
Working on Filer: eg-nasapp-b11  
u0156863@c152mad:/filers/admin/scripts/support>
```

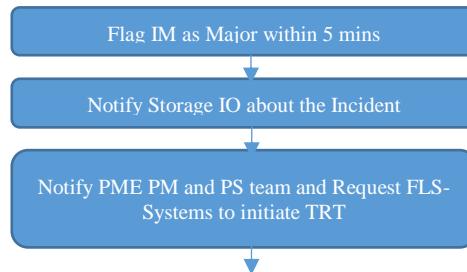
The output includes list of all NFS, iscsi hosts and CIFS shares including the support groups and their email addresses. Any IP addresses are also resolved to DNS names.

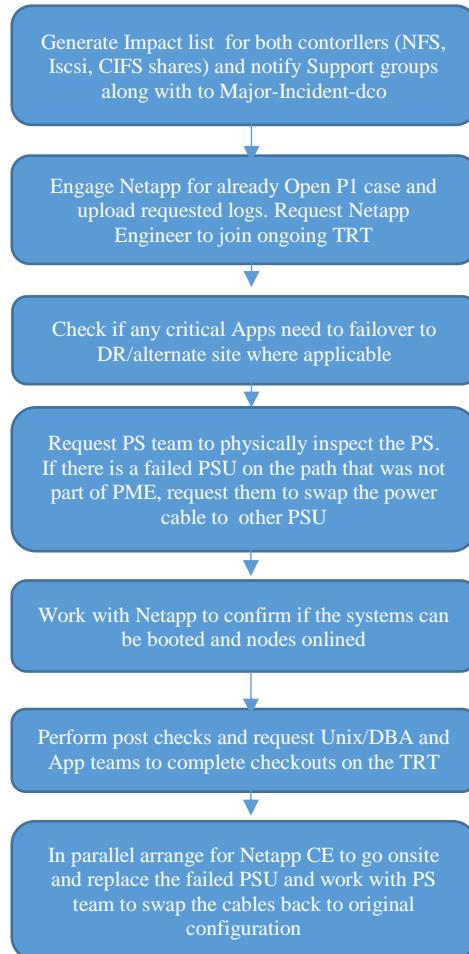
5. Copy the csv file to your desktop.
6. Delete the csv file from the jumpboxes to keep the infrastructure clean.

Note: This data is fetched through MSIL-Storage API. In the event of an accidental removal of any export entries be sure to run this script right away to capture the snapshot of exports prior to the deletion event.

### 5.1.4 Controller Down during PME event

During a PME event one side power will be down for maintenance. Occasionally the redundant PSU may not handle the load and fail resulting in both nodes getting powered down. This will lead to full outage for all applications hosted on the cluster. Follow the below process to handle such events:





### 5.1.5 NFS locks and handling NFS lock issues

Occasionally the team will receive a IM for NFS lock issue from DBA team. The below document explains how NFS locking works and how to handle the NFS lock issues:

CDOT

Break locks for a specific host:

The BU should specify the server which has locks and what storage volume is locked.

Collect the pfiler/cluster, vserver, volume, lif, and host IP address

The volume should be listed in the ticket.

On the jumpbox run “cdlist <vserver>” to list the pfiler/cluster the vserver belongs to.

```
u0144201@c152mad:~> cdlist cisclnt-f0120
dfmc-cis-alrm-f01.int.thomsonreuters.com [eg-cis-clsn-f01] cisclnt-f0120
```

Get the lif by running “ssh <pfiler/cluster> network interface show -vserver <vserver>”.

```
u0144201@c152mad:~> ssh eg-cis-clsn-f01 network interface show -vserver cisclnt-f0120
      Logical      Status      Network          Current      Current Is
Vserver     Interface   Admin/Oper Address/Mask       Node        Port     Home
-----
cisclnt-f0120
    cisclnt-f0120-lif01 up/up 10.205.126.252/22 eg-cis-clsn-f01-102 a0a-3051 true
```

Look up the host IP in Zipper or using “nslookup <hostname>” on the jumpbox.

```
u0144201@c152mad:~> nslookup deldm02
Server:           10.252.36.3
Address:          10.252.36.3#53

Name:  deldm02.int.westgroup.com
Address: 10.205.59.30
```

Using the collected information, list the lock IDs.

```
ssh <pfiler/cluster> vserver locks show -vserver <vserver> -volume <volume> -lif <vserver lif> -client-address <host IP address> -fields lockid
```

Example:

```
ssh eg-cis-clsn-f01 vserver locks show -vserver cisclnt-f0120 -volume
cb0396_ct_riskandfraud_peetoracle_nosnap -lif cisclnt-f0120-lif01 -client-address 10.205.59.30 -fields lockid
u0144201@c152mad:~> ssh eg-cis-clsn-f01 locks show -vserver cisclnt-f0120 -volume cb0396_ct_riskandfraud_peetoracle_nosnap -lif cisclnt-f0120-lif01 -client-addres
ss 10.205.59.30 -fields lockid
vserver      volume          lif          path
-----lockid
-----
cisclnt-f0120 cb0396_ct_riskandfraud_peetoracle_nosnap cisclnt-f0120-lif01 /cb0396_ct_riskandfraud_peetoracle/deldmdbs/oradata/DELDL02/ORCL/co
ntr0file/o1_mf_bwlbv7qj_.ctb7a693f-eb51-4099-bbea-02a2dc16123c
cisclnt-f0120 cb0396_ct_riskandfraud_peetoracle_nosnap cisclnt-f0120-lif01 /cb0396_ct_riskandfraud_peetoracle/deldmdbs/FRA/DELDL02/ORCL/contro
lfile/o1_mf_bwlbv7st_.ctb60e5e7cb-e1b6-439b-b8a4-2b27e611ea96
cisclnt-f0120 cb0396_ct_riskandfraud_peetoracle_nosnap cisclnt-f0120-lif01 /cb0396_ct_riskandfraud_peetoracle_nosnap/peetoracle/deldmdbs/oradata/DELDL02/ORCL/da
tafile/o1_mf_sysaux_bwlbrdkm .dbfa38b0196-1539-4dd4-8ed9-8e07ffc17c4f
cisclnt-f0120 cb0396_ct_riskandfraud_peetoracle_nosnap cisclnt-f0120-lif01 /cb0396_ct_riskandfraud_peetoracle_nosnap/peetoracle/deldmdbs/oradata/DELDL02/ORCL/da
tafile/o1_mf_undotbs1_bwlbrdm3 .dbfdel11ee3-dd91-4517-8fb6-3bc3dcce7b71
cisclnt-f0120 cb0396_ct_riskandfraud_peetoracle_nosnap cisclnt-f0120-lif01 /cb0396_ct_riskandfraud_peetoracle_nosnap/peetoracle/deldmdbs/oradata/DELDL02/ORCL/da
tafile/o1_mf_users_bwlbrt64 .dbf09c9a45c-5ef7-4b5f-ac2b-8541523add50
cisclnt-f0120 cb0396_ct_riskandfraud_peetoracle_nosnap cisclnt-f0120-lif01 /cb0396_ct_riskandfraud_peetoracle_nosnap/peetoracle/deldmdbs/oradata/DELDL02/ORCL/da
tafile/o1_mf_doc_face_d7wr3b38 .dbf84c01e32-a17e-43f1-a791-h38p52641486
```

In the example screenshot above, the vserver, volume, lif, and full path are all listed by default. Specifying the lockid field also includes the lockid. The full path shows which specific files are locked by the host.

To easily collect a list of just the locks, append an awk to the previous command. We are using awk to print the 5th column which is the lock ID.

```
ssh <pfiler/cluster> vserver locks show -vserver <vserver> -volume <volume> -lif <vserver lif> -client-address <host IP address> -fields lockid | awk '{print $5}'
```

Example:

```
ssh eg-cis-clsn-f01 vserver locks show -vserver cisclnt-f0120 -volume
cb0396_ct_riskandfraud_peetoracle_nosnap -lif cisclnt-f0120-lif01 -client-address 10.205.59.30 -fields lockid | awk '{print $5}'
u0144201@c152mad:~> ssh eg-cis-clsn-f01 locks show -vserver cisclnt-f0120 -volume cb0396_ct_riskandfraud_p
eetoracle_nosnap -lif cisclnt-f0120-lif01 -client-address 10.205.59.30 -fields lockid | awk '{print $5}'lockid
-----
b27a693f-eb51-4099-bbea-02a2dc16123c
60e5e7cb-e1b6-439b-b8a4-2b27e611ea96
a38b0196-1539-4dd4-8ed9-8e07ffc17c4f
del11ee3-dd91-4517-8fb6-3bc3dcce7b71
```

Before breaking the locks, confirm with the BU that you have the right information – vfile, volume, and server IP.

To break the locks, first ssh to the filer and enter advanced mode.

```
ssh <pfiler/cluster>
```

```
set -privilege advanced
```

```
u0144201@c152mad:~> ssh eg-cis-clsn-f01
```

```
eg-cis-clsn-f01::> set -privilege advanced
```

```
Warning: These advanced commands are potentially dangerous; use them only when directed to do so by NetApp personnel.  
Do you want to continue? {y|n}: y
```

```
eg-cis-clsn-f01::*>
```

From advanced mode break the locks. Only the lockid needs to be provided. For each lock break it will prompt for confirmation to proceed with the break.

```
vserver locks break -lockid <lockid>
```

Examples:

```
locks break -lockid b27a693f-eb51-4099-bbea-02a2dc16123c
```

```
locks break -lockid 60e5e7cb-e1b6-439b-b8a4-2b27e611ea96
```

```
locks break -lockid a38b0196-1539-4dd4-8ed9-8e07ffc17c4f
```

```
eg-cis-clsn-f01::> vserver locks break -lockid b27a693f-eb51-4099-bbea-02a2dc16123c  
Warning: Breaking file locks can cause applications to become unsynchronized and may lead to data corruption. If you are breaking a file lock on a volume that is being accessed by a FlexCache you must  
take the volume offline on the FlexCache to reestablish proper delegation synchronization between the origin and the cache.  
Do you want to continue? {y|n}: y  
  
eg-cis-clsn-f01::> vserver locks break -lockid 60e5e7cb-e1b6-439b-b8a4-2b27e611ea96  
Warning: Breaking file locks can cause applications to become unsynchronized and may lead to data corruption. If you are breaking a file lock on a volume that is being accessed by a FlexCache you must  
take the volume offline on the FlexCache to reestablish proper delegation synchronization between the origin and the cache.  
Do you want to continue? {y|n}: y  
  
eg-cis-clsn-f01::> vserver locks break -lockid a38b0196-1539-4dd4-8ed9-8e07ffc17c4f  
Warning: Breaking file locks can cause applications to become unsynchronized and may lead to data corruption. If you are breaking a file lock on a volume that is being accessed by a FlexCache you must  
take the volume offline on the FlexCache to reestablish proper delegation synchronization between the origin and the cache.  
Do you want to continue? {y|n}: y  
  
eg-cis-clsn-f01::*
```

### Break locks for a specific location:

If a specific file or folder has been locked, the BU must provide us the vfile and the path that has the issue.

If a file is specified, query against the full path. This will output what servers have the file locked.

```
ssh <pfiler/cluster> vserver locks show -vserver <vserver> -path <full path to file> -fields lockid,client-address
```

Example:

```
ssh eg-cis-clsn-f01 vserver locks show -vserver cisclnt-f0120 -path
```

```
/cb0396_ct_riskandfraud_peetoracle_nosnap/peetoracle/deldmdbs/oradata/DELDL01/ORCL/datafile/o1_mf_cl  
ear_pe_f9c9xqyc_.tmp -fields lockid,client-address
```

```
u0144201@c152mad:~> ssh eg-cis-clsn-f01 vserver locks show -vserver cisclnt-f0120 -path /cb0396_ct_riskandfraud_peetoracle_nosnap/  
peetoracle/deldmdbs/oradata/DELDL01/ORCL/datafile/o1_mf_clear_pe_f9c9xqyc_.tmp -fields lockid,client-address  
vserver          volume           lif      path  
                  lockid            client-address  
-----  
-----  
cisclnt-f0120 cb0396_ct_riskandfraud_peetoracle_nosnap cisclnt-f0120-lif01 /cb0396_ct_riskandfraud_peetoracle_nosnap/peetoracle/de  
dmdbs/oradata/DELDL01/ORCL/datafile/o1_mf_clear_pe_f9c9xqyc_.tmp a6de61dd-6045-4af2-8136-fccf9abae3c0 10.205.59.38
```



If a folder is specified, query against the folder path provided and add a wildcard. This will output what servers have which files locked within that folder or any subfolders therein.

```
ssh <pfiler/cluster> vserver locks show -vserver <vserver> -path <folder path>/* -fields lockid,client-address
```

Example:

In this example we're looking for all locks to files below the oradata path.

```
ssh eg-cis-clsn-f01 vserver locks show -vserver cisclnt-f0120 -path /cb0396_ct_riskandfraud_peetoracle_nosnap/peetoracle/deldmdbs/oradata/* -fields lockid,client-address
u0144201@c152mad:~> ssh eg-cis-clsn-f01 vserver locks show -vserver cisclnt-f0120 -path /cb0396_ct_riskandfraud_peetoracle_nosnap/peetoracle/deldmdbs/oradata/* -fields lockid,client-address
vserver          volume           lif      path
                lockid
-----
```

| vserver       | volume                                   | lif                 | path   | lockid                               | client-address |
|---------------|--|---------------------|--|--------------------------------------|----------------|
| cisclnt-f0120 | cb0396_ct_riskandfraud_peetoracle_nosnap | cisclnt-f0120-lif01 | /cb0396_ct_riskandfraud_peetoracle_nosnap/peetoracle/delmdbs/oradata/DELDMM01/ORCL/controlfile/o1_mf_c4n7nvkp_.ctl       | dab4562-961c-4203-b43b-f5bf5410c3e3  | 10.205.58.24   |
| cisclnt-f0120 | cb0396_ct_riskandfraud_peetoracle_nosnap | cisclnt-f0120-lif01 | /cb0396_ct_riskandfraud_peetoracle_nosnap/peetoracle/delmdbs/oradata/DELDMM06/ORCL/controlfile/o1_mf_bwn49nqo_.ctl       | 1d9a546a-5125-4308-ba2e-797347bcd7ac | 10.205.58.12   |
| cisclnt-f0120 | cb0396_ct_riskandfraud_peetoracle_nosnap | cisclnt-f0120-lif01 | /cb0396_ct_riskandfraud_peetoracle_nosnap/peetoracle/delmdbs/oradata/DELDMM05/ORCL/controlfile/o1_mf_bwn6k6cv_.ctl       | 341d43f6-4d67-430f-aabe-25e7802916a4 | 10.205.59.41   |
| cisclnt-f0120 | cb0396_ct_riskandfraud_peetoracle_nosnap | cisclnt-f0120-lif01 | /cb0396_ct_riskandfraud_peetoracle_nosnap/peetoracle/delmdbs/oradata/DELDMM03/ORCL/controlfile/o1_mf_bwnyn68v_.ctl       | eb166519-f59d-4019-8347-d21e09ef5c30 | 10.205.59.33   |
| cisclnt-f0120 | cb0396_ct_riskandfraud_peetoracle_nosnap | cisclnt-f0120-lif01 | /cb0396_ct_riskandfraud_peetoracle_nosnap/peetoracle/delmdbs/oradata/DELDMM08/ORCL/datafile/o1_mf_undotbs1_bwodn4s9_.dbf | 8d826c6e-ec11-441c-a5a6-cea990d4b3c5 | 10.205.58.18   |
| cisclnt-f0120 | cb0396_ct_riskandfraud_peetoracle_nosnap | cisclnt-f0120-lif01 | /cb0396_ct_riskandfraud_peetoracle_nosnap/peetoracle/delmdbs/oradata/DELDMM08/ORCL/datafile/o1_mf_users_bwodn161_.dbf    | f388994e-7129-45c5-994a-d91d6233fd40 | 10.205.58.18   |
| cisclnt-f0120 | cb0396_ct_riskandfraud_peetoracle_nosnap | cisclnt-f0120-lif01 | /cb0396_ct_riskandfraud_peetoracle_nosnap/peetoracle/delmdbs/oradata/DELDMM08/ORCL/datafile/o1_mf_undotbs1_bwodn4s9_.dbf | f388994e-7129-45c5-994a-d91d6233fd40 | 10.205.58.18   |

Depending on the BU needs we can query as needed to pull the correct lock list.

Before breaking any locks, confirm with the BU that the list of locks targeted is accurate.

## 7MODE

### Break locks for a specific host:

The BU should specify the server which has locks and what storage volume is locked.

Collect the pfiler, vfiler, and hostname.

Using the collected information, list the locks. The “-h” switch specifies looking for all locks for a specific host.

```
ssh <pfiler> vfiler run <vfiler> lock status -h <hostname>
```

Example:

```
ssh eg-naslowcc-f03 vfiler run clnt-corp-f0423 lock status -h ERD03
```

```
u0144201@c152mad:~> ssh eg-naslowcc-f03 vfiler run clnt-corp-f0423 lock status -h ERD03
=====
===== clnt-corp-f0423
===== NLM host ERD03
 17 0x1d18a490:0x000042b8 0:0 1 GRANTED (0xffffffff04e5f2d038)
 17 0x1d18a490:0x000042b7 0:0 1 GRANTED (0xffffffff04f7ff6818)
 17 0x1d18a490:0x00008181 0:0 1 GRANTED (0xffffffff04ea920d58)
 17 0x1d18a490:0x00008182 0:0 1 GRANTED (0xffffffff099de8d578)
 17 0x1d18a490:0x00008bea 0:0 1 GRANTED (0xffffffff04fde732d8)
```

Before breaking the locks, confirm with the BU that you have the right information – vfiler and server name.

Locks are usually broken per host (all locks for all volumes for a host on a given vfiler.) This is because file path is only displayed for certain protocols.

`ssh <pfiler> vfiler run <vfiler> lock break -h <hostname>`

Example:

`ssh eg-naslowcc-f03 vfiler run clnt-corp-f0423 lock break -h ERD03`

## 5.1.6 Stale SnapMirrors

### Summary

Stale SnapMirrors require cleanup in the environment, there could be numerous reasons for a stale snapmirror including

- Migration that did not occur
- Migration postponed and not cleaned up
- Post migration not cleaned up

### Process

Check the snapmirror status on source and destination to see if the relation is shown on both source and destination filers.

If the relation is in broken state with huge lag, then the relation is in a good candidate for cleanup.

- 1) `ssh <>vfiler run <>vfiler> snapmirror status <>vol_name>>`

Depending on which system the relationship is showing (Source/Destination), proceed with the snapmirror cleanup on that particular filer as detailed in the following section.

Consider the following guidelines when performing cleanup:

- Please raise a CR to schedule the changes
- Please ensure that snapshots on both source and destination volumes are released/cleaned-up for all Broken-off Relations.
- For Relations, which are IDLE/Snapmirrored ensure that the Lag is under 150Hrs (Tech Refresh and migrations could have a lead time of 7 days). In case the LAG is more, review the reason for huge LAG and do one of the following.
- Run a manual SnapMirror Update (if the relationship is still valid).
- Break the relation and clean up the SnapMirror snapshots (if the relation is no longer valid).

- Review the Migration Tracker to identify any ongoing migrations related to Tech Refresh, Thin Mitigation, DCR's and take necessary action.
- If snapmirror is not in tracker then
  - Review Email threads
  - Escalate to Storage support for review

### On Destination:

- Run the snapmirror status command on the destination filer.

```
ssh <>pfiler>> vfiler run <>vfiler>> snapmirror status <>vol_name>>
```

*Ex: ssh eg-nasmgmt-e02 vfiler run prod-mgmt-e0042 snapmirror status infra\_hpnacps768p\_n01ora1\_nosnap*

| Source                                     | Destination  | State      | Lag       | Status |
|--|--|------------|-----------|--------|
| prod-ecom-<br>e0503:infra_hpnacps768p_n01o | prod-mgmt-<br>e0042:infra_hpnacps768p_n01ora1_nosna<br>p | Broken-off | 364:55:36 | Idle   |

*Note that when run on destination filer, the snapmirror status command output shows the state as Broken-off*

- Run the snap list command to check the list of snapshots.

```
Ssh <>pfiler>> vfiler run <>vfiler>> snap <>vol_name>>
```

```
ssh eg-nasmgmt-e02 vfiler run prod-mgmt-e0042 snap list infra_hpnacps768p_n01ora1_nosnap
===== prod-mgmt-e0042
Volume infra_hpnacps768p_n01ora1_nosnap
working...
%used %/total date name
-----
0% (0%) 0% (0%) Mar 22 09:39 prod-mgmt-e0042(1928476979)_infra_hpnacps768p_n01ora1_nosnap.601
0% (0%) 0% (0%) Mar 22 01:59 prod-mgmt-e0042(1928476979)_infra_hpnacps768p_n01ora1_nosnap.600
```

NOTE: SnapMirror snapshots can be identified by the name represented with sl.no in brackets.

- Run the snap delete command to delete both the snapmirror snapshots to release the snapmirror relation.

```
ssh <>pfiler>> vfiler run <>vfiler>> snap delete <>vol_name>> '<>snap_name>>'
```

```
ssh eg-nasmgmt-e02 vfiler run prod-mgmt-e0042 snap delete infra_hpnacps768p_n01ora1_nosnap 'prod-mgmt-e0042(1928476979)_infra_hpnacps768p_n01ora1_nosnap.600'
```

```
ssh eg-nasmgmt-e02 vfiler run prod-mgmt-e0042 snap delete infra_hpnacps768p_n01ora1_nosnap 'prod-mgmt-e0042(1928476979)_infra_hpnacps768p_n01ora1_nosnap.601'
```

Note: Always delete the oldest snapshot first (check the Date column of the snap list output).

- Once the snapshots are deleted run the snapmirror status command to validate the relationship.

```
ssh <>pfiler>> vfiler run <>vfiler>> snapmirror status <>vol_name>>
```

```
ssh eg-nasmgmt-e02 vfiler run prod-mgmt-e0042 snapmirror status infra_hpnacps768p_n01ora1_nosnap
```

```
===== prod-mgmt-e0042
```

*Snapmirror is on.*

### Clean-up of Snapmirror.conf file on destination:

1. Once the relationship is cleaned up check if there are any entries in the snapmirror.conf file of the vfiler root volume. If there are any entries in the snapmirror file hash them out to avoid messages logging to the console.
2. Mount the root volume (/etc) of the vfiler on to a temporary mount point and check if snapmirror.conf file has entries specific to the volume.
3. Sudo mount <>vfiler>>:/etc tmp\_mount
4. cd tmp\_mount
5. cat snapmirror.conf

```
prod-ecom-e0503:infra_hpnacps768p_n01ora1_nosnap prod-mgmt-e0042:infra_hpnacps768p_n01ora1_nosnap - * 20,2 * *
```

6. If the file exists and if there entry for the corresponding volume, open the file in VI editor and comment out the entry.
7. vi snapmirror.conf

```
#prod-ecom-e0503:infra_hpnacps768p_n01ora1_nosnap prod-mgmt-e0042:infra_hpnacps768p_n01ora1_nosnap - * 20,2 *  
*
```

8. save and exit vi editor (wq!)
9. unmounts the root volume
10. sudo umount ./tmp\_mount

This completes the snapmirror cleanup on the destination filer.

### On Source:

- Run the snapmirror status command on the Source filer.  
ssh <>pfiler>> vfiler run <>vfiler>> snapmirror status <>vol\_name>>

```
ssh eg-nasecom-e12 vfiler run prod-ecom-e0503 snapmirror status infra_hpnacps768p_n01ora1_nosnap
```

| Source   | Destination                                      | State  | Lag       | Status |
|--|--|--------|-----------|--------|
| prod-ecom-e0503:infra_hpnacps768p_n01ora1_nosnap | prod-mgmt-e0042:infra_hpnacps768p_n01ora1_nosnap | Source | 364:55:36 | Idle   |

*Note that when run on the Source filer, the snapmirror status command output shows the state as **Source***

- Run the snap list command to check the list of snapmirror snapshots.

```
ssh <>pfiler>> vfiler run <>vfiler>> snap <>vol_name>>
```

```
ssh eg-nasecom-e12 vfiler run prod-ecom-e0503 snap list infra_hpnacps768p_n01ora1_nosnap
```

```
===== prod-ecom-e0503  
Volume infra_hpnacps768p_n01ora1_nosnap  
working...
```

```
%/used %/total date name
```

```
-----  
0% ( 0%) 0% ( 0%) Mar 22 09:39 prod-mgmt-e0042(1928476979)_infra_hpnacps768p_n01ora1_nosnap.601 (snapmirror)
```

- To clean up the snapmirror relation on the source filer run the following command:

```
ssh <>pfiler>> vfile run <>vfile>> snapmirror release <>vol_name>> <>dest:vol_name>>
```

```
ssh eg-nasecom-e12 vfile run prod-ecom-e0503 snapmirror release infra_hpnacps768p_n01ora1_nosnap prod-mgmt-e0042:infra_hpnacps768p_n01ora1_nosnap
```

- Run the snapmirror status command to see if the relation is cleaned up.

```
ssh <>pfiler>> vfile run <>vfile>> snapmirror status <>vol_name>>
```

```
ssh eg-nasecom-e12 vfile run prod-ecom-e0503 snapmirror status infra_hpnacps768p_n01ora1_nosnap
```

```
===== prod-ecom-e0503  
Snapmirror is on.
```

- You may notice that the snapmirror snapshot is deleted as well.

```
ssh <>pfiler>> vfile run <>vfile>> snap list <>vol_name>>
```

```
ssh eg-nasecom-e12 vfile run prod-ecom-e0503 snap list infra_hpnacps768p_n01ora1_nosnap
```

```
===== prod-ecom-e0503  
Volume infra_hpnacps768p_n01ora1_nosnap  
working...  
No snapshots exist.
```

### 5.1.7 Performance Troubleshooting

<Placeholder for main performance troubleshooting document . To be added in next version>

#### REALLOCATION:

If the volume has been around a long time, chances are it has had a lot of data read and written. Over the period especially if the space has fluctuated, data may not be laid out in the best manner.

So, Reallocate optimizes the layout of data on disk for “Sequential Read Access”.

#### When to run?

First, we measure the current layout which will present us with an optimization score between 1 to 10. Let say we set a threshold (4 by default), and if the optimization score is above the threshold you run the reallocation process.

#### When do we run in our TR environment?

We open cases for performance issues and depending what NetApp says such as if they see a lot of disk fragmentation they may request to do some reallocate to defragment it

#### Check if the volume is eligible for reallocation:

```
ssh <pfiler> reallocate measure -o /vol/cb0780_infra_virtual_cce0921_vol01_snap07.
```

```
m6042366@c152mad:~> ssh eg-nasclnt-e15 reallocate measure -o /vol/cb0780_infra_virtual_cce0924_vol04_snap07
Reallocation scan will be started on '/vol/cb0780_infra_virtual_cce0924_vol04_snap07'.
Monitor the system log for results.
m6042366@c152mad:~> ssh eg-nasclnt-e15 reallocate status
Reallocation scans are on
/vol/cb0780_infra_virtual_cce0924_vol04_snap07:
  State: Checking: public inode 106 of 32781, block 211395 of 3932159
  Schedule: n/a
  Interval: n/a
  Optimization: n/a
  Measure Log: n/a
```

In /etc/messages system recommends for running reallocate. Only then, we need to run reallocate on that volume:

*Tue Jun 27 14:30:01 CDT [eg-nasclnt-e15:wafl.reallocate.check.highAdvise: info]: Allocation check on '/vol/cb0780\_infra\_virtual\_cce0924\_vol04\_snap07' is 6, hotspot 0 (threshold 4), consider running reallocate.*

## Reallocation Process:

To manage reallocation scans, we must enable reallocation scans on our filer. The reallocation should be run on non-business hours.

We raise a normal change with two days lead time. Though it is a back-end process and no impact

We add the BU as the approver and we will notify them through the mail and intimate them that there will be no impact. We need to let them aware of the work which is going to be done

And also, not necessary we run reallocation on virtual volumes we can run on any of the volume as per NetApp suggestion

1. Check the status:

```
ssh <pfiler> reallocate status /vol/volname
```

```
u0159922 @c152mad:~> ssh eg-nasclnt-e15 reallocate status
Reallocation scans are on
No reallocation status.
u0159922 @c152mad:~>
```

```
ssh <pfiler> reallocate on | off
```

When jobs are off no new reallocation jobs may be started, or restarted.

2. Steps to take care before reallocation:

- a) The volume to be reallocated must be writable (no SnapMirror destinations)
- b) The volume or volume containing an object undergoing reallocation must be at least 5% free take the output of the utilization of the volume.

```
ssh <pfiler> df -g /vol/volname
```

```
ssh <pfiler> vol size volname +500g
```

- c) Add space to the volume to increase the snap reserve to handle the large snapshot . Existing Snapshot copies must leave at least 10% of the Snapshot reserve or 5% of the volume size free, whichever is less. This requirement does not apply to physical reallocation. The reallocation will stop if it runs out of space.

- d) Make sure the source snapshots are vaulted at the destination. As a process of reallocation snapshots get deleted to free up space

```
ssh <pfiler> vfiler run <vfilername> snap list sourcevolname  
ssh <pfiler> vfiler run <vfilername> snapvault status -l /vol/volname  
ssh <bkppfiler> vfiler run <bkpvfilername> snap list bkpvolname  
ssh <bkppfiler> vfiler run <bkpvfilername> snapvault status -l /vol/bkpvolname
```

*Example:*

*Sun Jun 25 23:00:58 CDT [eg-nasecom-f04:wafl.volume.snap.autoDelete: info]: Deleting snapshot 'sv\_infra\_virtual\_pef0269\_snap14.5' in volume 'infra\_virtual\_pef0269\_snap14' to recover storage*

*Mon Jun 26 23:40:49 CDT [eg-nasecom-f04:wafl.scan.start: info]: Starting file reallocating on volume infra\_virtual\_pef0269\_snap14.*

*Tue Jun 27 00:18:09 CDT [eg-nasecom-f04:wafl.volume.snap.autoDelete: info]: Deleting snapshot 'sv\_infra\_virtual\_pef0269\_snap14.5' in volume 'infra\_virtual\_pef0269\_snap14' to recover storage*

*Tue Jun 27 01:49:59 CDT [eg-nasecom-f04:wafl.volume.snap.autoDelete: info]: Deleting snapshot 'sv\_infra\_virtual\_pef0269\_snap14.4' in volume 'infra\_virtual\_pef0269\_snap14' to recover storage*

*Tue Jun 27 04:56:40 CDT [eg-nasecom-f04:wafl.volume.snap.autoDelete: info]: Deleting snapshot 'sv\_infra\_virtual\_pef0269\_snap14.3' in volume 'infra\_virtual\_pef0269\_snap14' to recover storage*

*Tue Jun 27 04:57:22 CDT [eg-nasecom-f04:wafl.volume.snap.autoDelete: info]: Deleting snapshot 'sv\_infra\_virtual\_pef0269\_snap14.2' in volume 'infra\_virtual\_pef0269\_snap14' to recover storage*

### 3. Performing Reallocation:

```
ssh <pfiler> reallocate start -o -n /vol/volname  
-o performs the scan only once.  
-n performs the scan without checking the layout of the LUN, file, or volume.
```

This option ignores any thresholds and simply begins data reallocation.

Please find the example below:

```
m6042366@c152mad:~> ssh eg-nasecom-f04 reallocate start -o -n /vol/infra_virtual_pef0269_snap14
```

Reallocation scan will be started on '/vol/infra\_virtual\_pef0269\_snap14'.

Monitor the system log for results.

### 4. To check the status of the reallocation:

```
ssh <pfiler> reallocate status /vol/volname
```

*Example:*

```
ssh eg-nasecom-f04 reallocate status
```

*Reallocation scans are on*

/vol/infra\_virtual\_pef0269\_snap14:

*State: Reallocating: public inode 19549 of 32781, block 731776 of 1183750 (61%)*

*Schedule: N/A*

*Interval: N/A*

*Optimization: N/A*

## 5. Post Checks:

The only way to check if the reallocation is completed is or not is to measure the layout

Once the reallocation is complete we need to initiate a perfstat and upload to netapp for reevaluation. It is always advisable to notify the BU once this completes (Reason: BU will be aware that the issue is fixed)

After the reallocation is complete output will be as below:

u0159922@c152mad :~> ssh eg-nasecom-f04 reallocate status

Reallocation scans are on

No reallocation status.

We need to measure the layout again and then check the /etc/messages like above (start of the document) and reclaim the added space.

For example run the command on the volume as shown below:

ssh eg-nasecom-f04 reallocate measure -o /vol/fl\_findlawprght odapps\_snap

Review the messages file:

ssh eg-nasecom-f04 rdfile /etc/messages | grep -i fl\_findlawprght odapps\_snap

Output will show as follows:

messages.0:Fri Jul 14 20:14:04 CDT [eg-nasecom-f04:wafl.reallocate.check.value:info]: Allocation measurement check on '/vol/fl\_findlawprodapps\_snap' is 2.

## 6. Steps to reclaim the space added.

ssh <pfiler> df -g /vol/volname

ssh <pfiler> vol size volname -500g

ssh <pfiler> df -g /vol/volname

## 7. To stop the reallocation: The stop command will remove any reallocation job information for pathname

ssh <pfiler> reallocate stop /vol/volname

### 5.1.8 CIFS Management

#### Security Style

7MODE:

The root volume is always created as unix security-style.

CIFS-only data volumes are created as ntfs with ntfs qtrees.

Multiprotocol (CIFS/NFS) data volumes are created as unix with unix qtrees.

Non-standard, unix volume with ntfs qtree is considered CIFS-only qtree.

CDOT:

All volumes in a CIFS-only vserver are created as ntfs with ntfs qtrees, root included. Setting the root volume to ntfs is a new standard and new vservers will be created this way while pre-existing vservers will have a unix root volume.

Multiprotocol (CIFS/NFS) data volumes are created as unix with unix qtrees.

Example CIFS-only setup on 7mode

```
u0144201@c152mad:~> ssh ln-naslowep-d01 vfiler run prod-ecom-d0075 qtree status
===== prod-ecom-d0075
Volume   Tree      Style Optricks  Status
----- -----
cb0551_rsadtcpd_snap           ntfs  enabled  normal
cb0551_rsadtcpd_snap rsa       ntfs  enabled  normal
prod_ecom_d0075_root           unix  enabled  normal
cb0103_precedentsauspd_snap    ntfs  enabled  normal
cb0103_precedentsauspd_snap precedents ntfs  enabled  normal
```

Example Multiprotocol setup on CDOT

```
u0144201@c152mad:~> ssh eg-naslowcc-e01 vfiler run clnt-corp-e0579 qtree status cb0057_filehistorydeve_nosnap
===== clnt-corp-e0579
Volume   Tree      Style Optricks  Status
----- -----
cb0057_filehistorydeve_nosnap   unix  enabled  normal
cb0057_filehistorydeve_nosnap orders   unix  enabled  normal
```

Example CIFS-only setup on CDOT

```
u0144201@c152mad:~> ssh pl-cis-clsp-p01 qtree show -vserver cisclnt-p0058
Vserver   Volume     Qtree      Style      Optricks  Status
----- -----
cisclnt-p0058 cb0838_ggo_legalonedataaccp_snap "" ntfs enable normal
cisclnt-p0058 cb0838_ggo_legalonedataaccp_snap legalmigration ntfs enable normal
cisclnt-p0058 cb0838_ggo_legalonedatadbaccp_snap "" ntfs enable normal
cisclnt-p0058 cb0838_ggo_legalonedatadbaccp_snap legalmigration ntfs enable normal
cisclnt-p0058 cisclnt_p0058_root ""      ntfs      enable      normal
5 entries were displayed.
```

## Initial CIFS setup

Running “cifs setup” on a 7Mode vfile or running “cifs create” on a CDOT vserver will create and start the CIFS server on that vfile or vserver tied to the provided Active Directory domain. This can take place before or after the volumes are created.

Example domain for 7Mode CIFS server

```
u0144201@c152mad:~> ssh ln-naslowep-d01 vfile run prod-ecom-d0075 cifs domaininfo
===== prod-ecom-d0075
NetBIOS Domain: ECOM
Windows Domain Name: ecom.tlrg.com
Domain Controller Functionality: Windows 2008 R2
Domain Functionality: Windows 2003
Forest Functionality: Windows 2003
Filer AD Site: lon
```

Example domain for CDOT CIFS server

```
u0144201@c152mad:~> ssh pl-cis-clsp-p01 cifs show -vserver cisclnt-p0058
                                         Vserver: cisclnt-p0058
                                         CIFS Server NetBIOS Name: CISCLNT-P0058
                                         NetBIOS Domain/Workgroup Name: ECOMQC
                                         Fully Qualified Domain Name: ECOMQC.TLRG.COM
Default Site Used by LIFs Without Site Membership:
                                         Authentication Style: domain
                                         CIFS Server Administrative Status: up
```

When the CIFS server is created, a few default shares are created off the root volume. In 7Mode, the default shares are ETC\$, HOME, and C\$. Per new standard, the HOME share should be deleted. In CDOT, the shares are admin\$, c\$, and ipc\$.

We do not use the default shares. This KB lists what the CDOT default shares could be used for.

<https://library.netapp.com/ecmdocs/ECMP1610207/html/GUID-5B56B12D-219C-4E23-B3F8-1CB1C4F619CE.html>

Example default shares on 7Mode

```
===== prod-ecom-d0075
Name      Mount Point          Description
-----  -----
ETC$      /vol/prod_ecom_d0075_root/etc    Remote Administration
                  BUILTIN\Administrators / Full Control
HOME      /vol/prod_ecom_d0075_root/home   Default Share
                  everyone / Full Control
C$        /                      Remote Administration
                  BUILTIN\Administrators / Full Control
```

Example default shares on CDOT

| Vserver       | Share   | Path | Properties                           | Comment                               | ACL |
|---------------|---------|------|--------------------------------------|---------------------------------------|-----|
| cisclnt-p0058 | admin\$ | /    | browsable                            | -                                     | -   |
| cisclnt-p0058 | c\$     | /    | oplocks<br>browsable<br>changenotify | BUILTIN\Administrators / Full Control |     |
| cisclnt-p0058 | ipc\$   | /    | browsable                            | -                                     | -   |

## Volume-level shares

Storage team creates a volume-level share for each CIFS volume. This allows the CIFS support team to create and manage the data shares and permissions. The share-name is <volume>\$ and points to the volume path, /vol/<volume> on 7Mode or /<volume> on CDOT.

Example volume-level shares on 7Mode

```
u0144201@c152mad:~> ssh ln-naslowep-d01 vfile run prod-ecom-d0075 cifs shares cb0551_rsadtcprod_snap$  
===== prod-ecom-d0075  
Name      Mount Point          Description  
----      -----  
cb0551_rsadtcprod_snap$ /vol/cb0551_rsadtcprod_snap  
          BUILTIN\Administrators / Full Control  
u0144201@c152mad:~> ssh ln-naslowep-d01 vfile run prod-ecom-d0075 cifs shares cb0103_precedentsauspd_snap$  
===== prod-ecom-d0075  
Name      Mount Point          Description  
----      -----  
cb0103_precedentsauspd_snap$ /vol/cb0103_precedentsauspd_snap  
          BUILTIN\Administrators / Full Control
```

Example volume-level shares on CDOT

```
u0144201@c152mad:~> ssh pl-cis-clsp-p01 cifs share show -vserver cisclnt-p0058 -share-name cb0838_ggo_legalon  
nedataccp_snap$,cb0838_ggo_legalonedatdaccp_snap$  
Vserver   Share     Path          Properties Comment  ACL  
-----  
cisclnt-p0058 cb0838_ggo_ /cb0838_ggo_    oplocks  -      BUILTIN\Administrators / Full Control  
            legalonedatc legalonedatdaccp_ browsable  
            cp_snap$    snap          changeNotify  
cisclnt-p0058 cb0838_ggo_ /cb0838_ggo_    oplocks  -      BUILTIN\Administrators / Full Control  
            legalonedatd legalonedatdaccp_ browsable  
            baccp_snap$  p_snap        changeNotify  
2 entries were displayed.
```

## Data Shares

If new storage is required for a new share, at minimum storage creates a new qtree with quotas on pre-existing storage, while at maximum storage creates a new vserver, cifs server, volume, volume-level share, and qtree with quotas.

Example data shares

The volume-level shares are named after the volume and point to the volume path.

The data shares are named after the qtree+subfolder and point to the volume\qtree\subfolder path.

```
Default cifs server shares  
  Default volume-level shares  
u0144201@c152mad:~> ssh pl-cis-clsp-p01 cifs share show -vserver cisclnt-p0058 -fields share-name,path  
vserver   share-name path  
-----  
cisclnt-p0058 admin$  /  
cisclnt-p0058 cs$    /  
cisclnt-p0058 cb0838_ggo_legalonedatccp_snap$ /cb0838_ggo_legalonedatccp_snap  
cisclnt-p0058 cb0838_ggo_legalonedatdaccp_snap$ /cb0838_ggo_legalonedatdaccp_snap  
cisclnt-p0058 ipc$   /  
cisclnt-p0058 legalmigrationDBqa$ /cb0838_ggo_legalonedatccp_snap/legalmigration/DBqa  
cisclnt-p0058 legalmigrationftpqa$ /cb0838_ggo_legalonedatccp_snap/legalmigration/ftpqa  
7 entries were displayed.  
  
Data shares created by Windows
```



The multiprotocol shares are named after the qtree and point to the volume\qtree path.

```

u0144201@cl52mad:~> ssh eg-nascorp-e09 vfile run prod-corp-e0498 cifs shares | grep /vol/
ETC$      /vol/prod_corp_e0498_root/etc      Remote Administration
HOME      /vol/prod_corp_e0498_root/home      Default Share
cb0179 trl ccrprode snap$ /vol/cb0179 trl ccrprode snap
psccr$   /vol/cb0179_trl_ccrprode_snap/psccr Share created by Praveen Kumar H.N(M179423) on 6/3/2015 6:43 AM for BCS32843-04
psregs$  /vol/cb0179_trl_ccrprode_snap/psregs Share created by GOKUL SARAVANAN(m179426) on 6/16/2015 12:54 PM for BCS32843-05
slips$   /vol/cb0179_trl_ccrprode_snap/slips Share created by RAMAKRISHNA K(M180853) on 6/4/2015 7:41 AM for BCS32843-03
ccrdb$   /vol/cb0179_trl_ccrprode_snap/ccrdb Share created by MADHURI MUDGAL(m180854) on 6/4/2015 12:22 AM for BCS32843-01
ccrwip$  /vol/cb0179_trl_ccrprode_snap/ccrwip Share created by Praveen Kumar H.N(M179423) on 6/10/2015 10:47 AM for BCS32843-02

```

## CIFS Access

There are three levels of CIFS access which cross both Storage and Windows standards.

### Domains and trusts

The CIFS server is created in an Active Directory domain, TEN, MGMT, ECOM, ECOMQC, TLR, TLRQA, LHTRP, CLRRS, ERF, TFPROWD, and TFCORP to name a few.

Most domains are trusted to the primary domains MGMT and TEN. Due to this trust, for any CIFS servers created in a domain trusted to MGMT (MGMT, ECOM, ECOMQC, LHTRP, CLRRS, TFPROWD) should use MGMT groups and any CIFS servers created in a domain trusted to TEN (TEN, TLR, TLRQA, ERF, TFCORP) should use TEN groups.

### AD Group Definition

| Group or Account                             | Definition  |
|--|---|
| BUILTIN\Administrators                       | Default local group on the vserver  |
| Everyone                                     | Open access to all, insecure  |
| NT AUTHORITY\Authenticated Users             | Group covering all valid domain accounts, more secure than Everyone                     |
| <domain>\<vserver>.<sharename>.m             | CIFS-only structure 1 <b>MODIFY</b> group*  |
| <domain>\<vserver>.<sharename>.r             | CIFS-only structure 1 <b>READONLY</b> group*  |
| <domain>\<vserver>.<sharename>.<subfolder>.m | CIFS-only structure 2 <b>MODIFY</b> group*  |
| <domain>\<vserver>.<sharename>.<subfolder>.r | CIFS-only structure 2 <b>READONLY</b> group*  |
| <domain>\<vserver>.<sharename>.c             | Multiprotocol <b>CHANGE</b> group*  |
| <domain>\<vserver>.<sharename>.f             | BU is granted FULL CONTROL access*  |
| MGMT\M-EaganServerAdmins                     | Windows AD group for MGMT trust domains   |
| TEN\M-EaganServerAdmins                      | Windows AD group for TEN trust domains  |
| MGMT\REST-STORAGE-SUPPORT-ServerAdmins       | Storage AD group for MGMT trust domains   |
| TEN\DG-APP-REST-STORAGE-SUPPORT-ServerAdmins | Storage AD group for TEN trust domains  |
| <domain>\M-Storage-Admins.G                  | Old storage AD group for various domains, should be replaced with appropriate new group |

\*TEN domain follows its own set of unique naming standards. TEN domain groups will be prefixed with “-DL-FIL” and end in “modify”, “read”, “change”, or “full” instead of just m, r, c, or f.

Example TEN groups on a Structure 2.

- DL-FIL-clnt-corp-e0848.odenfileeagan.Users.modify (TEN\DL-FIL-clnt-corp-e0...
- DL-FIL-clnt-corp-e0848.odenfileeagan.Users.read (TEN\DL-FIL-clnt-corp-e084...

### 1. LAG: Local Administrators Group

When the CIFS server is created, a default local group is created called BUILTIN\Administrators, commonly referred to as the LAG. The team which will be supporting the CIFS share creation and permissions needs to be added to the LAG. In most cases this is Windows-Support, but Remote Office teams manage some shares in the infrastructure.

Storage-Support is not required in the LAG since we do not manage CIFS creation and permissions, but we can grant ourselves this access to view the shares to assist in troubleshooting issues – Look, but do not touch!

BU groups or accounts should NEVER be added to LAG.

For Windows-Support, the MGMT\{EaganServerAdmins group should be used for all MGMT domains and trusts while the TEN\{EaganServerAdmins group should be used for all TEN domains and trusts.

For Storage-Support, the MGMT\REST-STORAGE-SUPPORT-ServerAdmins should be used for all MGMT domains and trusts while the TEN\DG-APP-REST-STORAGE-SUPPORT-ServerAdmins group should be used for all TEN domains and trusts.

Remote office groups are dependent on the build. (Examples TBD)

To view the LAG in 7Mode, first list the members of the local Administrators group. This will output a list of SIDS which will then need to be resolved into their human-readable names using cifs lookup. Viewing the LAG in CDOT will already list the human-readable names.

Example in 7Mode, first list the SIDS

```
u0144201@c152mad:~> ssh ln-naslowep-d01 vfile run prod-ecom-d0075 useradmin domainuser list -g Administrators
===== prod-ecom-d0075
List of SIDS in Administrators
S-1-5-21-1042301482-1521892575-1389358599-131073
S-1-5-21-1042301482-1521892575-1389358599-500
S-1-5-21-1149247497-1642356119-618142746-512
S-1-5-21-3556246720-3107459709-3646524347-3349
S-1-5-21-3556246720-3107459709-3646524347-16102
S-1-5-21-3556246720-3107459709-3646524347-40602
For more information about a user, use the 'cifs lookup' and 'useradmin user list' commands.
```

Example in 7Mode, second perform cifs lookup

```
u0144201@c152mad:~> ssh ln-naslowep-d01 vfile run prod-ecom-d0075 cifs lookup S-1-5-21-1042301482-1521892575-1389358599-131073
===== prod-ecom-d0075
name = PROD-ECOM-D0075\root
u0144201@c152mad:~> ssh ln-naslowep-d01 vfile run prod-ecom-d0075 cifs lookup S-1-5-21-1042301482-1521892575-1389358599-500
===== prod-ecom-d0075
name = PROD-ECOM-D0075\administrator
u0144201@c152mad:~> ssh ln-naslowep-d01 vfile run prod-ecom-d0075 cifs lookup S-1-5-21-1149247497-1642356119-618142746-512
===== prod-ecom-d0075
name = ECOM\Domain Admins
u0144201@c152mad:~> ssh ln-naslowep-d01 vfile run prod-ecom-d0075 cifs lookup S-1-5-21-3556246720-3107459709-3646524347-3349
===== prod-ecom-d0075
name = MGMT\{EaganServerAdmins
u0144201@c152mad:~> ssh ln-naslowep-d01 vfile run prod-ecom-d0075 cifs lookup S-1-5-21-3556246720-3107459709-3646524347-16102
===== prod-ecom-d0075
name = MGMT\svcAvNas
u0144201@c152mad:~> ssh ln-naslowep-d01 vfile run prod-ecom-d0075 cifs lookup S-1-5-21-3556246720-3107459709-3646524347-40602
===== prod-ecom-d0075
name = MGMT\REST-STORAGE-SUPPORT-ServerAdmins
```

#### Example in CDOT

```
u0144201@c152mad:~> ssh eg-cis-clsn-e01 cifs users-and-groups local-group show-members -vserver cisclnt-e0153
Vserver      Group Name          Members
-----
cisclnt-e0153  BUILTIN\Administrators    CISCLNT-E0153\Administrator
                           TLR\Domain Admins
                           TEN\m-eaganserveradmins
                           TLR\Domain Users
BUILTIN\Users
4 entries were displayed.
```

## 2. Share-level Access / Share Permissions

The share-level access is the permissions depicted in the “cifs shares” 7Mode or “cifs share show” CDOT output. In CDOT, this is referred to as the ACL access control list.

The Volume-level shares should only list “BUILTIN\Administrators” with Full Control access. The “Everyone” group should always be removed and replaced with the LAG. This is done by Storage because it is the volume-level share.

CIFS-only data shares should only list “BUILTIN\Administrators” with Full Control access and “NT AUTHORITY\Authenticated Users” with Change access. “Everyone” group should always be removed.

Multiprotocol CIFS/NFS data shares have unix permissions set open to 777. The share-level permissions are then locked down with “BUILTIN\Administrators” with Full Control access and a CHANGE group (<domain>\<vserver>.<sharename>.c) with Change access. Any BU groups or users requiring access are added to the CHANGE group.

The CIFS support team has access to modify the share-level permissions which is why Storage does not modify these permissions on data shares. Other than the permissions listed in the above descriptions, no other groups should be added. Remember, CIFS support team is in the LAG, so the LAG needs to be added to the share-level permissions and NOT the CIFS support team directly.

#### Example of CIFS-only data share on 7Mode, as seen by Storage

```
u0144201@c152mad:~> ssh ln-naslowep-d01 vfiler run prod-ecom-d0075 cifs shares rsadata$ 
===== prod-ecom-d0075
Name      Mount Point          Description
-----
rsadata$   /vol/cb0551_rsadtcpd_snap/rsa/data Share created by rama krishna(M180853) on 8/5/2015 4:46 PM for BCS31631-04
           NT AUTHORITY\Authenticated Users / Change
           BUILTIN\Administrators / Full Control
```

#### Example of CIFS-only data share on 7Mode, as seen by Windows

Computer Management

File Action View Help

Computer Management (PROD)

- System Tools
  - Task Scheduler
  - Event Viewer
  - Shared Folders
    - Shares
    - Sessions
    - Open Files
  - Local Users and Groups
  - Performance
  - Device Manager
- Storage
- Services and Applications

| Share Name                   | Folder Path          | Type    | # Client Connections | Description  |
|------------------------------|----------------------|---------|----------------------|--------------|
| C\$                          | C:\                  | Windows | 0                    | Remote A...  |
| cb0103_precedentsauspd_sn... | C:\vol\cb0103_pre... | Windows | 0                    |              |
| cb0551_rsadtcpd_snap\$       | C:\vol\cb0551_rsa... | Windows | 0                    |              |
| ETCS                         | C:\vol\prod_ecom...  | Windows | 0                    |              |
| HOME                         | C:\vol\prod_ecom...  | Windows | 0                    | Default S... |
| IPCS                         |                      | Windows | 20                   | Remote I...  |
| precedentsdata\$             | C:\vol\cb0103_pre... | Windows | 0                    | Share cre... |
| rsadata\$                    | C:\vol\cb0551_rsa... | Windows | 113                  | Share cre... |

rsadata\$ Properties

General Share Permissions Security

Group or user names:

- Authenticated Users
- Administrators (PROD-ECOM-D0075\Administrators)

Add... Remove

| Permissions for Authenticated Users | Allow                               | Deny                     |
|-------------------------------------|-------------------------------------|--------------------------|
| Full Control                        | <input type="checkbox"/>            | <input type="checkbox"/> |
| Change                              | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Read                                | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

#### Example of Multiprotocol data share on 7Mode, as seen by Storage

```
u0144201@c152mad:~> ssh eg-nascorp-e09 vfile run prod-corp-e0498 cifs shares
===== prod-corp-e0498
Name      Mount Point          Description
---      -----
ETCS     /vol/prod_corp_e0498_root/etc    Remote Administration
        BUILTIN\Administrators / Full Control
HOME     /vol/prod_corp_e0498_root/home   Default Share
        everyone / Full Control
C$       /                         Remote Administration
        BUILTIN\Administrators / Full Control
psccr$   /vol/cb0179_trl_ccrprode_snap/psccr Share created by Praveen Kumar H.N(M179423) on 6/3/2015 6:43 AM for BCS32843-04
        BUILTIN\Administrators / Full Control
        TLR\prod-corp-e0498.psccr.c / Change
psregs$  /vol/cb0179_trl_ccrprode_snap/psregs Share created by GOKUL SARAVANAN(m179426) on 6/16/2015 12:54 PM for BCS32843-05
        BUILTIN\Administrators / Full Control
        TLR\prod-corp-e0498.psregs.c / Change
slips$   /vol/cb0179_trl_ccrprode_snap/slips Share created by RAMAKRISHNA K(M180853) on 6/4/2015 7:41 AM for BCS32843-03
        BUILTIN\Administrators / Full Control
        TLR\prod-corp-e0498.slips.c / Change
ccrdb$   /vol/cb0179_trl_ccrprode_snap/ccrdb Share created by MADHURI MUDGAL(m180854) on 6/4/2015 12:22 AM for BCS32843-01
        BUILTIN\Administrators / Full Control
        TLR\prod-corp-e0498.ccrdb.c / Change
ccrwip$  /vol/cb0179_trl_ccrprode_snap/ccrwip Share created by Praveen Kumar H.N(M179423) on 6/10/2015 10:47 AM for BCS32843-02
        BUILTIN\Administrators / Full Control
        TLR\prod-corp-e0498.ccrwip.c / Change
```

#### Example of Multiprotocol data share on 7Mode, as seen by Windows; note there is no Security tab in the Properties window.

The screenshot shows the Windows Computer Management interface. On the left, the navigation pane includes System Tools, Task Scheduler, Event Viewer, Shared Folders (with sub-options Shares, Sessions, Open Files), Local Users and Groups, Performance, Device Manager, Storage, and Services and Applications. The 'Shared Folders' node is expanded. The main pane displays a table of shared folders:

| Share Name    | Folder Path          | Type    | # Client Connections | Description                      |
|---------------|----------------------|---------|----------------------|----------------------------------|
| bo41prod...   | C:\vol\cb0183_bis... | Windows | 0                    | Share created by PROD-CORP-E0498 |
| CS            | C:\                  | Windows | 0                    | Remote Admin share               |
| cb0179_trl... | C:\vol\cb0179_trl... | Windows | 0                    |                                  |
| cb0183_bis... | C:\vol\cb0183_bis... | Windows | 0                    |                                  |
| ccrdb\$       | C:\vol\cb0179_trl... | Windows | 2                    | Share created by PROD-CORP-E0498 |
| ccrwip\$      | C:\vol\cb0179_trl... | Windows | 3                    | Share created by PROD-CORP-E0498 |
| ETCS          |                      |         |                      |                                  |
| HOME          |                      |         |                      |                                  |
| IPCS          |                      |         |                      |                                  |
| psscrr\$      |                      |         |                      |                                  |
| psreg\$       |                      |         |                      |                                  |
| slips\$       |                      |         |                      |                                  |

A detailed view of the 'ccrwip\$' properties is shown in a modal window. The 'Share Permissions' tab is selected, displaying the following information:

- Group or user names:** prod-corp-e0498.ccrwip.c (TLR\prod-corp-e0498.ccrwip.c) and Administrators (PROD-CORP-E0498\Administrators)
- Permissions for prod-corp-e0498.ccrwip.c** table:
 

|              | Allow                               | Deny                     |
|--------------|-------------------------------------|--------------------------|
| Full Control | <input type="checkbox"/>            | <input type="checkbox"/> |
| Change       | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Read         | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

### 3. NTFS File Permissions / Security

NTFS permissions are set on CIFS-only builds. Multiprotocol builds only use the CHANGE group applied to the share-level permissions. This is because multiprotocol volumes and qtrees are set to unix security-style while NTFS permissions require ntfs security-style.

The CIFS support team manages the file-level permissions. Storage should NEVER modify these permissions. The NTFS permissions can be viewed in Computer Management under the Security tab of the share Properties or with "fsecurity" command on 7Mode or "vserver security file-directory show" command on CDOT.

There are two CIFS structure standards set by Windows D&E. Structure 1 is most common.

Structure 1

Volume

Qtree

Subfolder1 (share\$) ← Unique permissions set here

The share points to volume\qtree\subfolder1 and the permissions are restricted on subfolder1.

Permissions are set to “NT AUTHORITY\SYSTEM” account and “BUILTIN\Administrators” group with Full Control access. “NT AUTHORITY\Authenticated Users” group is removed. MODIFY (“<domain>\<vserver>.<sharename>.m”) and READONLY (“<domain>\<vserver>.<sharename>.r”) groups are added. Any BU users or groups needing access to the share will be added to the MODIFY or READONLY group depending on the access requested.

## Structure 2

### Volume

Qtree (share\$)

- Subfolder1a ← Unique permissions set here
- Subfolder1b ← Other unique permissions set here
- Subfolder1c ← Additional unique permissions set here

The share points to volume\qtree, but permissions are restricted on each subfolder1. Each subfolder1 will have unique permissions from each other.

The share/qtree will have “NT AUTHORITY\Authenticated Users” group with Readonly access, “BUILTIN\Administrators” group with Full Control access, and “NT AUTHORITY\SYSTEM” account with Full Control access.

Each subfolder1 has permissions set to “NT AUTHORITY\SYSTEM” account and “BUILTIN\Administrators” group with Full Control access. “NT AUTHORITY\Authenticated Users” group is removed. MODIFY (“<domain>\<vserver>.<sharename>.<subfolder>.m”) and READONLY (“<domain>\<vserver>.<sharename>.<subfolder>.r”) groups are added. Any BU users or groups needing access to the share will be added to the MODIFY or READONLY group depending on the access requested.

### Example Structure 1 NTFS permissions on 7Mode, as seen by Storage

```
u0144201@c152mad:~> ssh ln-naslowep-d01 vfiler run prod-ecom-d0075 fsecurity show /vol/cb0551_rs
adtcpd_snap/rsa/data

===== prod-ecom-d0075
[/vol/cb0551_rsadtcpd_snap/rsa/data - Directory (inum 98)]
  Security style: NTFS
  Effective style: NTFS

  DOS attributes: 0x0030 (---AD---)

  Unix security:
    uid: 0 (root)
    gid: 1 (daemon)
    mode: 0777 (rwxrwxrwx)

  NTFS security descriptor:
    Owner: BUILTIN\Administrators
    Group: MGMT\Domain Users
    DACL:
      Allow - ECOM\prod-ecom-d0075.rsaadata.m - 0x001301bf (Modify) - OI|CI
      Allow - ECOM\prod-ecom-d0075.rsaadata.r - 0x001200a9 (Read and Execute) - OI|CI
      Allow - NT AUTHORITY\SYSTEM - 0x001f01ff (Full Control) - OI|CI (Inherited)
      Allow - BUILTIN\Administrators - 0x001f01ff (Full Control) - OI|CI (inherited)
    SACL:
      No entries.
```

Example Structure 1 NTFS permissions on 7Mode, as seen by Windows

The screenshot shows the 'Properties' dialog for a file named 'rsadata.r'. The 'Security' tab is selected. The 'Object name' is listed as '\\PROD-ECOM-D0075.INT.THOMSONREUTERS.COM\rsadata.r'. The 'Group or user names' list includes 'SYSTEM', 'prod-ecom-d0075.rsadata.m (ECOM\prod-ecom-d0075.rsadata.m)', 'prod-ecom-d0075.rsadata.r (ECOM\prod-ecom-d0075.rsadata.r)' (which is highlighted), and 'Administrators (PROD-ECOM-D0075\Administrators)'. Below this, a note says 'To change permissions, click Edit.' with an 'Edit...' button. The 'Permissions for prod-ecom-d0075.rsadata.r' table shows the following:

|                      | Allow | Deny |
|----------------------|-------|------|
| Full control         |       |      |
| Modify               |       |      |
| Read & execute       | ✓     |      |
| List folder contents | ✓     |      |
| Read                 | ✓     |      |

Example Structure 1 NTFS permissions on CDOT, as seen by Storage

```
u0144201@cl52mad:~> ssh pl-cis-clsp-p01 vserver security file-directory show -vserver cisclnt-p0058 -path /cb0838_ggo_legalonedatadbaccp_snap/legalmigration/DBqa

    Vserver: cisclnt-p0058
    File Path: /cb0838_ggo_legalonedatadbaccp_snap/legalmigration/DBqa
    Security Style: ntfs
    Effective Style: ntfs
    DOS Attributes: 10
    DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
        Unix User Id: 65534
        Unix Group Id: 65534
        Unix Mode Bits: 777
    Unix Mode Bits in Text: rwxrwxrwx
    ACLs: NTFS Security Descriptor
        Control:0xaf14
        Owner:MGMT\M6015692
        Group:MGMT\Domain Users
        DACL - ACEs
            ALLOW-ECOMQC\cisclnt-p0058.legalmigrationDBqa.m-0x1301b1-0I|CI
            ALLOW-ECOMQC\cisclnt-p0058.legalmigrationDBqa.r-0x1200a9-0I|CI
            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-0I|CI (Inherited)
            ALLOW-BUILTIN\Administrators-0x1f01ff-0I|CI (Inherited)
```

Example Structure 1 NTFS permissions on CDOT, as seen by Windows

**legalmigrationDBqa\$ Properties**

General Share Permissions Security

Object name: \\CISCLNT-P0058.INT.THOMSONREUTERS.COM\legal...

Group or user names:

- SYSTEM
- cisclnt-p0058.legalmigrationDBqa.m (ECOMQC\cisclnt-p0058.le...
- cisclnt-p0058.legalmigrationDBqa.r (ECOMQC\cisclnt-p0058.le...
- Administrators (CISCLNT-P0058\Administrators)

To change permissions, click Edit. **Edit...**

Permissions for cisclnt-p0058.legalmigrationDBqa.r

|                      | Allow | Deny |
|----------------------|-------|------|
| Full control         |       |      |
| Modify               |       |      |
| Read & execute       | ✓     |      |
| List folder contents | ✓     |      |
| Read                 | ✓     |      |

Example Structure 2 NTFS permissions on 7Mode, as seen by Windows

In Computer Management, the base permissions are listed, but there are no MODIFY or READONLY groups specified. Need to open the share and view the subfolder permissions.

| Share Name    | Folder Path | Type    | # Client |
|---------------|-------------|---------|----------|
| CS            | C:\         | Windows | 0        |
| cb0052_ips_   |             |         |          |
| cb0512_dctr   |             |         |          |
| CullingTool   |             |         |          |
| ETC\$         |             |         |          |
| HOME          |             |         |          |
| IPCS          |             |         |          |
| ipsamsdevd    |             |         |          |
| Licenses\$    |             |         |          |
| odenfileeagan |             |         |          |
| TaxonomyT     |             |         |          |

**odenfileeagan\$ Properties**

General Share Permissions Security

Object name: \\CLNT-CORP-E0848.INT.THOMSONRE...

Group or user names:

- Authenticated Users
- SYSTEM**
- Administrators (CLNT-CORP-E0848\Administrators)

To change permissions, click Edit. **Edit...**

Permissions for SYSTEM

|                      | Allow |
|----------------------|-------|
| Full control         | ✓     |
| Modify               | ✓     |
| Read & execute       | ✓     |
| List folder contents | ✓     |
| Read                 | ✓     |

Opening the share shows the subfolders that have unique permissions. There is also a text document stating this is a Structure 2 build.

| CLNT-CORP-E0848.INT.THOMSONREUTERS.COM ▶ odenfileeagan\$ |                    |
|--|--------------------|
| New folder   |                    |
| Name   | Date created       |
| Apps   | 8/27/2015 2:07 PM  |
| ContentOpsManagement                                     | 8/28/2015 12:50 PM |
| CullingToolData  | 8/27/2015 2:07 PM  |
| Data   | 8/27/2015 2:07 PM  |
| Development  | 8/27/2015 2:07 PM  |
| Licenses   | 8/27/2015 2:07 PM  |
| Production   | 8/27/2015 2:07 PM  |
| QA_Checklists  | 8/27/2015 2:07 PM  |
| Research   | 8/27/2015 2:07 PM  |
| Software   | 8/27/2015 2:07 PM  |
| Support  | 8/27/2015 2:07 PM  |
| TaxonomyTool   | 8/27/2015 2:07 PM  |
| Tech_Transition  | 8/27/2015 2:07 PM  |
| Users  | 8/27/2015 2:07 PM  |
| cifs_standard_structure2_used_here.txt                   | 8/27/2015 2:07 PM  |

Each subfolder has unique permission groups created and applied. The unique groups are named for the subfolder.

CullingToolData Properties

General Security Previous Versions SecureShare Customize

Object name: \\CLNT-CORP-E0848.INT.THOMSONREUTERS.COM\odenfileeagan\CullingToolData

Group or user names:

- SYSTEM
- DL-FIL-clnt-corp-e0848.odenfileeagan.CullingToolData.modify (TEN\-DL-FIL-clnt-corp-e0848.odenfileeagan.CullingToolData.read (TEN\
- Administrators (CLNT-CORP-E0848\Administrators)

Licenses Properties

General Security Previous Versions SecureShare Customize

Object name: \\CLNT-CORP-E0848.INT.THOMSONREUTERS.COM\odenfileeagan\Licenses

Group or user names:

- SYSTEM
- DL-FIL-clnt-corp-e0848.odenfileeagan.Licenses.modify (TEN\-DL-FIL-clnt-corp-e0848.odenfileeagan.Licenses.read (TEN\
- Administrators (CLNT-CORP-E0848\Administrators)

Software Properties

General Security Previous Versions SecureShare Customize

Object name: \\CLNT-CORP-E0848.INT.THOMSONREUTERS.CO

Group or user names:

- SYSTEM
- DL-FIL-clnt-corp-e0848.odenfileeagan.Software.modify (TEN\DL-FIL-clnt-corp-e0848.odenfileeagan)
- DL-FIL-clnt-corp-e0848.odenfileeagan.Software.read (TEN\DL-FIL-clnt-corp-e0848.odenfileeagan)
- Administrators (CLNT-CORP-E0848\Administrators)

Users Properties

General Security Previous Versions SecureShare Customize

Object name: \\CLNT-CORP-E0848.INT.THOMSONREUTERS.CO

Group or user names:

- SYSTEM
- DL-FIL-clnt-corp-e0848.odenfileeagan.Users.modify (TEN\DL-FIL-clnt-corp-e0848.odenfileeagan)
- DL-FIL-clnt-corp-e0848.odenfileeagan.Users.read (TEN\DL-FIL-clnt-corp-e0848.odenfileeagan)
- Administrators (CLNT-CORP-E0848\Administrators)

Windows standards document  
<https://theshare.thomsonreuters.com/sites/windows/Operational%20Documents/Standard%20-%20Folder-Share-Standards.docx>

## 5.2 VENDOR ENGAGEMENT

All Netapp systems at TR are covered by premium support entitlements unless they are already EOSL. We have a few EOSL systems which are covered supported by vendor SMS instead of Netapp.

### 5.2.1 How to raise a Netapp case?

All hardware issues will automatically trigger a call home to Netapp and create a Netapp case. A netapp case can be open online on the web or by phone.

#### By Web

Launch the NetApp Support site and submit a case. Refer instructions in section [How to Open a Netapp case through Web](#)

#### By Phone

**United States and Canada:** 1 888 4 NETAPP (1 888 463 8277)

**EMEA:** 00.800.44.NETAPP (00.800.44.638277)

**India:** 000-800-100-8948 /+91 22 6101 4528

### **5.2.2 How to escalate issues to SAM?**

TR has a dedicated SAM team who will be responsible for vetting out any action plan coming from Netapp support and also responsible for managing critical case communications.

#### **Netapp SAM Coverage and contact information**

### **5.2.3 How to check if a EOSL system is under SMS support?**

Similar to Netapp autosupport any hardware failure on a SMS supported system would trigger a autosupport to SMS and create a case. A quick check of the autosupport option on the filer would show the following:

autosupport.to                    callcenter@sysmaint.com

### **5.2.4 How to manually log a case with SMS Support?**

Calls can be logged with SMS in a number of ways.

By phone:

U.S.: +1 877-405-0330

India: 000-800-100-3918

International: 00-800-1110-0888

By email:

callcenter@sysmaint.com

By Web:

by logging in to our customer support portal [www.mysplogon.com](http://www.mysplogon.com) (singlePoint)

- Exception - Priority 1 system down issues must use the Contact Center #

SMS Contact Center agent will record details necessary to start a service incident and provide a unique call reference number, which will remain with the call until completion. They will also assign a field engineer to triage with the designated Point of Contact recorded on the incident.

Details of the SMS incident can be tracked via singlePoint

## **5.3 EXCEPTION LIST**

A list of Engineering approved exceptions to standards can be referenced [here](#)

Always reference the standards document prior to executing any request and ensure no non-standard configurations are deployed. It is mandatory to use the ServiceNow Automation workflows or WFA workflows where available to ensure standard configurations are correctly deployed.

For all non-standard requests engage Storage D&E for review.

## **5.4 APPENDIX**

### **5.4.1 How to configure a new Vlan?**

<Placeholder.TBA in next version>

### **5.4.2 How to raise a PCA?**

PCA (Production Change Approval) is an emergency change which we need to get approval from our Director or from our Managers. This bypasses the standard lead times required for standard scheduled changes.

As a standard practice, all Emergency Production Change Requests will have Director/Head Of approval from the Business Unit executing the Emergency Change as well as from the Business Unit(s) potentially impacted by the change. The Business Unit executing the change is required to gain Director/Head Of approval for the Emergency Production Change Request. Without such approval, the Emergency Production Change should not be executed."

If our PCA impacts a single BU, we need to get BU director approval as well. In case of shared filers, we need to notify the BU's via an email & approvals from storage PCA & MI team should be enough.

Emergency Change Request Process:

[https://theshare.thomsonreuters.com/sites/SPM/ChM/\\_layouts/WordViewer.aspx?id=/sites/SPM/ChM/Shared%20Documents/Emergency%20Change%20Request%20Process.docx&Source=https%3A%2F%2Ftheshare%2Ethomsonreuters%2Ecom%2Fsites%2FSPM%2FChM%2FShared%2520Documents%2FForms%2FAllItems%2Easpx&DefaultItemOpen=1&DefaultItemOpen=1](https://theshare.thomsonreuters.com/sites/SPM/ChM/_layouts/WordViewer.aspx?id=/sites/SPM/ChM/Shared%20Documents/Emergency%20Change%20Request%20Process.docx&Source=https%3A%2F%2Ftheshare%2Ethomsonreuters%2Ecom%2Fsites%2FSPM%2FChM%2FShared%2520Documents%2FForms%2FAllItems%2Easpx&DefaultItemOpen=1&DefaultItemOpen=1)

This change by default includes the MI team as approvers. We need to get approval from the MI team also to execute the change. Below is the default approvers list when a PCA has raised.

1. Storage-Support
2. PCA-storage-AMERS/ PCA-Storage-APAC
3. Major Incident Team

Open a new change, In categories select emergency

|                   |                   |
|-------------------|-------------------|
| Database          | Database          |
| Emergency         | Emergency         |
| F&R Legacy Builds | F&R Legacy Builds |
| Facility          | Facility          |

In sub category select Break-fix

| SubCategory       | Category  | Description       |
|-------------------|-----------|-------------------|
| Break Fix         | Emergency | Break Fix         |
| Lead Time Not Met | Emergency | Lead Time Not Met |

In the name, you have to select Datacentre- Storage Amers/ Datacentre –Storage Apac. It depends up on the time zone. If you are executing the change in APAC time you have to select Datacentre –Storage Apac. If you are executing the change in Amers time, select Datacentre- Storage Amers.

|                            |  |
|----------------------------|--|
| DataCenter - Storage AMERS | Emergency Changes executed by DataCenter Storage teams during the AMERS time |
| DataCenter - Storage APAC  | Emergency Changes executed by DataCenter Storage teams during the APAC time  |

Current membership:

PCA-storage-AMERS – Jill Gerdig, Shrinath Kurdekar

- PCA-storage-APAC – Karthic Kulandaivelu, Divyashri Prabhu

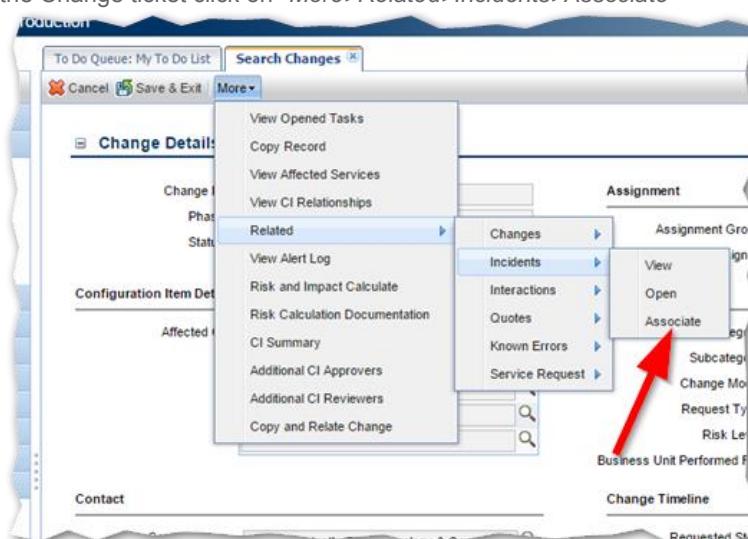
## Classification

|                               |                            |
|-------------------------------|----------------------------|
| Category                      | Emergency                  |
| Subcategory *                 | Break Fix                  |
| Change Model *                | DataCenter - Storage AMERS |
| Risk Level                    |                            |
| Business Unit Performed For * | Data Center Operations     |

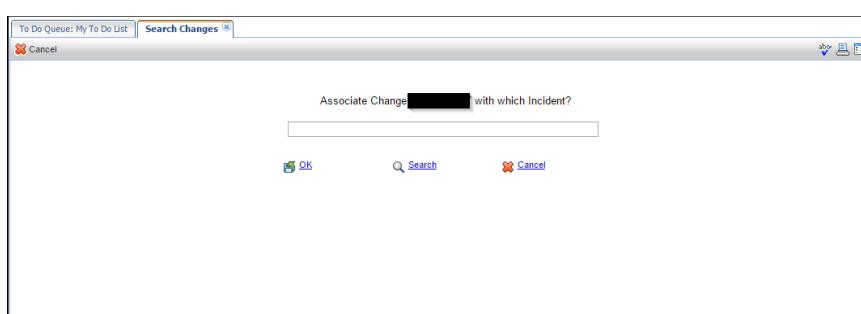
You have to fill the list of question in the description

- Who is the BU Director or level above that has already approved?
- What customers/services/applications will the change request affect?
- What is the current internal and/or external impact?
- When did the impact start?
- CI impacted by CR
- Change Detail including action plan as received and agreed from NetApp

The Incident ticket needs to be associated with this Change Request ticket so that the two items can be tied together. To associate an IM to the Change ticket click on "More>Related>Incidents>Associate"



This will bring up the following window to associate the relevant IM to this ticket Type in the relevant IM and click OK, save the CR record as normal.



Full approval within SM9 should be gained on the CR prior to execution. Please ensure that this is done prior to execution of the Change. If this is causing a business impact and the change needs to be execute as soon as possible to restore service, then verbal approval should be given from the approval groups and SM9 approval followed up post change execution.

### 5.4.3 Raising a Major Incident

The Major Incident Management team will ensure the Major Incident Processes are followed during a Major Incident's investigation and recovery. They will ensure escalations are made and communications issued to impacted or at risk stake holders.

#### Objectives of the Major Incident:

To ensure clear timely communications are issued and attain the fastest possible service mitigation.

#### CONTACT INFORMATION

Contact the team via the hotline manned 24/7 +1 651 848 8000

Email – major-incident-shared@thomsonreuters.com

When any Panic happens, we will get a P1 auto generated IM. The Incident ticket should be marked as a Major Incident and the team engaged. The Major Incident flag should be checked within 30 minutes of receiving incident ticket to get the awareness to our customers and stakeholders as quickly as possible. Detailed impact information should be provided including impacted Business Units, products and services.

1. Open the P1 auto-generated Incident
2. At the right side below the classification you will find a Major Incident option and you have to check in the check box.

**Classification**

---

|                      |                         |
|----------------------|-------------------------|
| Category *           | incident                |
| Area *               | Application             |
| Sub Area *           | Performance Degradation |
| Priority/Tolerance * | P1 / <1hour             |
| Impact *             | 4 - User                |
| User Impact *        | 4 - None                |

Major Incident

After checking the box, we need to save the IM, which will populate another window and we have to update the Information regarding the incident.

The Major Incident will send an email to us and a TRT call will be raised. We have to provide the impacted host list as well the BU's list. The Major Incident team will engage them in a TRT Call.

### 5.4.4 Bug Database and Key Known Bugs

A list of known bugs that have impacted our environment along with details on the release these are fixed can be found [here](#)

Below are some of the most critical ones to be aware of:

## PCI-NMI bug

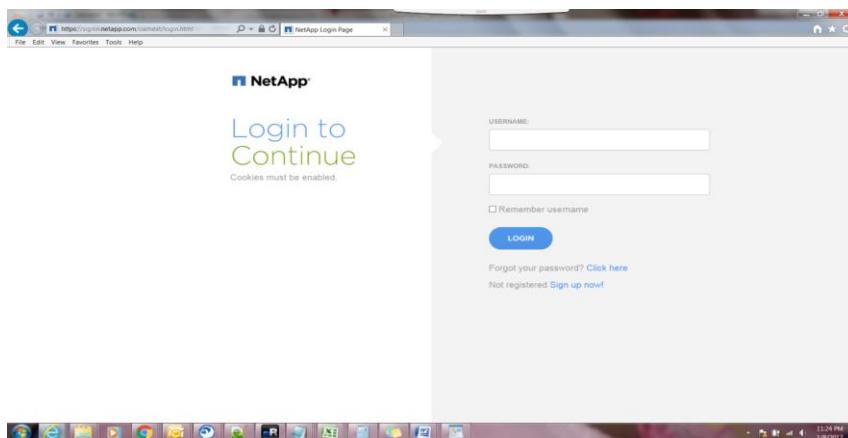
## Long CP and Iscsi Bugs

## WAFL inconsistency Issue

### 5.4.5 How to Open a Netapp case through Web

1. Use the following link to login into NetApp support site to log a case.  
<https://signin.netapp.com/oamext/login.html>

Login using your NetApp registered username and password.



2. In "My Home" page you will find "Create Case" button. Click on the "Create Case" button.

| Status | Case Number | Priority | Serial Number | Description                           | System/Host Name | Date Last Updated |
|--------|-------------|----------|---------------|---------------------------------------|------------------|-------------------|
| Active | 2006610165  | P2       | 800000113178  | [NAS]NFS LOCKS DURING A TAKEOVER (TR) | LN-NASECOM-D01   | 23-Dec-2016       |
| Closed | 41242592    | P2       |               | NSS - CHANGED MY EMPLOYER             |                  | 31-Oct-2016       |
| Closed | 41242577    | P2       |               | NSS - ACCESS LEVEL UPGRADE            |                  | 28-Oct-2016       |
| Closed | 6246114     | P2       |               | NSS - ACCESS LEVEL UPGRADE            |                  | 19-May-2016       |

3. Key in the filer serial number in the text box highlighted. Click the "GO" button. If you do NOT have serial number but know the host (filer) name move to next step

4. Ignore this step if you followed step 3. If you have hostname, select the “system/Host Name” option from the highlighted dropdown box and key in the host name in the next box and click “GO” button.

5. It will display the system details for the mentioned serial number and hostname. Cross check the displayed results and click on the “select>” which was highlighted.

|                             | Serial Number | Cluster Serial Number | Cluster Name | Location                               | System Name    | Product Number | OS Version     | Auto Support Status | Group  |
|-----------------------------|---------------|-----------------------|--------------|--|----------------|----------------|----------------|---------------------|--------|
| <a href="#">SELECT &gt;</a> | 850000207704  |                       |              | TR-CPS-SN-SINGAPORE-18 SCIENCE PARK DR | SN-NASECOM-S01 | FAS6210 MODEL  | 8.1.3P1 7-MODE | ON                  | TR-CPS |

6. Please select the problem Category from the options provided in drop down (2. Questions/Problem Category).

**Parts & Parts >> Create Case**

**Describe the Problem or Question**

**1. Product Affected (Optional)**

850000207704    TR-CPS-SN-SINGAPORE-18    SN-NASECOM-S01    FAS6210 MODEL    8.1.3P1 7-MODE    ON    TR-CPS

**2. Question / Problem Category**

Select

If you are having issues identifying the appropriate codes to open your case, view full mapping of all codes.

**3. Question / Problem**

Please briefly describe your problem here (250 characters maximum), you will have the opportunity to fully define and add more details to your problem later in the case creation process

Cancel / Choose a different system **GO**

SINGAPORE-18 S01    MODEL    7-MODE

7. Select the sub-category from the selected problem Category using the drop-down box.

**Parts >> Create Case**

**Describe the Problem or Question**

**1. Product Affected (Optional)**

850000207704    TR-CPS-SN-SINGAPORE-18    SN-NASECOM-S01    FAS6210 MODEL    8.1.3P1 7-MODE    ON    TR-CPS

**2. Question / Problem Category**

Client/Host Software > Select

If you are having issues identifying the appropriate codes to open your case, view full mapping of all codes.

**3. Question / Problem**

Please briefly describe your problem here (250 characters maximum), you will have the opportunity to fully define and add more details to your problem later in the case creation process

Cancel / Choose a different system **GO**

SINGAPORE-18 S01    MODEL    7-MODE

8. Select the sub-category of the sub-category once again from the drop-down box.

**Parts >> Create Case**

**Describe the Problem or Question**

**1. Product Affected (Optional)**

850000207704    TR-CPS-SN-SINGAPORE-18    SN-NASECOM-S01    FAS6210 MODEL    8.1.3P1 7-MODE    ON    TR-CPS

**2. Question / Problem Category**

Client/Host Software > SnapManager/SnapDrive > Select

If you are having issues identifying the appropriate codes to open your case, view full mapping of all codes.

**3. Question / Problem**

Please briefly describe your problem here (250 characters maximum), you will have the opportunity to fully define and add more details to your problem later in the case creation process

Cancel / Choose a different system **GO**

SINGAPORE-18 S01    MODEL    7-MODE

9. Give a brief explanation about the problem (Explanation should not exceed 250 characters). Click on "Go" button once done.

Parts >> Create Case

Describe the Problem or Question

**1. Product Affected (Optional)**

|              |  |                |               |                |    |        |
|--------------|--|----------------|---------------|----------------|----|--------|
| 850000207704 | TR-CPS-SN-SINGAPORE-18 SCIENCE PARK DR | SN-NASECOM-S01 | FAS6210 MODEL | 8.1.3P1 7-MODE | ON | TR-CPS |
|--------------|--|----------------|---------------|----------------|----|--------|

**2. Question / Problem Category**

Client/Host Software > SnapManager/SnapDrive > SnapDrive for Windows

*If you are having issues identifying the appropriate codes to open your case, [view full mapping of all codes](#).*

**3. Question / Problem**

Luns missing in snapdrive

Cancel / Choose a different system **GO**

SINGAPORE-18 S01 MODEL 7-MODE

10. It will display all the existing cases available for this filer. If the case, you are going to open exists click cancel otherwise click on button "continue with a New case" at the bottom.

Cases & Parts >> Create Case

### Open A Case - Duplicate Cases

Tell us which Product is affected and what you're trying to solve or learn.

Note: This page is for Technical Cases only. Please use our [Feedback Form](#) if you need other assistance.

|                              |  |  |
|------------------------------|--|--|
| Product Affected:            | Serial# 850000207704, TR-CPS-SN-SINGAPORE-18 SCIENCE PARK DR, Autosupport:ON, Group:TR-CPS | <a href="#">Change Product / Problem</a> |
| Question / Problem Category: | Client/Host Software > SnapManager/SnapDrive > SnapDrive for Windows                       |  |
| Question / Problem:          | Luns missing in snapdrive  |  |

**Please note:** The case(s) below was created for this same serial number (850000207704) and is either still Open or was created within the past 7 days. Before creating a new case please ensure your request has not already been processed. To view or edit an existing case click on the case number.

| Case Number | Serial Number | Cluster Serial Number | Cluster Name | Status                    | Symptom                          | Date Submitted          |
|-------------|---------------|-----------------------|--------------|---------------------------|----------------------------------|-------------------------|
| 2006556632  | 850000207704  |                       |              | Pending Customer Data     | SDW GETS HUNG AT SERVER BOOT UP. | 10/20/2016 01:44:34 PST |
| 2008674653  | 850000207704  |                       |              | Pending Solution Proposed | [HW] SHELF POWER INTERRUPTED     | 01/05/2017 16:34:33 PST |
| 7043314     | 850000207704  |                       |              | Completed                 | [HW] SHELF POWER INTERRUPTED     | 01/06/2017 00:00:00 PST |

Cancel **Continue with a New Case**

11. Click on "Continue" button at the bottom

Cases & Parts >> Create Case

### Open A Case - Extra Information Needed

< Back to Describe the Problem or Question

If you'd prefer to skip this, click [Continue: Open a Case](#) >

|                              |  |  |
|------------------------------|--|--|
| Product Affected:            | Serial# 850000207704, TR-CPS-SN-SINGAPORE-18 SCIENCE PARK DR, Autosupport:ON, Group:TR-CPS | <a href="#">Change Product / Problem</a> |
| Question / Problem Category: | Client/Host Software > SnapManager/SnapDrive > SnapDrive for Windows                       |  |
| Question / Problem:          | Luns missing in snapdrive  |  |

For LUN troubleshooting and case framing please review the [LUN Technical Triage Template](#). If you were unable to solve your problem with the Triage Template then please continue the case creation process.

Cancel Problem Resolved **Continue**

12. Fill all the information for mandatory fields and click "Go" button at the bottom with will create a new case for you.

Cases & Parts >> Create Case

### Open A Case - Case And Contact Information

< Back to Review related Articles

|                                     |  |                                 |
|-------------------------------------|--|---------------------------------|
| <b>Product Affected:</b>            | Serial# 850000207704, SN-NASECOM-S01, TR-CPS-SN-SINGAPORE-18 SCIENCE PARK<br>DR, Autosupport, Group:TR-CPS | <b>Change Product / Problem</b> |
| <b>Question / Problem Category:</b> | Client/Host Software > SnapManager/SnapDrive > SnapDrive for Windows                                       |                                 |
| <b>Question / Problem:</b>          | Luns missing in snapdrive  |                                 |

**Main Contact**

\* First Name: Anil Kumar  
 \* Last Name: Vytla  
 \* Email Address: anil.vytla@thomsonreuters.com  
 \* Office Phone: 04067142136  
 Mobile Phone:  
 \* Contact Preference: Select One

E-mail address(es) entered here will be cc'd on case status updates. Separate multiple e-mail addresses with a comma.  
**Email Addresses:**

Receive email updates on status change.

**Additional Contacts**

**Upload Files**

If you have a screen capture, a log file, or any other content that might help us diagnose your question or problem, please upload it here.

**Choose File** No file chosen. (How to upload large file)

**Problem Information**

\* Priority level:  P4: General technical question or request for information  
 P3: Occasional disruption or problem  
 P2: Serious or repetitive disruption / very poor performance  
 P1: System not serving any data

**Speak to an agent** Provide contact information and we will call you.

**Live Chat to Submit Case** 04:30 PM PT Sun to 05:00 PM PT Fri

\* Problem Summary: Luns missing in snapdrive 1974 chars left

\* When was the issue first observed? Example Answer: 2 days ago, 03.07.09 17:00 250 chars left

\* Were there any recent changes or maintenance activities performed? Example Answer: We move this VFiler to a new domain 250 chars left

\* OS Version: 8.1.3P1 7-MODE 86 chars left

\* Please describe the environment. (Filer model, ONTAP version, Protocols and application versions in use, etc.) Example Answer: FAS3020C, OnTap 7.2 4P9, Clients are W2k, XP and Vista. The VFiler is a CISF only VFiler, W2k3 R2 domain 250 chars left

**GO**

## 5.4.6 Offline volumes (prior to deletion)

### Summary

Due to the impact of destructive commands on a Shared Filer and potential disruption to business. Volumes should not be instantly deleted. This procedure calls for the volume to be checked for IOPS before off-lining and renaming of the volume. All deletion should occur after a minimum of 7 days.

Note: Exception is if this will cause business outage due to capacity issues. Any such instances need escalation and agreement from Storage Management before proceeding.

### Steps for off-lining a volume

1. Create a CR with list of volumes that are being offline. The CR should include config admin and Support groups that own the volume as approvers.
2. Check the current state of the volume

- a. If the volume is already offline, just rename the volume to the standard (volumename\_<CRNO>\_<expiry date>) note : Expiry should be kept for 7days from the day when you offline ( eg : test\_CR0091\_EXP10May2012).
  - b. If the volume is in restricted state, check for any data copy process is running. If so, then we can ignore this volume.
3. If the volume is online but with other names like volumename\_Migrated, which means this volume is migrated and but forgot to offline/destroy.
- a. Find the source migration CR and confirm whether this volume is really migrated and also check the new location where it is migrated.
  - b. Check for the exports entry or the exportfs details.
  - c. Storage will verify the protocol of the volume (CIFS/NFS/ISCSI) (do reset the protocol statistic to zero and then monitor).
  - d. Storage team Double check the volume list given by platform team. – Storage team.
4. Check for Mounts, Verify NFS, CIFS, ISCSI details.
5. Check the host is mounted on any of the servers by using command **/usr/sbin/showmount -a <vfiler name>**

- a. If any hosts are mounted as below, please reach out to Unix team and get confirmation that no volume is mounted on server.

```
-bash-3.2$ /usr/sbin/showmount -a clnt-corp-e0219
All mount points on clnt-corp-e0219:
atsh9011.int.westgroup.com:/vol/at_casetrack_dev_nosnap/dev_logs
atsh9025.int.westgroup.com:/vol/at_casetrack_test_nosnap/test_logs
c194chknewsaq.int.westgroup.com:/vol/at_newsroomfeedsqael_nosnap/new_newsroom
c716wuzcsdbqe.int.westgroup.com:/vol/at_dr_secure_alerts515q_n01oral1_nosnap/n01oraadmin1
c716wuzcsdbqe.int.westgroup.com:/vol/at_dr_secure_alerts515q_n01oral1_nosnap/n01oracluster1
c716wuzcsdbqe.int.westgroup.com:/vol/at_dr_secure_alerts515q_n01oral1_nosnap/n01oradata1
c716wuzcsdbqe.int.westgroup.com:/vol/at_dr_secure_alerts515q_n01oral1_nosnap/n01oraggs
c716wuzcsdbqe.int.westgroup.com:/vol/at_dr_secure_alerts515q_n01oral1_snap/s01oradata1
c716wuzcsdbqe.int.westgroup.com:/vol/at_dr_secure_alerts515q_s01oraadmin1_snap/s01oraadmin1
c774zkcsdbqe.int.westgroup.com:/vol/at_dr_secure_alerts515q_n01oral1_nosnap/n01oraadmin1
c774zkcsdbqe.int.westgroup.com:/vol/at_dr_secure_alerts515q_n01oral1_nosnap/n01oracluster1
c774zkcsdbqe.int.westgroup.com:/vol/at_dr_secure_alerts515q_n01oral1_nosnap/n01oradata1
c774zkcsdbqe.int.westgroup.com:/vol/at_dr_secure_alerts515q_n01oral1_nosnap/n01oraggs
c774zkcsdbqe.int.westgroup.com:/vol/at_dr_secure_alerts515q_s01oral1_snap/s01oradata1
c774zkcsdbqe.int.westgroup.com:/vol/at_dr_secure_alerts515q_s01oraadmin1_snap/s01oraadmin1
c813ewdnewsaq.int.westgroup.com:/vol/at_newsroomfeedsqael_nosnap/new_newsroom
c836jpbnewsaq.int.westgroup.com:/vol/at_newsroomfeedsqael_nosnap/new_newsroom
carlin-nas.int.westgroup.com:/vol/at_cobalt5t_n01oral1_nosnap/n01raadmin1
carlin-nas.int.westgroup.com:/vol/at_cobalt5t_n01oral1_nosnap/n01racluster1
cmp111mgc.int.westgroup.com:/vol/clnt_corp_e0219_root
ctbin9010.int.westgroup.com:/vol/at_newsroomfeedsqael_nosnap/new_newsroom
nerstrand.int.westgroup.net:/etc
```

## 6. Check for IO operations – NFS Statistics

- a. Enable the NFS statistics at vfiler level - **options nfs.per\_client\_stats.enable on**

```
-bash-3.2$ ssh eg-nasclnt-e06 vfiler run clnt-corp-e0219 options nfs.per_client_stats.enable
===== clnt-corp-e0219
nfs.per_client_stats.enable off
```

```
-bash-3.2$ ssh eg-nasclnt-e06 vfiler run clnt-corp-e0219 options nfs.per_client_stats.enable on
===== clnt-corp-e0219
```

```
-bash-3.2$ ssh eg-nasclnt-e06 vfiler run clnt-corp-e0219 options nfs.per_client_stats.enable  
===== clnt-corp-e0219  
nfs.per_client_stats.enable on
```

NOTE: Usually this options should **NOT** remain **O** , because causes an performance reduction, Please change it to **OFF** when you finish - options nfs.per\_client\_stats.enable off

- b. Reset the IO counter at vfiler level usin nfsstat -z

```
-bash-3.2$ ssh eg-nasclnt-e06 vfiler run clnt-corp-e0219 nfsstat -z  
===== clnt-corp-e0219
```

- c. Then Run nfsstat -l at vfiler to get the nfs call stat

**NOTE: PLEASE MONITOR FOR SOME TIME IF ANY READ and WRITES ARE HAPPENING IN THE VOLUME**

Example output with NFS iops

```
-bash-3.2$ ssh eg-nasclnt-e06 vfiler run clnt-corp-e0219 nfsstat -l
```

```
===== clnt-corp-e0219  
10.204.66.105 c716wuzcsdbqe.int.westgroup.com NFSOPS = 2168 (95%) (here it should not show any nfs calls )  
10.204.66.107 c774zwkcsdbqe.int.westgroup.com NFSOPS = 121 ( 5%)
```

```
-bash-3.2$ ssh eg-nasclnt-e06 vfiler run clnt-corp-e0219 nfsstat -l  
===== clnt-corp-e0219  
10.204.66.105 c716wuzcsdbqe.int.westgroup.com NFSOPS = 2168 (95%)  
10.204.66.107 c774zwkcsdbqe.int.westgroup.com NFSOPS = 121 ( 5%)
```

Example output if no NFS call or host is accessing the volume below

```
-bash-3.2$ ssh eg-nasclnt-e06 vfiler run clnt-corp-e0414 nfsstat -l
```

```
-bash-3.2$ ssh eg-nasclnt-e06 vfiler run clnt-corp-e0414 nfsstat -l  
===== clnt-corp-e0414  
-bash-3.2$
```

## 7. Check for IO operations – Stats Show

Check for stats show volume command for any read write operation on that particular volume. There should not be read and write ops to this volume. It should be zero for everything. Else please reach out to application team for confirmation.

- a) Stats show example with iops as below, If IOPS is happening please reach out to Application and Unix team. **Do NOT proceed with volume offline until the volume has been unmounted and confirmed by the Application team.**

```
-bash-3.2$ ssh eg-nasclnt-e06 stats show volume:at_dr_secure_alerts515q_s01ora1_snap  
volume:at_dr_secure_alerts515q_s01ora1_snap:instance_name:at_dr_secure_alerts515q_s01ora1_snap  
volume:at_dr_secure_alerts515q_s01ora1_snap:node_name:
```

```

volume:at_dr_secure_alerts515q_s01ora1_snap:instance_uuid:62acd2cb-c954-11e2-b883-123478563412
volume:at_dr_secure_alerts515q_s01ora1_snap:vserver_name:
volume:at_dr_secure_alerts515q_s01ora1_snap:vserver_uuid:
volume:at_dr_secure_alerts515q_s01ora1_snap:avg_latency:342.34us
volume:at_dr_secure_alerts515q_s01ora1_snap:total_ops:28/s
volume:at_dr_secure_alerts515q_s01ora1_snap:read_data:0b/s
volume:at_dr_secure_alerts515q_s01ora1_snap:read_latency:0us
volume:at_dr_secure_alerts515q_s01ora1_snap:read_ops:0/s
volume:at_dr_secure_alerts515q_s01ora1_snap:write_data:240000b/s
volume:at_dr_secure_alerts515q_s01ora1_snap:write_latency:401.22us
volume:at_dr_secure_alerts515q_s01ora1_snap:write_ops:22/s
volume:at_dr_secure_alerts515q_s01ora1_snap:other_latency:116.67us
volume:at_dr_secure_alerts515q_s01ora1_snap:other_ops:5/s

```

```

-bash-3.2$ ssh eg-nasclnt-e06 stats show volume:at_dr_secure_alerts515q_s01ora1_snap
volume:at_dr_secure_alerts515q_s01ora1_snap:instance_name:at_dr_secure_alerts515q_s01ora1_snap
volume:at_dr_secure_alerts515q_s01ora1_snap:node_name:
volume:at_dr_secure_alerts515q_s01ora1_snap:instance_uuid:62acd2cb-c954-11e2-b883-123478563412
volume:at_dr_secure_alerts515q_s01ora1_snap:vserver_name:
volume:at_dr_secure_alerts515q_s01ora1_snap:vserver_uuid:
volume:at_dr_secure_alerts515q_s01ora1_snap:avg_latency:342.34us
volume:at_dr_secure_alerts515q_s01ora1_snap:total_ops:28/s
volume:at_dr_secure_alerts515q_s01ora1_snap:read_data:0b/s
volume:at_dr_secure_alerts515q_s01ora1_snap:read_latency:0us
volume:at_dr_secure_alerts515q_s01ora1_snap:read_ops:0/s
volume:at_dr_secure_alerts515q_s01ora1_snap:write_data:240000b/s
volume:at_dr_secure_alerts515q_s01ora1_snap:write_latency:401.22us
volume:at_dr_secure_alerts515q_s01ora1_snap:write_ops:22/s
volume:at_dr_secure_alerts515q_s01ora1_snap:other_latency:116.67us
volume:at_dr_secure_alerts515q_s01ora1_snap:other_ops:5/s

```

b) Stats show example for no IOPS occurring, output should be like below

```

-bash-3.2$ ssh eg-nasclnt-e06 stats show volume:bis_bi2a_n01ora1_nosnap
volume:bis_bi2a_n01ora1_nosnap:instance_name:bis_bi2a_n01ora1_nosnap
volume:bis_bi2a_n01ora1_nosnap:node_name:
volume:bis_bi2a_n01ora1_nosnap:instance_uuid:0dbaf756-b24a-11e2-b883-123478563412
volume:bis_bi2a_n01ora1_nosnap:vserver_name:
volume:bis_bi2a_n01ora1_nosnap:vserver_uuid:
volume:bis_bi2a_n01ora1_nosnap:avg_latency:0us
volume:bis_bi2a_n01ora1_nosnap:total_ops:0/s
volume:bis_bi2a_n01ora1_nosnap:read_data:0b/s
volume:bis_bi2a_n01ora1_nosnap:read_latency:0us
volume:bis_bi2a_n01ora1_nosnap:read_ops:0/s
volume:bis_bi2a_n01ora1_nosnap:write_data:0b/s
volume:bis_bi2a_n01ora1_nosnap:write_latency:0us
volume:bis_bi2a_n01ora1_nosnap:write_ops:0/s
volume:bis_bi2a_n01ora1_nosnap:other_latency:0us
volume:bis_bi2a_n01ora1_nosnap:other_ops:0/s

```

```

-bash-3.2$ ssh eg-nasclnt-e06 stats show volume:bis_bi2a_n01ora1_nosnap
volume:bis_bi2a_n01ora1_nosnap:instance_name:bis_bi2a_n01ora1_nosnap
volume:bis_bi2a_n01ora1_nosnap:node_name:
volume:bis_bi2a_n01ora1_nosnap:instance_uuid:0dbaf756-b24a-11e2-b883-123478563412
volume:bis_bi2a_n01ora1_nosnap:vserver_name:
volume:bis_bi2a_n01ora1_nosnap:vserver_uuid:
volume:bis_bi2a_n01ora1_nosnap:avg_latency:0us
volume:bis_bi2a_n01ora1_nosnap:total_ops:0/s
volume:bis_bi2a_n01ora1_nosnap:read_data:0b/s
volume:bis_bi2a_n01ora1_nosnap:read_latency:0us
volume:bis_bi2a_n01ora1_nosnap:read_ops:0/s
volume:bis_bi2a_n01ora1_nosnap:write_data:0b/s
volume:bis_bi2a_n01ora1_nosnap:write_latency:0us
volume:bis_bi2a_n01ora1_nosnap:write_ops:0/s
volume:bis_bi2a_n01ora1_nosnap:other_latency:0us
volume:bis_bi2a_n01ora1_nosnap:other_ops:0/s

```

8. Once all of these checks are passed, and then rename the volume as per the standard and offline the volume.
9. Complete post checks and close the CR.

#### Performing the checks on the Down filer

1. SSH <down filer> cf status
2. SSH <down filer> vfiler status
3. SSH <down filer> vfiler status -r
4. SSH <down filer> Vfiler run “\*” lun show
5. SSH <down filer> Vfiler run “\*” igrup show
6. SSH <down filer> vfiler run “\*” cifs domaininfo

Use the below script to verify ping of all vFilers:

```
for i in <down filer> ;do echo "-----$i-----";for j in `ssh $i  
vfiler status |awk -F " " '{print $1}' |grep -v vfiler0` ; do echo  
"===== $i ====="; ping -c 2 $j; done;done
```

## 5.5 ORACLE ZFS

<Placeholder. To be added in next version>

### 5.5.1