

EMEA NAS Infrastructure

Process Control Manual

Classification: **Internal**
Issuer: Paul McInerney
Department: EMEA NAS & Mainframe Storage Management
Authors: Clive Bates
Paul McInerney

Version: 4.32

Contents

Contents.....	2
Introduction.....	6
1.1 Purpose of Document.....	6
1.2 NAS Infrastructure Operations Group Overview.....	6
1.3 Management	6
1.4 Client Base	6
1.5 Role	7
1.6 Location & Contact Details.....	7
1.7 Hours of Cover.....	8
1.8 Faults & Requests	8
1.9 Shared Group Data	8
1.10 Websites	8
Controls Verification Systems (CVS) Checks	9
1.11 Introduction.....	9
1.12 Process	9
CITMP Introduction	10
1.13 Introduction.....	10
1.14 CITMP Levels.....	10
1.15 Review of Level 3s and RCSA.....	10
1.16 Presentations.....	10
1.17 Applicability	10
Resource Management	12
1.18 Roles and Responsibilities.....	12
1.19 NAS Management	26
1.20 Netapp Filer resource assignment	26
Change Management	27
1.21 Introduction.....	27
1.22 Virtual Change Getting Started.....	27
1.23 EMEA NAS Infrastructure Procedures	27
1.24 Pre-Implementation checkout	27
1.25 Post-Implementation checkout.....	27
1.26 Virtual Requests.....	28
Problem Management	34
1.27 Definition of Problem Management	34
1.28 Identification and Documentation	35
1.29 Escalation and Notification.....	37
1.30 Determination.....	38
1.31 Bypass and Recovery	39
1.32 Resolution	39
1.33 Management Oversight	39
1.34 MIS Reporting.....	39
Information Security	41
1.35 Information Security	41
1.36 NAS Infrastructure Rights.....	41
1.37 Entitlement Reviews.....	42
1.38 Joiners & Leavers.....	42
1.39 Functional Account Management.....	43
1.40 TEARS EVENT JUSTIFICATION AND REVIEWS	50
1.41 Information Systems Inventory.....	52
1.42 Vulnerability and Threat Patch Management	52
Continuity of Business	54
1.43 Contingency Requirements	54
Implementing / Decommissioning NetApp Filers.....	55
1.44 Implementing NetApp Filers.....	55
1.45 Decommissioning of NetApp Filers Requirements	55
Internet Management.....	57
Contracting and Outsourcing	58

Architecture	59
Project Management	60
Software Management	61

Version Control

Date	Version	Reason for Change
04-06-03	1.2	Added DFM backup scheduled Job check and changed all NAS references to read NetApp. Update document template to new standard
17-12-02	Draft 1.0	New Document
25-02-03	Draft 2.0	Changed format of document to move away from a functional based one to a daily checks format
03-03-03	2.0	Production Release of this document.
17-06-03	2.1	1. Document renamed to Process Control Manual to comply with CITMP. 2. Reformat of document to comply with new group standards. 3. Updated section 3.1.1 with new DFM Check and updated file locations. 4. Updated WebAdmin Server Checks (Removed ISOEUK01/02) 5. Updated NetApp Filer System Message Log URL. 6. Added checks for AD / EUR. 7. Updated GPMS queue details, 8. Added LDRPS yearly check.
19-06-03	2.2	Reformatted document to include page breaks.
26-06-03	2.3	Added Problem Management section and re-numbered.
30-06-03	2.4	Added check summary table.
16-07-03	2.5	Added location of check sheets.
22-07-03	2.6	Expanded section 3 on Problem management
31-10-03	2.7	Added Continuity of Business Section
21-11-03	2.8	1. Added check for EU Account Descriptions to monthly checks (2.7.1) 2. Updated Automated job checks to include McAfee and NetApp Snapshots (2.5.1) 3. Updated the Filer section to include the new filer names. 4. Updated Snapshot checks URL. 5. Added DFM backup check. 6. Updated WebAdmin 3.0 server list to include EURDCLN012. 7. Added check for Administrator groups.
27-11-03	2.9	1. Added section on resource management, groups rights.
08-12-03	2.10	1. Added section on Server management (3.4) 2. Removed al references in hyperlinks to \\nasldn02 and replaced with g:\ 3. Added Monthly check for Approved Administrators 4. Added Yearly check on automated Scripts. 5. Updated Administrators Group check section. 6. Added links to TAS and Server list in the EU Domain Controllers section. 7. Updated Data Fabric Manager Check section. 8. Updated the DFM Backup Section. 9. Added performance baseline checks to the WebAdmin section. 10. Added EURDMZ checks
14-01-04	2.11	1. RITS section added to new starters process. 2. Added section on Information Systems Inventory. 3. Change monitoring server name from ldnctisw001 to ldnctisw002 4. Added reference to NetApp Filer installation document. 5. Added section on System Management Processes. 6. Added process for AD group renaming. 7. Added Quarterly check for Filer shares to summary sheet.

15-01-04	2.12	1. Added section on the use of the EUDCADM account.
23-01-04	2.13	1. Updated wording in section 3.7.2.
09-03-04	2.14	1. Adding section 2.7.10 on monthly archiving of emails for the DL *GT EMEA Wintel Infrastructure 2. Added section 3.5.6 on upgrading Net App Filers to Data ONTAP v6.4.2P6
14-04-04	3.00	1. Changed document name to "EMEA Wintel Inf PCM 2.15" 2. Changed all instances of EU Wintel to EMEA Wintel. 3. Expanded on Group Information. 4. Added section on Change Management. 5. Re arranged document to follow WIO agreed format.
27-04-04	3.00	1. Updated section on group information. 2. Added Websites section. 3. Updated CITMP Section. 4. Updated Change Management Section. 5. Added Section on Event Log review in the Resource management section 6. Changed URL for EURDMZ reporting tool 7. Updated Virtual Tech Queue details
05-05-04	3.01	1. Added document Information on front page. 2. Moved sections Wintel Infrastructure Rights, Reviews, Joiners & Leavers, Domain Controller Loan Administrator Accounts to Information Security Section. 3. Moved Section Information Systems Inventory to Information Security Section. 4. Updated section on Functional Account Inventory. 5. Updated section on Vulnerability and Threat Patch management process. 6. Updated section on Entitlement Reviews. 7. Updated section on the adminADMT process. 8. Added a daily check to check for new un-approved functional accounts. 9. Added section on the EU Account Lockout Page. 10. Updated NetApp Filers local Admins check
19-05-04	3.02	1. Updated Column to CVS Checks sheet. 2. Updated Section on MIS Reporting
19-05-04	3.03	1. Updated section on Functional Account Inventory. 2. Updated section on Vulnerability and Threat Patch management process. 3. Updated Joiners and Leavers section. 4. Updated section on capacity planning.
25-05-04	3.04	1. Updated section on Event Log Reviews and Functional Account Inventory.
28-05-04	3.05	1. Updated section on Server Reconciliation
17-06-04	3.06	1. Added section detailing process the allows data owners to add resources to filer.
09-09-04	3.07	1. Functional Account Creation for EMEA Wintel Infrastructure added
19-10-04	3.08	1. Updated section on loan of EUDCADM to include expiration date. 2. Updated section on loan of EUDCADM to reflect new path of tracking spreadsheet. 3. Removed Weekly CVS check of database integrity as this has been decommissioned. 4. Updated hours of cover to reflect on site until 18:00. 5. Added entry to daily checks to send out morning status report. 6. Added entry to daily checks to update Service Notification Tool. 7. Added entry to daily checks to include the checking of users on all SOE locators. 8. Added entry to daily checks to monitor newly created EU accounts. 9. Added daily and quarterly checks for WINS servers. 10. Added daily checks for FTP servers. 11. Added daily checks for GDS infrastructure.
09-11-04	3.09	1. Added process for bulk account deletion
22-11-04	3.10	1. Added information regarding capacity planning carried out by ENI 2. Added capacity planning to daily checks
11-01-05	3.11	1. Added weekly check for the SOE DB Locators. 2. Removed GPMS Queue Details, and added VT MAC details. 3. Added EURDCME001 to the WebAdmin checks list. 4. Updated server retirement process. 5. Replaced all instances of "Generic" with "Functional". 6. Added daily check for the WAAT import process.
13-01-05	3.12	1. Added chapter 16 2. Added section 16.1 for NAS Problem Management

04-02-05	3.13	1. Added section 16.2 for NAS Resource Management
07-02-05	3.14	1. Added section 16.2.4.1 for Anti Virus scanning installation and configuration
08-02-05	3.15	1. Insert new section 16.2.1.1 Licensing (all subsequent sections increase by one) 2. Updated location of NetApp snapshots report in section 4.5.2.1 3. Updated section 16.2.1.3 with table detailing which group memberships are used on NAS
01-03-05	3.16	1. Added section 16.4 on NAS Information Security 2. Added section 16.2.2 on use of administrative protocols: SSH and HTTPS 3. Added section 16.2.1.4.1 regarding the use of TAS as global hardware repository
04-04-05	3.20	1. Updated the CVS section to include the procedures as an attachment. 2. Updated to the ENI Entitlements section to refer to the CVS section.
26-04-05	3.21	1. Added section on segregation of duties for the NAS platform
15-06-05	3.23	1. Added a section on NAS Roles and Responsibilities.
27-06-05	3.24	1. Updated all links and document locations 2. Added Maker Checker Process for VT tickets.
11/07/05	3.25	1. Added section 9.8 DPC Non Supported
02/08/05	3.26	1. Updated the embedded document in the changes section.
30/08/05	3.27	1. Clarified the section on the Independent Review of Filer Audit Logs.
27/10/05	3.29	1. Updated section on Post-implementation under Change Management 2. Added section on Pre-implementation under Change Management.
27/10/05	3.30	1. Added section on TEARS event justification & reconciliation 2. Server Security Configuration Review 3. Server Critical File Management Review 4. Enterprise Security Monitoring - Further Reading
2/11/05	3.32	1. Updated ESM justification section
09/05/06	3.33	1. Updated all links and document locations
10/08/06	3.34	1. Updated section 9.5 Modifying the Authorised Administrators Table
04/09/06	3.35 Draft	1. Split WINTEL PCM creating separate PCM's for NAS and WINTEL
28/12/06	3.36	1. Updated draft to make final document
03/05/07	3.36	1. Corrected hours of work
20/06/07	3.37	1. Removing AV Scanners 2. Updating links 3. Adding additional audit check to process
29/06/07	3.38	1. Added decommissioning of NetApp devices section
06/08/2007	3.39	1. Added section 6.6 on Quotering for Hungary and dealing with Virtual Requests
12/08/08	3.39.1	1. Updated vscan mandatory_scan option to be set to off. 2. Added vscan abort_timeout option to be set to 45 seconds
21/12/08	4.0	1. Updated team structure after TI Re-Org
19/05/09	4.1	1. Updated new team Structure after latest re-org 2. Updated dual control password as controlling team has changed.
11/06/09	4.2	1. Added new section "Implementing NetApp Filers" 2. Added new section "Functional Accounts Not Owned by ENI"
22/09/09	4.21	1. Updated section "ENI NAS Filer Responsibilities" with rules of snapshot management on deduplication enabled volumes.
14/10/09	4.3	1. Added "Non EERS Entitlements" and "EERS Entitlements" sections under "Entitlement Reviews"
02/12/09	4.31	1. Amended Org Chart
18/05/10	4.32	1. Amended Org Chart

Introduction

1.1 Purpose of Document

This document contains procedures for the EMEA NAS Infrastructure SA team, which are part of EMEA NAS & Mainframe Storage Management, within Datacenter Product Support, under EMEA Datacenters.

This document is regularly reviewed and updated when there have been changes within a policy or a new procedure has been inserted.

This and all other documents referred to or attached are classified as INTERNAL.

1.2 NAS Infrastructure Operations Group Overview

EMEA NAS Infrastructure is part of EMEA NAS & Mainframe Storage Management within the Datacenter Product Support Team, a member group of EMEA Datacenters, is a technology infrastructure support function that primarily offers a service to manage & maintain the NetApp (Network Appliance) Filers for EMEA.

The environment consists of Network Appliance filers running ONTAP operating system. All systems comply with Global Distributed Storage Engineering standards and meet the expectations outlined by CITMP.

EMEA NAS Infrastructure is managed by Paul McInerney (x66659, Paul.McInerney@citi.com). Datacenter Product Support is managed by Mike Styles (x53090, Michael.Styles@citi.com).

1.3 Management

DC PSG (Data Centre Product Support Group) has 7 sub-divisions, as follows.

EMEA NAS & Mainframe Storage Management

EMEA Distributed Storage

EMEA Middleware

EMEA DBA

EMEA Regional Backups

Storage Optimization

Financial Billing

The table below identifies PSG sub-divisions, along with Managers.

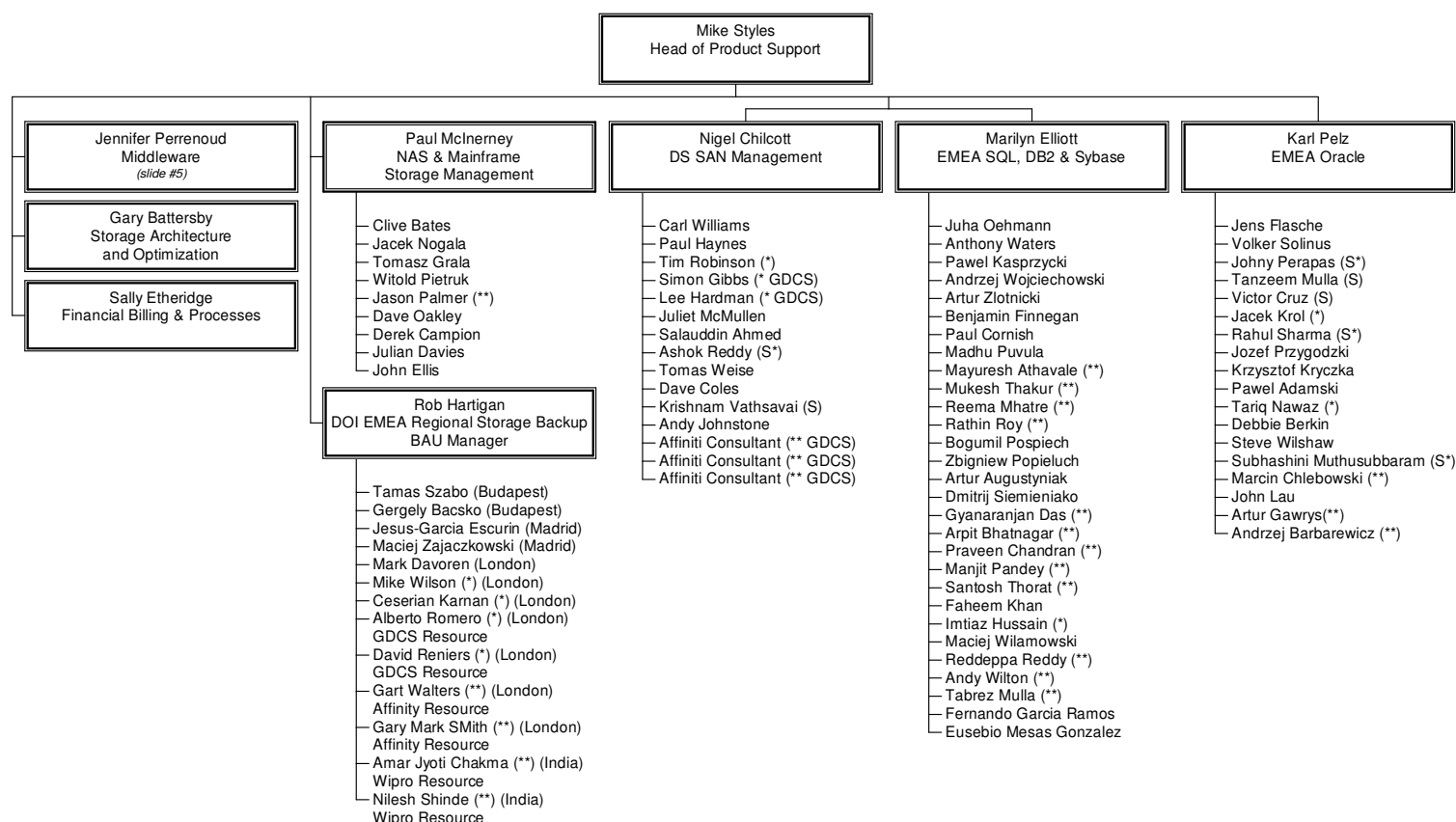
EMEA NAS & Mainframe Storage	EMEA Distributed Storage	EMEA Middleware SA's	EMEA DBA SA's	Storage Optimization	Financial Billing
Paul McInerney	Nigel Chilcott	Jennifer Perrenoud	Marilyn Elliott	Gary Battersby	Sally Etheridge

1.4 Client Base

The client base for the Data Centre Product Support sub-divisions vary:

EMEA NAS Infrastructure SA – European SA Community

The below organisational chart shows this structure and helps clarify where EMEA NAS Infrastructure fits in.



1.5 Role

BAU Technical Assistance EMEA NAS Infrastructure SA

Ownership & management of NetApp Filer (NAS Storage) for the EMEA region

1.6 Location & Contact Details

The EMEA NAS Infrastructure SA team is located at 2 sites across EMEA, London and Warsaw.

The London team are on the 2nd Floor, Riverdale House, Lewisham, London.

The Warsaw team are in Room 1-048, 1st Floor ul. Goleszowska 6, 01-249 Warszawa.

Name	Position	Telephone
Paul McInerney	EMEA NAS Infrastructure (LDN)	X66651
Clive Bates	EMEA NAS Infrastructure (LDN)	X65859
Jason Palmer	EMEA NAS Infrastructure (NetApp)	X68518
Witold Pietruk	EMEA NAS Infrastructure (WSW)	X2504
Tomasz Grala	EMEA NAS Infrastructure (WSW)	X1023
Jacek Nogala	EMEA NAS Infrastructure (WSW)	X1062

Contact Method	Details
Group Line (Both Teams)	+44 (0)20 7986 4589 x64589
Group Line (Warsaw)	+48 (0) 22 690 1015
Email	*GT EMEA NAS Infrastructure
Intranet	http://Wintelinfraweb.eur.nsroot.net
Virtual Tech Break Fix	EMEA NAS Infrastructure
Virtual Change Group	EGNASSA
Virtual Change Approval Group	EGNASSAM

1.7 Hours of Cover

Monday to Friday, as follows:

EMEA NAS Infrastructure: 8am-6pm (GMT)

Outside of normal working hours (6pm-8am & weekends), critical escalations should be reported to the Citigroup Command Centre on telephone number 020 7986 2020 or x62020.

1.8 Faults & Requests

All faults and action requests to be logged using Virtual Tech and queries sent by e-mail. The team aims to respond to faults in a timely manner. However, it is not possible to pre-determine the expected resolution or completion time of a fault or request as all faults and requests vary in nature.

1.9 Shared Group Data

There are a variety of sources of information maintained by the group.

These are as follows:

- H Drive for group information. The H Drive will be the primary location for any specific documentation that an Analyst may require.
- Shared Public Folder location for support contact information, shared calendars, etc.
Available to all members of the group:
[Outlook:\Public Folders\All Public Folders\Europe\Technology\Data Centre\Data Centre Product Support\EMEA NAS Infrastructure](#)
- Intranet website <http://Wintelinfraweb.eur.nsroot.net>

1.10 Websites

EMEA NAS Infrastructure share the EMEA Wintel Infrastructure website, this can be located at the following URL:

<http://wintelinfraweb.eur.nsroot.net/>

The Continuity of Business is stored in the BCS utility COB Trac.

Controls Verification Systems (CVS) Checks

1.11 Introduction

This section will introduce CITM Policy Standards and Procedures, which define controls to minimize technology risk. Our day-to-day processes are designed to comply with the CITM Standards. In addition to the yearly review of all procedures for compliance with CITM Policy (RCSA self inspection), a series of CVS checks and tasks are carried out as detailed below. These form part of our core procedures.

Tasks centre on ensuring the environment is available and stable.

Some tasks need to be performed on a daily basis whilst others are spread out on a less frequent period.

1.12 Process

This process is detailed in a separate document called "ENI-CVS-003 CVS Step By Step Guide" and can be found in the following location:

<H:\Doc Control Sys\01 Current Documents>

CITMP Introduction

1.13 Introduction

The **Citigroup Information Technology Management (CITM) Policy** outlines a common approach for addressing technology-related risk in Citigroup's operating environments and helps promote process improvement within our team. Organisations must then refine their CITM Policy into standards applicable to their business areas and further broken down into day-to-day procedures, which are compliant with the CITM Policy.

A key requirement of CITMP is that all relevant staff are aware of the policy and follow the standards and processes in their day-to-day operating activity.

1.14 CITMP Levels

1.14.1 Level 1 Policies

The policy breaks down into a 10 key areas which are viewed as high-level corporate policies or Level 1 CITMP's. You can view the CITMP Level 1 policies here <http://www.citigroup.net/citmp/>

1.14.2 Level 2 Standards

Each Business area will then use the Level 1 Policies to prepare standards applicable to their environment. These are then deemed CITMP Level 2 Technology Standards and encompass the 10 control areas mentioned within the Level 1 documents. You can view the CITMP Level 2s here <http://www.citigroup.net/citmp/>

1.14.3 Level 3 Procedures

The Level 2 standards apply across the business. Each group or team should ensure that they are compliant with the Level 2 standards. To this effect, Level 3 procedures are designed which encompass day-to-day activity for the group or team. These are functional Level 3 procedures and may extend across a number of groups. For example the Change Management Level 2 Standards give rise to a Regional Level 3 Change Management procedure, which is applicable to all groups and teams.

1.15 Review of Level 3s and RCSA

As part of our review of all procedures and policies and our compliance with Level 2 standards, RCSA must be completed each quarter. This is based on the Level 2 Standards and used to test our day-to-day procedures (Level 3s) against the Standards.

RCSA is a self-inspection test to verify that the controls are adequate, documented and followed within our Level 3 procedures.

EMEA NAS Infrastructure CITMP information, including completed RCSAs are available from the group drive under the audit folder.

1.16 Presentations

Two useful online presentations on the RCSA exercise are available online.

In case the source changes, please visit <http://www.citigroup.net/citmp/> and use the menu system to locate pages referencing RCSA.

RCSA Overview:

<http://www.citigroup.net/citmp/>

RCSA Training:

<http://www.citigroup.net/citmp/>

1.17 Applicability

The CITM Policy requires organizations to establish and maintain documented processes. Each organization must review the effectiveness of those processes on an annual basis and update them as necessary.

The following section contains statements and procedures in relation to CITM Policies for 2003.

CITM Policy	Applicability to EMEA NAS Infrastructure
Change Management	Applicable
Resource Management	Applicable
COB	Applicable
Information Security	Applicable
Problem Management	Applicable
Internet Management	Not Applicable
Architecture	Not Applicable
Outsourcing/vendor management	Not Applicable
Project Management	Not Applicable
Software Management	Not Applicable

The remainder of the document will be arranged under the relevant headings of the applicable CITM Policy.

Resource Management

The purpose of this section is to provide a centralized NAS Infrastructure section within the ENI PCM. Development on this section is currently on going.

1.18 Roles and Responsibilities

1.18.1.1 ENI NAS Filer Responsibilities

Although this is not an exhaustive list, the EMEA NAS Infrastructure team's responsibilities specific to Filer are as follows:

- Managing the devices ensuring that they are available and serving data.
- COB invocation (testing and real). Any planning for business testing will need to be completed by the BCS (Business Continuity Services) teams.
- Performing daily checks on the devices, consisting of the following:
 1. Checking the event logs for any errors.
 2. Ensuring the Snapshots complete and do not overrun their respective disk space limits:
 - on volumes with deduplication enabled and snap reserve set to 25%: snapshots should not exceed 80% of snapshot reserve,
 - on all other volumes: snapshots should not exceed snapshot reserve (15% or 20% depending on volume configuration).
 3. Ensuring that the Snapmirror's complete and that the lag times do not exceed the set thresholds.
 4. Daily MIS reporting on Filer status. (This will be part of the daily check report).
- Manage any support cases with the vendor Network Appliance ensuring satisfactory problem resolution.
- Identify and manage any failed disks. This will involve correctly identifying the failed disk and raising the necessary VT tickets and Virtual Change requests to the local support groups to replace the disks.
- Entitlement review of local accounts.
- Ontap upgrades.
- Volume creations.
- Qtree creations.
- Managing the expansion projects ENI will be responsible for:
 - All project office documentation (Design, CDA).
 - Completing the disk space expansion calculations based on growth trending etc.
 - Co-ordination with Vendor for delivery, installation and base configuration.
 - Software configuration.
 - Ensuring full production status for the devices (Monitoring, TAS / Aperture etc)

1.18.1.2 Data Owners NAS Filer Responsibilities

The local SA's will be responsible for performing the following tasks:

Data management at the Qtree level, consisting of the following:

1. Managing of the WebAdmin structure ensuring production and COB configurations are correct and current.
2. Adding the WebAdmin resources to the NAS Filers (Drives etc).
3. Data migrations.
4. Managing disk space allocations to the business users.
5. NTFS Permissioning for user and shared data areas, including bi-yearly entitlement reviews.
6. Creation of user and group shares.
7. Ensuring segregation on data volumes i.e. ENI do not to have access to business data.
8. Space reporting and management at the Qtree level.
9. Requesting qtrees / data to be backed up or restored including retention times.
10. Tape management for the backup of the Filers.
11. Assisting with local access for Vendor's in the event of any problems for Regional remote sites
12. Providing justification to ENI for disk space expansion.

1.18.2 NAS Filer Expansion

1.18.2.1 Overview

Due to the complexity and time taken to gain the approvals this is normally only undertaken once per year, but the methodology outlined below can be utilised at any stage.

This will also be limited to what ENI perform and not what is expected from other teams, for example Backup Infrastructure or Business Aligned SAs.

The process used can be broken down into the following steps:

Project initiation.

Budget forecast.

Businesses aligned SAs requested for details of disk space required.

Data analysis.

Required disk space is agreed.

These are discussed in detail below:

1.18.2.2 Project Initiation

At the start of the project, the first step is to initiate the project with the London Project office. This is to ensure that the whole process will be managed by one of the project office managers who will ensure that all the necessary streams are included in the project and that the proper SILC process and documentation is followed.

1.18.2.3 Budget forecast

Each year as part of the TI budget process, a Level 0 amount is factored in to cover the expansion of the London NAS environment. This figure is based on trending and growth.

1.18.2.4 Businesses aligned SA's requested for details of disk space required.

ENI contact the business aligned SA community to request disk utilisation information for the Wintel platform. This is then used with disk utilisation information for the NAS environment to ascertain the current disk utilisation. With this request a standard email is circulated to ensure that the data returned is correct.

1.18.2.5 Data Analysis.

Once the data has been collated this is then analysed with the previous years data to determine the following:

Percentage BAU growth over the past year.

Projected percentage growth to the expected delivery date (due to length of project).

Exceptional growth (including any project requirements).

These figures are then fed into a spreadsheet to assist in the analysis of this data and to produce the final required figure across all businesses in London.

1.18.2.6 Required disk space is agreed.

When the final figure for each of the business's growth is obtained, this is then fed back to the Business aligned SA's for their agreement. Once this is agreed the project office SILC process is followed, utilising their project managers to co-ordinate with the various streams etc and using the formal documentation to present and justify the MTE.

1.18.3 Filer Business COB Testing

1.18.3.1 Overview

At the business request the ENI team will facilitate the failing over of the business volumes / vfilers to the disaster recovery Filers. Once the testing has been completed, the data will be copied back to production and the production volumes brought back online.

1.18.3.2 Performing the Testing

The following steps need to be followed to ensure that the testing can be performed and that the integrity of the Filers can be protected:

1 Week before the test a maintenance change must be raised in Virtual Change, unless the business have already created a change request which covers the failover of the volume(s) / vfiler(s).

On the test morning the following tools can be used to generate the scripts required for volume failovers:

- H:\Software\Tools\NetApp Batch Tools\COB Tools\cifs.vbs (This is to generate the updated cifsconfig_share.cfg files).
- H:\Software\Tools\NetApp Batch Tools\COB Tools\COBcmds.vbs (This is used to generate the steps required for the testing).

If the failover involves vfiler then the following scripts would be used:

- H:\Software\Tools\NetApp Batch Tools\COB - NFS vfiler Scripts\Template\SetVariables.cmd (Set required variables to be used by the main script, enter these values relating to the vfiler being failed over to COB)
- H:\Software\Tools\NetApp Batch Tools\COB - NFS vfiler Scripts\Template\failover.cmd (Main script which controls the failover referencing previously set variables)
- H:\Software\Tools\NetApp Batch Tools\COB - NFS vfiler Scripts\Template\drfile.exe (Modifies the rc and snapmirror.conf files)
- H:\Software\Tools\NetApp Batch Tools\COB - NFS vfiler Scripts\Template\timeout.exe (Allows a timed pause within main script)

Open the EMEA NAS Infrastructure conference line.

Follow the steps generated by the above script for non vfiler volumes, while the vfiler script runs automatically.

- 10 Minutes - EMEA NAS Infrastructure (ENI) to mail the relevant audience to advise them that the volumes / vfiler on the production Filers are about to be stopped, rendering them inaccessible. Any staff that have files on these volumes / vfiler still open and unsaved, must save their work and close these files immediately, as otherwise when the volumes / vfiler are taken down, any unsaved work will be lost.
- 1 Hour - ENI to bring down the production volumes and to begin work on bringing on line volume / vfiler on the DR partners.
- ENI to mail the relevant audience to advise them that the relevant volumes / vfiler on the DR partners are on line and work can recommence. Staff who were already logged in, must logout and log back in to allow their drive mappings to reconnect to the DR partners. At this stage, any issues connecting to drives, should be reported to BCS. A conference line will be open for the duration of the COB test.
- Test Ended - ENI to mail the relevant audience to advise them that volumes / vfiler on DR Filers are about to be stopped, rendering them inaccessible. Any staff that have files on these volumes still open and unsaved, must save their work and close these files immediately, as otherwise when the volumes are taken down, any unsaved work will be lost.
- ENI to bring down volume / vfiler on the DR partners and to commence to copy back from the DR partners to the Production volumes any files that were changed on the DR volumes, overwriting the previous copy held on the Production volumes. Once the copies have completed, ENI to begin work on bringing on line volumes / vfiler on the Production Filers.
- ENI to mail the relevant audience to advise them that copies have completed and that volumes / vfiler on the production Filers are now back on line. Staff who were already logged in, must logout and log back in to allow their drive mappings to reconnect to the Production Filers. At this stage, any issues connecting to drives, should be reported to BCS. A conference line will be open for the duration of the COB test.

1.18.4 Filer Password Age Control

1.18.4.1 Overview

A compensating control has been developed to cater for the fact that the Network Appliance Filers do not support password aging. The compensating control is based on a scripted solution that scans the list of Filers for user accounts and calculates the password age based upon the date. The script adheres to the following rules:

NetApp local SOE ID operator accounts are 7 characters in length

NetApp local operator accounts must undergo a password reset activity every 45 days

NetApp local operator accounts should be marked for deletion after 75 days of inactivity

NetApp local functional IDs must undergo a password reset once a year

Each local account operator will receive a warning mail everyday their account has a password age greater than 45 days

Each local functional ID which has a password age greater than 365 days will send a warning email to the support group for everyday the account has passed this threshold

Each day, a summary report should be produced listing all accounts that do not have a nominal account status.

The repository must maintain accurate account information even when the remote scanning target is not contactable or inaccessible due to permission denied issues

The script must warn if the scan of a particular device is taking longer than 10 seconds

The repository should maintain a record of account information even when the remote scanning targets are temporarily removed from the target list

This script is scheduled to run nightly @ 04:30.

Full details of this can be found in the following document:

<H:\Doc Control Sys\Documentation\NetApp Filer>Password Age Control\NAPAC1-2.doc>

1.18.4.2 Actions to be taken:

1.18.4.2.1 *Summary Mail*

For the summary mail, depending on the status action may be required:

- Expired accounts (45 days < age < 75 days)
No action required if there are accounts listed here as this is within the normal password expired time frame
- Inactive accounts (age > 75 days)
The individuals with the accounts in violation need to be contacted and ensure that the passwords are changed or if this is not possible arrangements need to be made to have the accounts removed from the Filers listed and other Filers.
- New user accounts created since last scan
For any new accounts created, these need to be investigated and reconciled to a request and appropriate approval to ensure that these were valid actions.
- Suspect records (in repository)
No action required by independent reviewer. These will be investigated by the Filer SA's
- Password scan overruns (devices taking > 10 secs to scan)
No action required by independent reviewer. These will be investigated by the Filer SA's
- Un-contactable / permission denied hosts
No action required by independent reviewer. These will be investigated by the Filer SA's

1.18.4.2.2 *Individual Violation Emails (CC'd)*

- For all violation e-mails sent out to the individual SA's, the following is required:

- Password age is < 75 days.

No action required by independent reviewer.

- Password age is > 68 days.

A reminder mail needs to be sent to the individual reminding them to change their password.

- Password age is >= 75 days.

The individuals with the accounts in violation need to be contacted to ensure that the passwords are changed or if this is not possible arrangements need to be made to have the accounts removed from the Filers listed and other Filers.

1.18.5 Filer Audit Logs

1.18.5.1 Overview

A compensating control has been developed to cater for the fact that the NetApp (Network Appliance) Filers do not support the independent reviewing of the Audit Logs. The compensating control is based on a scripted solution that extracts any changes to the audit logs and then summarises any changes on a daily basis. The summary is then e-mailed out to the group distribution list and to an independent reviewer. The script adheres to the following rules:

Audit log retrieval should execute every 30 minutes to ensure all events are retrieved
 Each day, a summary report should be produced listing all non-prejustified events
 The repository must maintain accurate account information even when the remote scanning target is un-contactable or inaccessible due to permission denied issues
 Critical events are deemed as leading to a loss of data access (for example: halting the storage device or terminating the CIFS emulation service)
 Warning events are deemed as leading to a degradation in service offering (for example: turning off ndmpd or stopping the block level contingency copies)
 Log files that have been deleted must be flagged as suspicious events
 Verbose audit logs will rollover to a new log file. The script must capture the tail of the incremented log file and the header of the new log file

This script is scheduled to run as per the following schedules:

Every 30 minutes

Nightly @ 01:00

Full details of this can be found in the following document:

<H:\Doc Control Sys\Documentation\NetApp Filer\Audit Log Reviews\NAALRARS1-0.doc>

In addition to this, ENI have set auditing on the audit logs to ensure that these cannot be tampered and a script is run on a daily basis to confirm that the logs have not been manually amended. The process is as follows

- Verify that the filerlist is up to date and includes all managed devices - reconcile differences and rectify any issues found. The filerlist is reconciled against a Monthly CVS check "Scheduled Scripts Filer List Reconciliation" to ensure that it is up to date.
- A scheduled script (comit_alf.cmd) will generate a list of Filers where vol0 permission settings do not match for 3 key directories on each filers vol0 - output will be written to the group drive
- Corporate Wintel NT SA's examine the output of the script daily and highlight any exceptions that need to be rectified
- ENI script to commit all CIFS Audit events to the .evt file in the /vol/vol0/AuditLog directory and produce an extract of the events from the messages file for collection by Corporate Wintel NT SA to verify

Corporate Wintel NT SA's script will collect and manage all .evt files generated and review events where ownership and/or permissions change and request justification to ensure the integrity of the .evt files generated.

A copy of the comit_alf.cmd script is located in the following location:

[\\dnctisadfm001\d\\$\Scripts\CVS - AuditLog](\\dnctisadfm001\d$\Scripts\CVS - AuditLog)

NB: Switzerland – Due to local data laws the Swiss NAS Filers are attached to the Swiss Secure Domain, with 2 vfilers in EUR.NSROOT.NET. Due to this there is a separate Audit Log Script that is run locally from ZRHCTINASSA001 and the report that is generated has the suffix "-ZRH" at the end of the subject line.

1.18.5.2 Independent Review

1.18.5.3 Overview

The independent reviewer needs to review the Audit Logs email that is sent out and ensure that all action taken on the filers that can be defined as a change to the system has a valid request associated with it (Virtual Change or Virtual Tech).

1.18.5.4 Actions to be taken:

Audit Log review mail is generated and emailed to NAS management and to the Independent reviewer on a daily basis.

NAS event Log reports all events or activities performed on the filers. The events can be categorized in three categories:

- Informational task – These represents commands, which are used to check status (volumes, snapshots etc) or options set on a filer (examples include – snapmirror status, df -g, vol status etc)
- Warning – Events are deemed as leading to a degradation in service offering (for example: turning off ndmpd or stopping the block level contingency copies)
- Critical - Events are deemed as leading to a loss of data access (for example: halting the storage device or terminating the CIFS emulation service)

All the events representing the Warning or Critical commands executed on a filer are identified with either Yellow or Red flags. NAS event Log is reviewed to verify that only authorized NAS SA's and business system administrators have executed changes on a filer and that there is a valid request for the action taken (Virtual Change or Virtual Tech). The notification mail must be reviewed within one week of receipt.

If a change is identified without supporting documentation, an email is sent to the responsible party requesting justification for the performed change.

Any suspicious activity is reported to Security Incident Response Team (SIRT) following the SIRT process defined in NAS Information Security PCM.

Once the independent reviewer responds with confirmation that all required events have been justified, the email received is kept in the EMEA NAS Infrastructure's shared drive as process evidence, in the following area:

<H:\Reporting\Checks\CVS> then traverse down the folders YYYY / MM / DD

1.18.5.5 Classification of Event

The classification of the events that the audit log script monitors is based around a Audit review perspective and not around the system health one. The reason for this is that this is an audit review and not system health, so for example the addition of a user is classified as critical however a volume add or create is classified as a warning.

The events and their classifications are detailed in the spreadsheet, which can be found in the following location:

<H:\Doc Control Sys\Documentation\NetApp Filer\Audit Log Reviews\Audit Events Clasification.xls>

1.18.6 Provisioning

New system installations basically follow the guidelines and configurations on the Global Distributed Storage Engineering website collated in to the OnTap Solution Guide:
<http://catecollaboration.citigroup.net/domains/platstor/gdse/products/techstdshmpgs/netappfiler.aspx>

However there are a number of configuration options that are specific to the London environment and these are detailed in the following sections.

1.18.6.1 Software and component licensing

1.18.6.1.1 Infrastructure expansion

The London NAS infrastructure has an annual capacity planning cycle where businesses request storage for the forthcoming year and new hardware is purchased on an annual basis. Once the storage requirements have been finalised the order is placed under the Project Office project lifecycle process. Other locations within EMEA provide a justification as and when more space is required.

1.18.6.1.2 Obtaining licenses

Operating system and software licenses are bought as part of the purchase process and incorporated into the purchase order. Once the NAS infrastructure is installed, and the Autosupport feature is turned on (options autosupport.enable on), the NAS Filer will register itself within the vendor's product database. Once the device is registered, a member of ENI should log in to the now.netapp.com website and print out the paper copies of the licenses, by following the procedure below:

- Login to now.netapp.com (see NAS problem management section on obtaining a NOW login)
- From the service and support screen select, under the 'My NetApp Products' section, click the 'My Licenses for Serial Numbers' link.
- Choose criteria to search for (either serial number or system host name) and type the appropriate value in the input box on the screen. Then click the 'GO' button.
- Each license type detail will be returned.
- Click the 'Print' link, found in the 'Action' column for each license.
- An on-line version of the license will load into Internet Explorer.
- From the 'File' menu in IE select the print option to make a hardcopy of the license.
- Do this for each license for each device and file the hardcopies in the NAS license binder that is stored in the ENI desk area
- In addition open the license matrix document found at 'H:\Doc Control Sys\Documentation\NetApp Filer\EMEA NAS Infrastructure Filer Licenses 3.00.doc' and input the license details in the table.

The process outlined above removes the dependency on the vendors website for licensing information, and the hard copies remove the dependency on accessing electronic copies of the documents in the event of a catastrophic systems failure.

If the vendors website is offline, the license key codes can be determined by issuing the 'license' command from the console of each device. However there is no facility to print the hard copy licenses if the vendors website is not available. In this case, the London NetApp account manager should be contacted to instigate a bypass process and produce the license hard copies via an alternate process.

1.18.6.1.3 Additional licenses

Any additional software licenses that are required once the NAS infrastructure is installed should be raised via the appropriate internal purchasing process. Once obtained, the above procedure should be followed to obtain hard copies of the new license keys and the information within the license key matrix must be updated.

1.18.6.1.4 Adding additional licenses

To add an additional license feature to one of the NAS infrastructure devices (once the license has been purchased from the vendor), logon onto the device console and issue the 'license add <code>' command. Replace '<code>' with the actual alpha key code provided by the vendor.

1.18.6.2 Hardware and Software End-of-Life (EOL) management

Both hardware and software used on the EMEA Filers are certified by Global Distributed Storage Engineering. Details of these certifications can be found on the Engineering web site, using the link below.

<http://catecollaboration.citigroup.net/domains/platstor/gdse/products/techstdshmpgs/netappfiler.aspx>

A Vendor EOA list can be found : <http://now.netapp.com/NOW/products/ea/#index>

Hardware Support : Network Appliance will repair or replace all defective Field Replaceable Units (FRUs) for a period of 5 years from the End of Availability date for each hardware product under a current service agreement.

1.18.6.3 Segregation of Duties

In order to meet audit requirements on the NetApp NAS platform, a compensating control has been devised whereby NAS administrators will not have default access to the user data stored on the data volumes.

As such a segregation of roles is achieved so that the NAS Administrators manage the health of the hardware and operating system, including Anti Virus Scanning services, system security and provisioning. Data Administration groups are responsible for the permissioning of data and creating of data shares in the data partitions.

This process is detailed in a the ENI Operational Filer Installation document and can be found in the following location:

<H:\Doc Control Sys\01 Current Documents\ENI Operational Filer Installation v2.0.doc>

1.18.6.4 System volume security (Vol0)

In conjunction with GDSE's secure configuration, the following configuration has been devised and approved for the NTFS security on the system volume (C\$, Vol0) for London Filers.

Four groups have been defined for this function and the roles and requirements are listed in the table below.

Group Name	Members	Purpose
<local>\Administrators	<local>\administrator EUR\app_idn_eni_Per_NetAppAdmins EUR\{reg.code}ctisvcnasav01 EUR\{reg.code}ctisvcnasav02 EUR\ldnctisvcnas01 <local>\cb81537 <local>\pm67350 <local>\jp49700 <local>\tg76015 <local>\jn76047	Provides local administrators account with Full Control management rights over the NTFS on Vol0, and device administration privileges

	<local>\wp92684 <local>\ldnctisvcnas01 <local>\{reg.code}\{bus.code}svcbck01	
EUR\app_ldn_eni_Per_NetAppAdmins	EUR\cb81537 EUR\pm67350 EUR\jp49700 EUR\tg76015 EUR\jn76047 EUR\wp92684	Provides NAS administrators with Full Control management rights over the NTFS on Vol0
EUR\app_ldn_ewi_Per_NetAppAdmins_RO	EUR\ldnctisvcnas01 EUR\ldnctisvcmon01	Provides functional ID read only rights to Vol0 to extract and review the system message and audit logs
NAM\NetApp_Inventory	NAM\srv_nasscripts	Allows functional accounts in this group read only rights to Vol0 for inventory purposes Functional accounts cannot login in to Filer console in non-interactive SSH mode unless a public key pair has been installed on the Filer, thereby maintaining administrative control

1.18.6.4.1 Share level security

Using the NetApp Admin web GUI, the following permissions need to be configured on the C\$ share. From the management home page, select Secure Filerview, and logon to the filer with a NAS Admin local account. In the Filerview menu select CIFS / Shares / Manage and then find the entry for C\$ in the main window. Then click on the Change Access link from the operations column in the table. Click the add access control link and enter the following user/ group details and permissions:

<local>\Administrators	Full Control	(substitute 'local' with the hostname)
EUR\app_ldn_eni_Per_NetAppAdmins	Full Control	
EUR\cti_gb_Per_NetAppAdmins_RO	Full Control	
NAM\NetApp_Inventory	Full Control	

Note: Full Control of CIFS share is required to access this mount point. Read access only allows you to review the share level entitlements, not actually mount the share.

1.18.6.4.2 File system security (NTFS)

The following security permissions need to be applied to the C: drive on the Filer. These permissions should be set so that all child objects inherit permissions from the root. There are a number of exceptions to this rule that are detailed after the following table.

<local>\Administrators	Full Control	(substitute 'local' with the hostname)
EUR\app_ldn_eni_Per_NetAppAdmins	Full Control	
EUR\cti_gb_Per_NetAppAdmins_RO	Read Only	
NAM\NetApp_Inventory	Read Only	

The exceptions to these policies have a copy of the standard permissions listed above with the following changes:
etc\hosts.equiv and etc\inventory.src which require NAM\NetApp_Inventory to have Full Control.

1.18.6.5 Snapshot Configuration

The configuration adopted for the NAS platform in EMEA differ from the recommended settings by GDSE. The details of this is as follows:

GDSE Recommendation			EMEA NAS Implementation	
Snapshot Type	Schedule	Retention	Schedule	Retention
Hourly Snapshots	Every day at 12:00 Noon and 5:00PM	2	Every day at 12:00 Noon.	12
Nightly Snapshots	Monday through Saturday at 12:00AM	22	Monday through Saturday at 12:00AM	12
Weekly Snapshots	Every Week on Sunday 12:00AM	3	Every Week on Sunday 12:00AM	2

These settings have been implemented as an extension to the best practices used at the time for the NAS Filers, whereby daily copies of the data took place from the production devices to the COB devices at midday and midnight. Additionally the system administrators were consulted prior to the implementation of the Filer platform and they all agreed with this principle.

Some EMEA regions have further exceptions due to business requirements, including Germany, Hungary and Poland.

1.18.6.6 Inventory

1.18.6.6.1 TAS Inventory

Prior to the installation and provisioning of new hardware, and as part of the new hardware SILC process, EMEA NAS Infrastructure is required to enter the hardware details into the Global Inventory system (TAS). A single sign-on access is required to the TAS application. TAS can be accessed via the following URL:

https://tas.ny.smb.com/tas/lois_main/LOIS_Home.asp.

Aperture is also now used to control required workflow regarding installation of new equipment in to selected data centres. Not all EMEA data centres are registered in Aperture and where this is the case TAS should be used. Systems entered in to Aperture feed in to TAS once the process is completed. A single sign-on access is required to the Aperture application, and can be accessed via the URL:

<https://aperture.nam.nsroot.net/WAS/SS/AWESS.aspx?x=awe&xcsid=VISTA&xcapp=splash&log=saved>

1.18.6.6.2 WebAdmin Inventory

The following steps are required to add new Filers to the DPC inventories in WebAdmin:

- Copy the inventory source file from [H:\Doc_Control_Sys\Documentation\NetApp Filer\Production Support Manual\inventory.src](#) to etc\inventory.src on each filer you wish to add to inventory
- Ensure the NTFS security permissions are set as described in [1.18.6.4.2](#)
- Log onto the ENI DFM server LDNCTISADFM01 via a terminal server session.
- Browse to D:\apps\apps_srv\Collectors\netapps\1\EU\ and open the file filers2syscollect.txt.

- Insert the names of the new hosts to add to inventory into the existing list. Note that the host names need to have @EU appended to their names so the inventory records are collated into the correct node in WebAdmin. Do not delete the existing hosts as you are appending to the existing inventory.
- Browse to D:\TESTERS\EU on LDNCTISADFM01 and run the command syscollect.cmd from the command line. This will test connectivity and generate the PC Keys for the devices.
- Within WebAdmin select the DPC node netappfilers_eu.ross.eur.dpc and click on Add NAS.
- Enter Filer name and associated PC key from the output file Filers2WebAdmin.EU.NAM.

A full detailed overview of this process can be found at

<H:\Doc Control Sys\Documentation\NetApp Filer\Inventory Process\Citigroup GTAM Inventory Collection Process.doc>.

1.18.6.7 Anti-Virus Installation and Configuration

The Anti Virus Scanners for the NetApp Filers are owned by the EMEA WINTEL Infrastructure team. EWI Install, configure and Support these devices.

Please consult the section within the GDSE OnTap Solution Guide for a full overview of the CTI Anti-Virus solution for NetApp Filers:

<http://catecollaboration.citigroup.net/domains/platstor/gdse/products/techstdshmpgs/netappfiler.aspx>

1.18.6.7.1 Scanning Server Build

For the recommended hardware platform, EWI follow the specifications found on the Wintel Engineering website for NAS Anti Virus scanning servers (see Infrastructure section at <http://www.citigroup.net/tie/de/wintel/standards/hardware/servers/servers.html#standards>).

The operating system and application installation is the same as an SOE print server build, with the exception that the Anti Virus package used during the installation is the McAfee NetShield for NetApp anti-virus product. The wrap is available on GDSGold and is designated **nsna71xx**

1.18.6.7.2 Scanning Functional ID

ENI use functional ID's called EUR\<reg.code><bus.code>svcnasav0*, e.g. ldntisvcnasav01, to perform the anti-virus scanning. This is tracked under the process outline in section 1.39 of this PCM.

The accounts need the following rights in order to perform the scanning process:

- Add functional ID to CIFS local administrators group on each Filer to be managed using the account for that server.
- Add functional ID to local administrators group on each scanning server
- On scanning server, set the *AV Scanner* service to run as the functional ID

1.18.6.7.3 E-Policy Orchastrator (ePO)

The configuration of the Anti-Virus software is achieved through the E-Policy Orchestrator management console. Members of EMEA NAS infrastructure have access to the container Directory\EMEA_Wintel_Infra\EMEA NetApp ePO, where the area is then split in to Country, Region, Scan Group. However, a request to EISS is required to initially move the new AV scanning server to this location. Configure the Scan Group with the Filers to be scanned and move to required AV scanning servers to the Scan Group.

Once completed, verify the scanning server have received the assignments from the EPO server.

1.18.6.7.4 Filer Configuration

To complete the configuration, log onto the console of the filer and issue the following commands for the host filer and all vfilers:

- Vscan options timeout set 45
(required for successful scanning of .xla files and other large files)
- Vscan options mandatory_scan off
(disables mandatory scanning)
- Vscan options abort_timeout set 45
(sets the filer to abort the vscan request after 45 seconds, to resolve possible issue of user applications hanging due to the av scanner having scanning issues)
- Vscan
(to confirm the scanning servers that are registered with the filer)
- Vscan options use_host_scanners set on
(only to be performed on vfilers, configures the vfielrs to use the AV Scanners registered with the host Filer)

Once complete and verified, the anti-virus scanning can be enabled by issuing the following command:

- Vscan on

This completes the configuration of anti-virus on the Filer platform.

1.18.7 Administrative protocols

Where at all possible, administrators should ensure that connectivity to the NAS Filers is achieved via SSH or HTTPS (SSL). This will ensure that all passwords and commands travel over the network in an encrypted state.

The console port should only be used when connectivity via the device network ports is not possible, or an administrator needs to reboot a NAS device and needs to monitor the boot sequence. The console port should be used sparingly because the Telnet protocol is used to connect to the Cisco terminal server (inter-mediatory to the Filers console port), and therefore commands and passwords are transmitted over the Citigroup network as clear text.

1.18.7.1 Centralised management server

ENI has two centralised management servers for NAS (one production and one contingency). These server allows non-interactive SSH2 sessions to be run against the London NAS Filers. The procedures in this section outline various management processes than apply to these management servers.

1.18.7.1.1 Adding a new management server

This section describes the steps involved in building and commissioning a new management server to integrate into the existing EMEA NAS infrastructure. This would be installed by EMEA Wintel Infrastructure and is only detailed here for information only.

- Build a Windows server to the latest SOE build standard (similar hardware standard requirements are an entry level web server). Ensure the build process includes the creation of a D: data partition to store the SSH keys.
- From the console (not by terminal services), SPAC package TCCL4430 (or above) onto the management server.
- Once the SPAC is installed insure that the SOESSHD service is stopped, and the startup parameter is set to disabled. This will ensure no one can SSH to the management server.

1.18.7.1.2 Decommissioning an old management server

This section describes the steps involved in decommissioning an old management server. This activity needs to be conducted on every NAS Filer for every administrator that possessed SSH2 rights to that device.

- Browse to the file `c$\etc\sshd\<soe_id>\.ssh\authorized_keys` on every filer.
- Open the file in a text editor and delete the line in the `authorized_keys` file that relates to the management host you wish decommission.
- Repeat this step for every SSH administrator on each Filer
- Follow the steps in section 1.18.7.1.5 (Deleting an SSH user from the management server) for all user profiles, to ensure all private keys are deleted from this management server.

1.18.7.1.3 Adding a new SSH2 user to the management server

This section describes the steps involved in generating public and private SSH keys for each new SSH user. This SSH user must have a local account on each NAS device in order to authenticate with it, and rights to terminal server to the management server. This process must be conducted on each management server because the keys record a unique user ID / host name combination pair.

- Logon to the management server via a terminal server session
- `START > Run > CMD`
At the command prompt browse to the directory `C:\APPS_SRV\SSH Communications Security\SSH Secure Shell` and issue the following command, and press ENTER:
`ssh-keygen2.exe`
- You will be prompted to enter a catch phrase, it is recommended to leave this blank.
- Once complete the public and private keys will have been created in the location `c$\Documents and Settings\{SOE ID}\Application Data\SSH\UserKeys`.
`id_dsa_2048_a` (Private key)
`id_dsa_2048_a.pub` (Public key)
- Browse to your key store directory on the management server. You should find it at `c$\Documents and Settings\{SOE ID}\Application Data\SSH\UserKeys` on the management server. Modify the NTFS security on this directory and all sub-directories so that only you have access to this directory tree. Keys are private to you and should not be available to any other users. Ensure that local administrator and administrators group are also removed from the permissions.
- Run the following command from this directory to convert your TecTia formatted public key to an OpenSSH format the Filer can understand.
`ssh-keygen -i -f id_dsa_2048_a.pub >> authorized_keys2`

1.18.7.1.4 Adding an SSH user to a new management server

This section describes the steps involved in generating public and private SSH keys on a new management server. The procedure is exactly the same as listed in the previous section, but in this instance every Filer administrator will have to generate a new key on the new management server. This process must be conducted on each management server because the keys record a unique user ID / host name combination pair.

1.18.7.1.5 Deleting an SSH user from the management server

This section describes the steps involved in removing public and private SSH keys on a management server. You will have to perform this activity on each management server on which the SSH user has been configured.

- Browse to your key store directory on the management server. You should find it at `d$\data\home\` on the management server.
- Look for the directory named after the SOE ID of the administrator whose keys you are trying to delete
- Delete the directory and all subdirectories to remove the public keys

- Browse to c\$\Documents and Settings\{SOE ID}\Application Data\SSH\UserKeys and delete all files.
- Do this step on each management server

1.18.7.1.6 Adding a new SSH user to a NAS Filer

This section describes the steps involved in adding public SSH keys to each NAS Filer. This SSH user must have a local account on each NAS device in order to authenticate with it, and CIFS administration rights over Vol0 in order to install the public key. If you have multiple management servers you need to take the unique public key from each server and add it to the authorized keys on each NAS Filer.

- Browse to your key store directory on the management server. You should find it at c\$\Documents and Settings\{SOE ID}\Application Data\SSH\UserKeys\authorized_keys2 on the management server. Open the file with a text editor and copy the first line. The encryption key will start "ssh-dss".
- Browse to Vol0 on the target NAS Filer and navigate to: C\$\etc\sshd\
- Create a directory named after your SOE ID
- Then create a sub directory called ".ssh"
- Then create a file called "authorized_keys" (note no file suffix)
- Open the file in a text editor and paste the encryption key you copied in the first step
- You need to paste in each unique public key combination to this file. Therefore you should do the same process on the contingency management server and append the public key to the second line of the "authorized_keys" file.
- Save the file

1.18.7.1.7 Adding SSH users to a new NAS Filer

This section describes the steps involved in adding public SSH keys to a new NAS Filer. This SSH user must have a local account on each NAS device in order to authenticate with it, and CIFS administration rights over Vol0 in order to install the public key. If you have multiple management servers you need to take the unique public key from each server and add it to the authorized keys on each NAS Filer.

- Browse to Vol0 on an existing NAS Filer and navigate to: C\$\etc\sshd\
- Copy the directory named after your SOE ID
- Browse to Vol0 on the new (target) NAS Filer and navigate to: C\$\etc\sshd\
- Paste in the directory you copied

1.18.7.1.8 Deleting an SSH user on a NAS Filer

This section describes the steps involved in deleting a public SSH key to a NAS Filer. This process should be conducted when a NAS administrator leaves the EMEA NAS Infrastructure group. This process needs to be conducted on each NAS Filer on which the administrator has non-interactive SSH access.

- Browse to Vol0 on each NAS Filer and navigate to: C\$\etc\sshd\
- Look for the directory named after the SOE ID of the administrator whose keys you are trying to delete
- Delete the directory and all subdirectories to remove the public keys
- Do this step on each NAS Filer

1.19 NAS Management

1.19.1 Network Appliance Installation Process

The full build and commissioning process for the NetApp Filers is documented separately. This document can be found here:

<H:\Doc Control Sys\01 Current Documents\ENI Operational Filer Installation v2.0.doc>

1.20 Netapp Filer resource assignment

The term 'Resource' in the context of Filer resource assignment refers to the assignment of drive/shares to Netapp Filers within Webadmin.

1.20.1 Webadmin 3.x

Webadmin 3.x users native active directory ACL'S to manage the Netapp Filer server objects. The server objects for the Netapp Filers are located in the following OU:

OU={Country_code}OU=Servers,OU=app_ldn_eni,OU=app_ldn,OU=app_gb,OU=app,DC=eur,DC=nsroot,DC=net

The standard Webadmin 3.x administration groups provide for server administrators to carry out daily tasks. Unfortunately this includes deleting the server object which would result in the Filer being removed from the domain. In order to grant the rights to only update the resource assignments, a security group has been defined along with non-standard ACL's that are applied to the OU holding the Netapp Filers. These details are as follows:

Security group: CN= app_ldn_eni_Per_{country_code}_NetApp_Resource_Assignment,OU=Dept_Grps,OU=app_ldn_eni,OU=app_ldn,OU=app_gb,OU=app,DC=eur,DC=nsroot,DC=net

ACL's applied to EUR\cti_gb_Per_Netapp_Resource_Assignment to Netapp Filer server OU:

Permission	Applied to
Read All Properties	Child objects only
Read/ Write SOE Resources	Child objects only

Change Management

1.21 Introduction

Change Management is the process used to plan, schedule, apply, distribute and track changes. An effective change management process ensures the integrity and reliability of the environment while maintaining the pace of change required by business needs. (Stated in CITM Policy Change Management Level 1).

Change Management procedures for Level 3 are regional and are referred to by EMEA NAS Infrastructure and can be found by using the following link.

<https://globalconsumer.collaborationtools.consumer.citigroup.net/sites/CTI-EMEA-Service-Support/ChangeMgmt/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2fsites%2fCTI%2dEMEA%2dService%2dSupport%2fChangeMgmt%2fShared%20Documents%2fProcedures%20and%20Help%20Guides&FolderCTID=&View=%7bD29C592E%2d01B7%2d428A%2d8F9A%2dA41D30F0FC77%7d>

EMEA NAS Infrastructure make use of the Virtual Change management system as defined in the regional Level 3 procedures.

The Virtual Change Classes for the group are defined as follows:

Approvers		Members	
Manager	EGNASSAM	EMEA NAS Infrastructure Management	EGNASSA

1.22 Virtual Change Getting Started

1.22.1 Account Request

EMEA NAS Infrastructure members have valid Virtual Change User Id's.
Access via single sign on.

1.22.2 Password Resets

Access via single sign on.

1.22.3 Change Matrix

The link below is to a document, which details which procedures require a change request to be submitted what type it should be raised as:

<H:\Doc Control Sys\01 Current Documents\ENI Changes Matrix.xls>

1.23 EMEA NAS Infrastructure Procedures

The following document forms part of our change management procedures and is based upon the existing 3 regional change management document.

<H:\Doc Control Sys\01 Current Documents\ENI Virtual Change Procedures v2.doc>

1.24 Pre-Implementation checkout

All changes flagged for implementation are entered into the EMEA NAS Infrastructure weekly team agenda and reviewed. Any issues are recorded in the minutes from the meeting.

1.25 Post-Implementation checkout

All changes flagged for implementation the previous week, are entered into the EMEA NAS Infrastructure weekly team agenda and reviewed. Any issues are recorded in the minutes from the meeting.

After a member of EMEA NAS Infrastructure has implemented a change the following procedure is used to check the result of the change and notify the requester of the outcome. If there are

production issues with the change that has been implemented, then the requestor will be notified.

It is the responsibility of the change owner/implementer to close the Virtual Change record as detailed in the ENI Virtual Change Procedures v2.doc.

<H:\Doc Control Sys\01 Current Documents\ENI Virtual Change Procedures v2.doc>

1.25.1 Green Zones

All scheduled changes are raised to occur during designated "green zones", a mutually agreed time with the business when risk to the business is low.

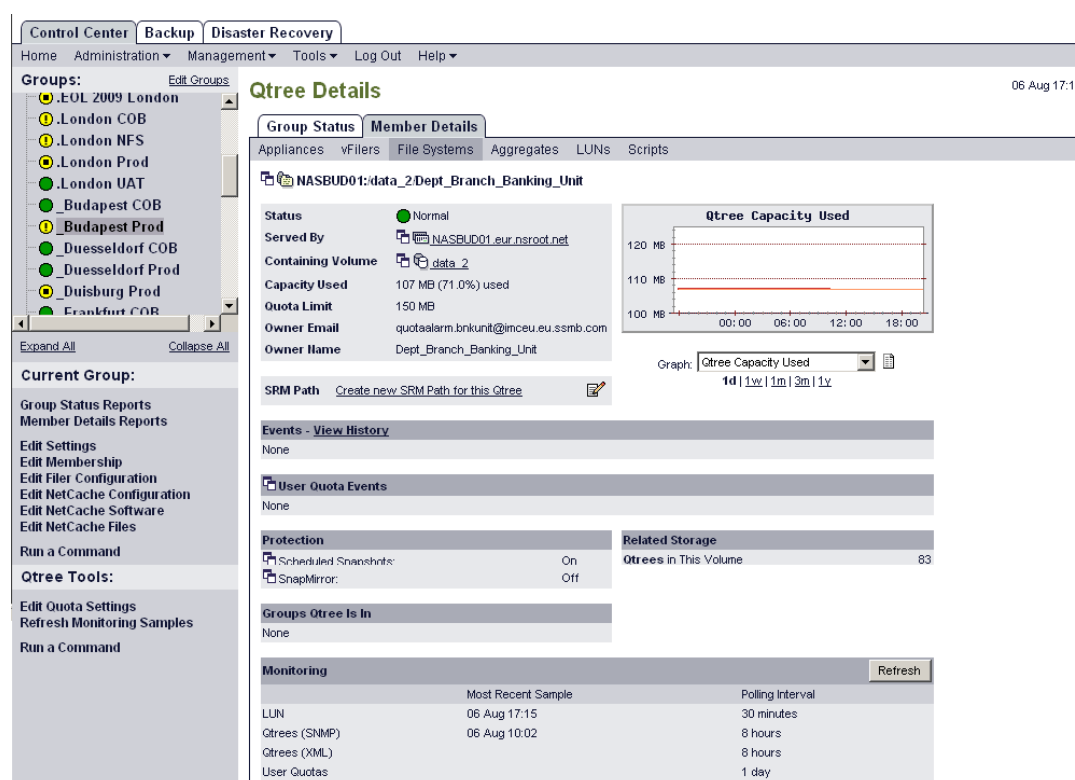
1.26 Virtual Requests

1.26.1 Hungary / Poland and Quota Changes

At present, the majority of VR's coming through into the EMEA NAS Infrastructure Queue are to do with Hungary / Poland and Quota's on NASBUD01 and NASBUD02 / WSWCTINAS201A and WSWCTINAS201B.

Typically, Quotas are monitored via DFM, which can be found as follows:

<https://dfm.eur.nsroot.net/dfm/report/suite> (an example of a Qtree quota is shown below)



You can edit an individual Qtree quota by clicking on "edit quota settings" in the above screenshot, which may be relevant to the VR as this is where you edit the email contact setting to alert when the quota has been exceeded. This is done on an individual Qtree basis.

1.26.2 Checking the VR queue

Any quota requests will be obtainable from our VR queue

My Tickets	My Group Tickets	My Tasks	My Requests	My Group Requests	My Projects
Ref #	Item(s)	Created By	Due Date	Status	Assigned To
VR1766744	Change Disk Quota	Zsuzsanna Feher	8/7/2007 11:13:00 AM 0d 6h 0d 6h	Approved	EMEA NAS Infrastructure
Justification Please decrease home_lafi quota by 2 GB because of an employee (tt02635)leaving, and his date moved from here.					
Results: 1					
1					

1.26.3 Decreasing a quota

The following steps are performed to decrease a quota file. This is so we can keep track of what quota changes have been made and to ensure an excessive amount of requests does not place a strain on the ENI Team.

1.26.3.1 Step 1 - Confirm Change

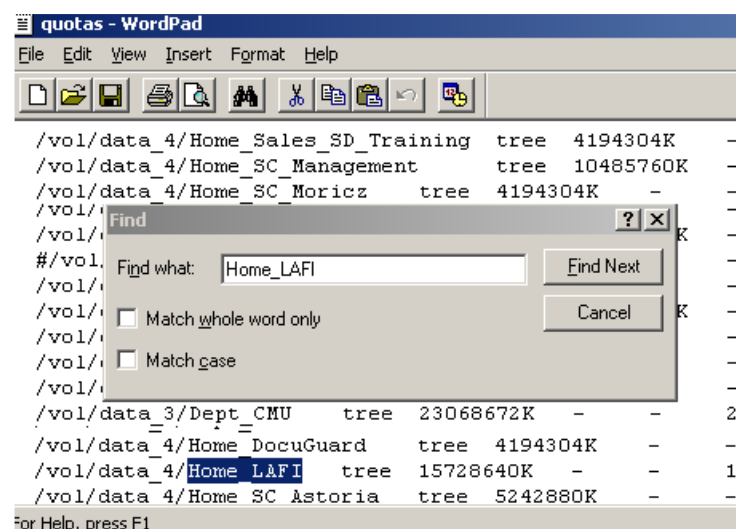
This may require you to access the questionnaire part of the VR as this should have the size and location of the request.

Item History	Questionnaire
User Questionnaire Item -Change Disk Quota	
Change Disk Quota	Please provide the following information:
Name of the Department	Home_LAFI
Path of department directory (e.g. g:\technology)	data_4\$
Increase or Decrease quota	Decrease
Desired additional disk quota	1000 MB

Although in this example we don't have the Filer details, we can check either NASBUD01, NASBUD02, WSWCTINAS201A or WSWCTINAS201B to confirm which filer this volume is located on, this is in fact NASBUD02.

1.26.3.2 Step 2 – Check Quota File

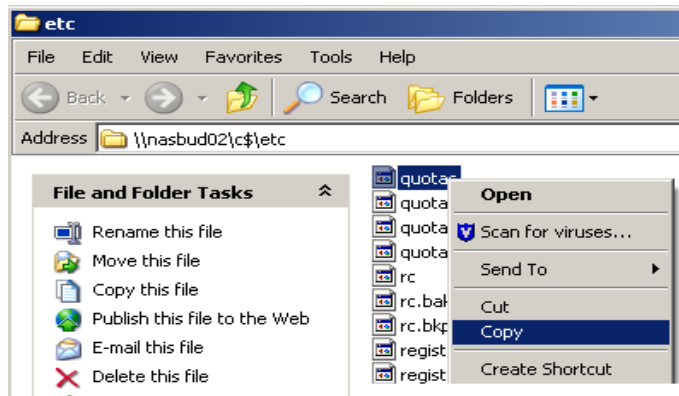
Once we know the Filer, it's time to check the quota entry.



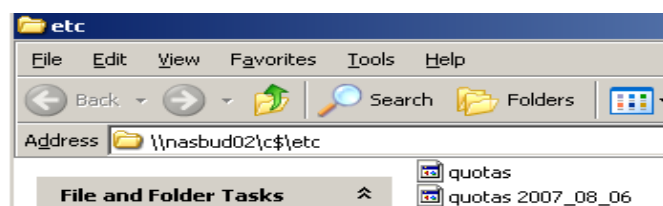
From the screenshot you can see the current setting for the quota entry.

1.26.3.3 Step 3 – Backup the Quota File

Before making any changes to the Filer, we must make a backup of the "live" quotas file in case we need to roll back from this change. The easiest way to do this is to copy the current quota file and append the current date to the end of the file.



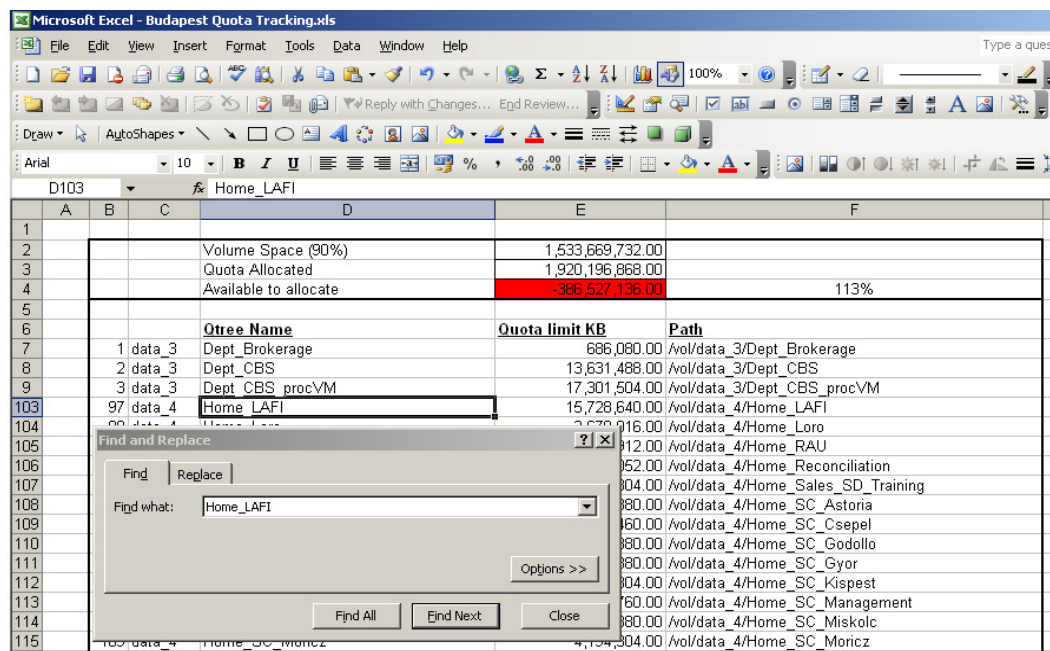
This can be seen as follows:



1.26.3.4 Step 4 – Track the Quota Change

To be able to track this change and to make sure the sum of the quota files does **not** exceed 90% of the volume size, when we edit the quota file, we need to ensure the new size is reflected in the spreadsheet which can be found at:

H:\Doc Control Sys\Documentation\Space Management\HU
H:\Doc Control Sys\Documentation\Space Management\PL



	A	B	C	D	E	F
1						
2				Volume Space (90%)	1,533,669,732.00	
3				Quota Allocated	1,920,196,868.00	
4				Available to allocate	-386,527,136.00	113%
5						
6				Qtree Name	Quota limit KB	Path
7	1	data_3		Dept_Brokerage	686,080.00	/vol/data_3/Dept_Brokerage
8	2	data_3		Dept_CBS	13,631,488.00	/vol/data_3/Dept_CBS
9	3	data_3		Dept_CBS_procVM	17,301,604.00	/vol/data_3/Dept_CBS_procVM
103	97	data_4		Home_LAFI	15,728,640.00	/vol/data_4/Home_LAFI
104	98	data_4		Home_Loro	2,672,016.00	/vol/data_4/Home_Loro
105				Home_RAUI	12.00	/vol/data_4/Home_RAUI
106				Home_Reconciliation	652.00	/vol/data_4/Home_Reconciliation
107				Home_Sales_SD_Training	104.00	/vol/data_4/Home_Sales_SD_Training
108				Home_SC_Astoria	180.00	/vol/data_4/Home_SC_Astoria
109				Home_SC_Csepel	160.00	/vol/data_4/Home_SC_Csepel
110				Home_SC_Godollo	180.00	/vol/data_4/Home_SC_Godollo
111				Home_SC_Gyor	180.00	/vol/data_4/Home_SC_Gyor
112				Home_SC_Kispest	104.00	/vol/data_4/Home_SC_Kispest
113				Home_SC_Management	160.00	/vol/data_4/Home_SC_Management
114				Home_SC_Miskolc	180.00	/vol/data_4/Home_SC_Miskolc
115				Home_SC_Moricz	4,134,304.00	/vol/data_4/Home_SC_Moricz

1.26.3.5 Step 5 – Quota Report (before)

We are almost ready to make the quota change, but before we do that we must provide evidence of the quota report from the filer, which in this case is NASBUD02

```
NASBUD02> quota report /vol/data_4/Home_LAFI
Type      ID      Volume      Tree      K-Bytes      Limit      Files      Limit      Quota Specifier
Used
tree      57      data_4      Home_LAFI      6806980      15728640      23524      -      /vol/data_4/Home_LAFI
```

Make sure this information is copied into the VR for tracking and proof.

1.26.3.6 Step 6 – Edit the Quota File

Once we have worked out the new size of the quota entry, this needs to be amended in the quota file of the relevant filer. This can usually be done via wordpad and the following path:

[\\filename\c\\$\etc](#) (or direct from the “run” command as: wordpad [\\filename\c\\$\etc\quotas](#))

```
/vol/data_4/Home_DocuGuard tree 4194304K - - 4110417K
/vol/data_4/Home_LAFI tree 14704640K - - 15414067K -
/vol/data_4/Home_SC_Astoria tree 5242880K - - 5138022K
```

1.26.3.7 Step 7 – Quota Resize and Report (after)

Once this change has been made, we need to resize the volume that the quota is located on and we should be able to see the new change to the quota file.

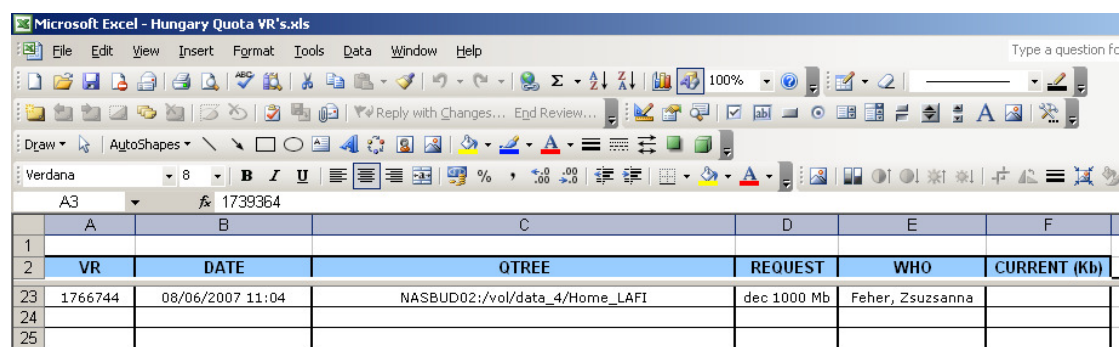
```
NASBUD02> quota resize data_4
NASBUD02> quota report /vol/data_4/Home_LAFI
Type      ID      Volume      Tree      K-Bytes      Limit      Files      Limit      Quota Specifier
Used
tree      57      data_4      Home_LAFI      6806980      14704640      23524      -      /vol/data_4/Home_LAFI
```

Please Note – If you do not run the quota resize command, the change in the quota file will *not* take effect.

1.26.3.8 Step 8 – Complete tracking spreadsheet

As we are tracking all Virtual Requests and correlating that info with the quota alerts we receive from DFM, it is necessary to update the spreadsheet located at:

H:\Reporting\ Hungary Quota VR's.xls
H:\Reporting\ Poland Quota VR's.xls



	A	B	C	D	E	F
1						
2	VR	DATE	QTREE	REQUEST	WHO	CURRENT (Kb)
23	1766744	08/06/2007 11:04	NASBUD02:/vol/data_4/Home_LAFI	dec 1000 Mb	Feher, Zsuzsanna	
24						
25						

1.26.4 Increasing a Quota

When a request for an **increase** in a quota file comes in, it is effectively the same as the decrease but with the calculation of the quota entry slightly different.

1.26.4.1 Step 1 – Confirm detail in VR

We know the qtree and path as it is specified in the agreed process and should be detailed in the VR. If it is not, assign the VR back to the owner requesting the full qtree and quota path:

```
8/8/2007 10:10:47 AM The full path is \\nasbud02\data_3$\spec_citiplc_nam_isa_candc
```

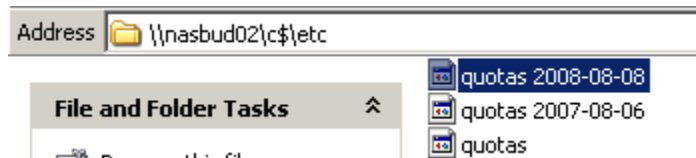
1.26.4.2 Step 2 – Quota Report (before)

```
NASBUD02> quota report /vol/data_3/SPEC_CitiPLC_NAM_ISA_CandC
```

Type	ID	Volume	Tree	Used	Limit	Used	Limit	Quota Specifier
tree	49	data_3	SPEC_CitiPLC_NAM_ISA_CandC	616396	665600	898	-	/vol/data_3/SPEC_CitiPLC_NAM_ISA_CandC

Make sure you paste this information into the VR for tracking and proof.

1.26.4.3 Step 3 – Backup the Quota file



1.26.4.4 Step 4 – Track the Quota change

Microsoft Excel - Budapest Quota Tracking.xls

	A	B	C	D	E	F
1						
2				Volume Space (90%)	1,533,669,732.00	
3				Quota Allocated	1,014,141,840.00	
4				Available to allocate	519,527,892.00	60%
64	58	data_3	SPEC_CitiPLC_NAM_ISA_CandC		1,177,600.00	/vol/data_3/SPEC_CitiPLC_NAM_ISA_CandC

H:\Doc Control Sys\Documentation\Space Management\HU

H:\Doc Control Sys\Documentation\Space Management\PL

1.26.4.5 Step 5 – Locate the Quota entry

Use WordPad and the “find” utility to locate the correct quota entry on the relevant filer:

```
/vol/data_3/SPEC_CitiPLC_NAM_ISA_CandC tree 665600K - - 652288K -
```

Find what: spec_citiplc_nam_isa_candc

Find Next

Cancel

Match whole word only

Match case

1.26.4.6 Step 6 – Edit the Quota entry

Update the quota file with new entry:

```
/vol/data_3/SPEC_CitiPLC_NAM_ISA_CandC tree 1177600K - - 652288K -
```

1.26.4.7 Step 7 – Quota resize and Report (after)

Logon to the filer and run quota resize so the new entry get's picked up. Make sure you paste this information into the VR for tracking and proof.

```
NASBUD02> quota resize data_3
NASBUD02> quota report /vol/data_3/SPEC_CitiPLC_NAM_ISA_CandC
```

Type	ID	Volume	Tree	Used	Limit	Used	Limit	Quota Specifier
tree	49	data_3	SPEC_CitiPLC_NAM_ISA_CandC	616396	1177600	898	-	/vol/data_3/SPEC_CitiPLC_NAM_ISA_CandC

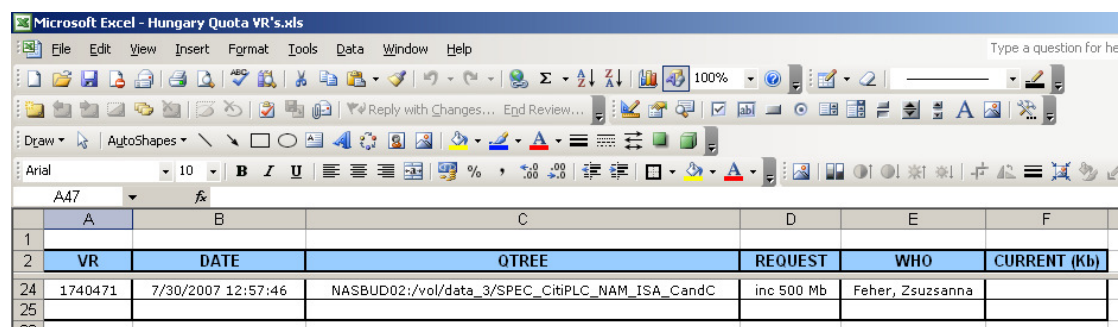
Please Note – If you do not run the quota resize command, the change in the quota file will *not* take effect.

1.26.4.8 Step 8 - Complete tracking spreadsheet

As we are tracking all Virtual Requests and correlating that info with the quota alerts we receive from DFM, it is necessary to update the spreadsheet located at:

H:\Reporting\Hungary Quota VR's.xls

H:\Reporting\Poland Quota VR's.xls



	A	B	C	D	E	F
1						
2	VR	DATE	QTREE	REQUEST	WHO	CURRENT (Kb)
24	1740471	7/30/2007 12:57:46	NASBUD02:/vol/data_3/SPEC_CitiPLC_NAM_ISA_CandC	inc 500 Mb	Feher, Zsuzsanna	
25						

Problem Management

1.27 Definition of Problem Management

Problem tickets will be logged to us through Virtual Tech. The monitoring and action of these tickets is a core part of our function. The Virtual Tech queues are monitored on a continual basis throughout our core support hours of 08:00 - 18:00 (GMT).

Virtual Tech tickets should be raised for all problems brought to our attention. Generally, these problems are raised by other groups or users themselves and get passed to us.

If a problem is brought to your attention, you should ensure that a valid problem ticket is raised by either the user/Helpdesk or Desktop support. If you have discovered a problem, it is also possible to raise a ticket to either our group or another support team. The majority of operating system and hardware related problems on the NAS platform are automatically logged by the Command Centre, as all NAS Filers are monitored via Netcool, also EMEA NAS Infrastructure, and the vendor, are notified via email by the auto support system native to the NAS platform.

EMEA NAS Infrastructure follow the Server Operations Level III Procedures for problem management, but in addition to this have defined processes in Chapter 7 for problem management.

1.27.1 Break / Fix

Upon receipt of an auto support case a corresponding problem ticket must be created in Virtual Tech and assigned to the EMEA NAS Infrastructure queue. The problem ticket must include the vendor case number, and the vendor case must include the Citigroup problem ticket number. Vendor case notes can be updated by searching for the case at

<http://now.netapp.com>

Note you need to create a login at the NOW website to be able to update the vendor case notes.

1.27.1.1 Failed Disks

When a disk fails on a NAS device, the device will send an automated email to both the vendor and the EMEA NAS Infrastructure team.

A member of ENI will ensure that the failed disk is correctly identified by checking the auto support e-mail in the section pre-ceded by "SYSCONFIG-R" where the faulty disk can be identified in the sub section "Broken Disks". Or can console on to the Filer and identify the problem disk using a number of storage commands.

Additionally the end of the e-mail in the "==== MESSAGES ====" section or using the messages file itself should also be checked to verify that the error logs indicated the same disk has failed. Finally Filer View can be checked to confirm the same disk is flagged as faulty or broken. This must then be independently verified by another team member using the above process.

If both members agree that the correct disk has been identified then a problem ticket is raised in Virtual Tech to the local team expected to carry out the disk change detailing the name and location of the device, and the size of the failed disk and that this is required to be replaced outside of the hour's 07:00 - 18:00. This will allow for the onboard spare to be rebuilt without interruption. If however there are multiple disk failures on the same system and there are no spare disks available to rebuild the failed disk to, then the failed disk needs to be replaced as a priority and at the first available opportunity including during the working day in the Virtual Tech ticket." Once the Virtual Tech ticket has been raised the Emergency Change must be raised in Virtual Change and EUDIR Approval obtained prior to carrying out the swap.

As part of the Virtual Tech ticket, ENI need to request that the local engineers verify if they can identify if the failed disk has been highlighted (failure LED lit), and if this has not happened automatically, then ENI need to turn on the led on the failed disk. If this is not possible then the LED's on disks either side of the failed disk need to be turned on using the LED_on %HBA

Adapter and port number. disk number%" command. The local team will then replace the failed unit with one of the on site spares provided by the vendor.

Once it has been confirmed that the failed disk has been replaced, then any of the LEDs turned on to identify the failed disk need to be turned off using the LED_off %HBA Adapter and port number. disk number%" command.

A local team will then follow their safe media procedures as defined in their PCM. The vendor will ship a replacement drive to the registered RMA contact for that location, in order to back fill the on site spares stock. Until a sanitization procedure has been established, no disks should be returned to the vendor, and no disks should be sent for destruction.

1.28 Identification and Documentation

1.28.1 Criteria

The criteria for creating problem tickets is defined as follows:

- Filer outage.
- Loss of service.
- Performance issues.
- File storage disk space.

For any other requests that fall outside of the above lists, a problem ticket should NOT be created. These should be treated as business as usual requests and should be logged to the request queue: EMEA NAS Infrastructure MAC.

1.28.2 Actionable Alerts

The team may be notified by a number of means of any issues. The below is a list defining the actionable alerts, but is by no means conclusive:

- Automated system alerts.
- Phone calls to either individuals, or to the group line.
- Emails.
- People walking into the group area and verbally notifying you.
- If a ticket is created in a different problem management system, then a corresponding ticket needs to be raised in the groups problem management system.
- If an issue is escalated to a vendor, then a corresponding ticket needs to be raised in the groups problem management system, and the vendors reference logged.

1.28.3 Ticket Creation

For each actionable alert a problem ticket must be created and this ticket must include all of the following points:

If vendor ticket is required this should be logged through the NOW case system

<http://now.netapp.com/>

- Client information (e.g. name, phone, location, cost centre)
- Problem category (e.g. desktop/monitor)
- Problem description (details gathered from clients, alerts and internal communications)
- Severity/Impact statement (indicators that identify risk to the firm and user population impacted).
- The time and date the problem was identified
- Creator of the ticket and the person or group to which it was assigned.

Virtual Tech will only create a valid ticket if the above details are entered into the system.

1.28.4 Problem Severity Definition

Any ticket that is assigned to Severity Level 1 must contain full justification as to why it meets the criteria for Severity Level 1. If there are insufficient problem details to enable the resolver groups to work the issues or justify why the ticket is deemed a severity 1, the ticket may be

sent back to the OHD (Originating Helpdesk or individual who logged the call) for further information.

- Severity 1 (4 hours)
- Severity 2 (8 hours)
- Severity 3 (24 hours)
- Severity 4 (non-problem) – These are placed in the EMEA NAS Infrastructure MAC Queue

Each production problem must be assigned one of four severity levels – 1 (critical), 2 (high), 3 (medium) or 4 (low). The following table summarizes the definitions for three of the four severity levels. Organizations may document their severity definitions with greater specificity, as guided by business requirements.

Technology Operations Outage Level Definitions

	Severity 1	Severity 2	Severity 3
Definitions:	All outages to a business and/or site affecting critical service for <u>external</u> and/or <u>internal</u> clients which results in negative client perception, monetary impact, potential loss of opportunity, or a substantial risk to Citigroup reputation.	Any degradation of service to a business and/or site affecting <u>external</u> and/or <u>internal</u> clients or a failure in technology infrastructure diversity/redundancy. If degraded service or diversity/redundancy is not resolved to a standard it could lead to monetary loss or a substantial risk of Citigroup reputation. Recurring/chronic degradation of service or diversity/redundancy must be classified as Severity 1.	A low impact incident affecting a single user, multiple users or a development system.
Guidelines: Chronic definition: 2 occurrences in 1 - 9 days 3 occurrences in 10 - 59 days 4 occurrences in 60 - 180 days	- Vulnerabilities - Major system, network, application, voice, etc. failures - Data Corruption 100% customer facing devices unavailable - Degradation of time critical services - Single branch that is isolated from the infrastructure. Outage Reporting is Mandatory	- Major system failures where seamless fail-over exists - Degradation of non-time critical services - Degradation of Customer facing devices/applications services Outage Reporting is Optional	Single Customer outage Outage Reporting is not required

1.28.5 Problem Updates

All tickets logged to the team queues must be examined and actioned in accordance with the Server Operations Level III Procedures for problem management. The tickets will be logged by either the Helpdesk (for users not able to use Virtual Tech), passed through from our CSS Desktop Teams, passed through from another SA group or logged by the Command Centre (London, Operations).

Examine the ticket and confirm that it is indeed allocated for our team.

If the ticket belongs to another support group or if you need to pass it back to the sender group, please ensure that you provide clear reasons for your actions and enter these into the ticket update field. When a ticket is re-assigned to a different resolver group you must also send the new group a e-mail to ensure that they are aware of the ticket.

The severity level of the ticket should also be reviewed to ensure that the correct classification is used. If this is incorrect it should be updated to reflect the correct status.

Ensure that any SEV-1 tickets in your name or assigned to the group have regular detailed updates at least every 2 hours.

If you find a ticket that is missing an update, you must investigate and/or speak to your colleague if the ticket is assigned to them and again ensure that the updates are inserted into the ticket.

For all Virtual Tech tickets raised that are identified as genuine system faults, these need to be recorded in the outages / issues section of the Daily Check report. These can be found here: H:\Reporting\Checks\Daily

1.29 Escalation and Notification

1.29.1 Notification

In the event of a Severity 1 ticket being raised, the Command Centre will be responsible for co-ordinating conference calls and escalation/notification to other resolver groups, management and business areas. If we are the resolver group of a Severity 1 or 2 incident, an entry and update to EMS must be made immediately to ensure that proper notification of the problem is made to other affected areas.

EMS is a global repository for critical issues, which provides the following.

(<https://archcntr.nam.nsroot.net/ARCHCNTR/tools/EMS/index.asp>)

The following also needs to be completed in the case of all Severity 1 or 2 incidents.

Notification of major outages to IT and Business management.

Completion of a detailed major outage report including root cause identification / analysis (EMS).

Follow-up of any action plans necessary to permanently correct the outage condition.

A system that will act as the sole repository for inputting, tracking and distributing major outage reports.

1.29.2 Escalation

The process of updating a ticket will ensure that any escalation requests from the customer are noted and reflected within the ticket. EMEA NAS Infrastructure are a resolver group, therefore the tickets will be "owned" by us. The analyst taking the call for the escalation request should update the ticket and contact the person working on the ticket so that the issue brought to their attention.

1.29.3 Security Incidents (SIRT)

It is very important that we realize what action is required if we encounter a security incident. There is a **SIRT (Security Incident Response Team)** process that is designed to deal with the following types of issues:

Security Incidents include, but are not limited to:

Loss of confidentiality;

Destruction of data;

Loss of system integrity, system degradation or denial of service;

Loss of data integrity;

Unauthorized use of corporate resources;

Fraud;

Other intrusions.

Security incidents pose a threat to the corporation and can result in financial loss, degraded service or damage to Citigroup's reputation.

While it may seem appropriate for businesses to deal with what appear to be trivial incidents, they must still be thoroughly documented and reported to CISO.

Even though an incident may appear trivial, it may have serious legal implications.

There is currently a process in place with the Helpdesks to deal with SIRT (Security Incident Response Team) issues. Further detail and contact information available from

<http://www.citigroup.net/informationsecurityservices/>

If a SIRT is identified, you should immediately advise Paul McInerney and in his absence Michael Styles. This is to ensure that All SIRT related issues and incidents are routed via our BISO (Andrew Cunningham) *GT EMEA TI DC BISO, or if Andrew is not available then the GISO (Tamas Szuharda). In instances where you involve EISS, the above should also be applied.

1.29.4 Specific Vendor Support Agreements

The specific service level agreements between Citigroup and Network Appliance can be found here:

<http://now.netapp.com/Self-Service/Start/usrPage.asp>

If for any reason the defined service level agreements are not met then this should be escalated to the following people:

EMEA NAS Infrastructure Manager – Paul McInerney
Network Appliance UK Account Manager – Tony Delle-Site
Network Appliance EMEA Region Account Manager – Ben Allchin

1.29.5 Callout

The call out procedures for the team can be found here:

http://wintelinfraweb.eur.nsroot.net/tools/eni_rota/secure/rota_callout.asp

This includes the out of hour's procedures and relevant contact numbers for all the team members.

The Command Centre also has access to relevant contact numbers and further escalation should the primary person be unavailable.

For any leavers or joiners to the team, or if the rota's change, or if the contact details change, then the call-out rota and the web site above needs to be updated to reflect this.

1.30 Determination

For any new problem tickets opened, please refer the below knowledge bases to assist in resolving the issues in a quick and timely basis.

1.30.1 Knowledge Base

The following are the knowledge bases used by EMEA NAS Infrastructure:

NetApp Filer - <http://now.netapp.com/Self-Service/Start/usrPage.asp>.

GPMS database.

Virtual Tech database.

Global Distributed Storage Engineering -

<http://catecollaboration.citigroup.net/domains/platstor/gdse/products/techstdshmpgs/netappfiler.aspx>

1.31 Bypass and Recovery

1.31.1 Temporary Fixes

All fixes that are implemented that are of a temporary measure need to be recorded as such in the Daily Checks report. These need to remain on the report until a permanent fix is implemented.

1.32 Resolution

1.32.1 Problem Ticket Elements

When a problem ticket is closed the resolver closing the ticket must ensure that the following entries in the ticket are correct:

Problem category (e.g. desktop/monitor)

Resolution description

Severity/impact statement (indicators that identify risk to the firm and clients impacted).

End time (time the problem was resolved)

Final disposition

Root cause indicator

1.32.2 Post Mortems

For all Severity 1 & 2 tickets all post mortem details need to be updated into the Executive Monitoring System. This can be found here:

<http://ems.ny.ssmb.com/ems/index.asp>

1.33 Management Oversight

To ensure that tickets are closed properly a sample of all tickets raised to the group need to be reviewed on a weekly basis and checked to ensure that the following information has been correctly detailed:

Problem category (e.g. desktop/monitor)

Resolution description

Severity/impact statement (indicators that identify risk to the firm and clients impacted).

End time (time the problem was resolved)

Final disposition

Root cause indicator

This sample needs to be discussed in the weekly team meeting to ensure that the whole team is aware of the current issues and to also address any trends in the faults reported.

Also as part of the closed loop process these need to be discussed to ensure that the full impact of the problem and resolution is addressed and understood.

As part of the prevention and continuous improvement process, during the weekly meetings, the weekly metrics need to be discussed to ensure that any trends are identified. Also the tickets should also be analysed to ensure that the proper root cause was identified. The following needs to be documented for each of the sampled tickets:

Document the problem tickets reviewed

Document all root causes identified

Document and assign ownership of root cause resolution

Track status of root cause resolution

1.34 MIS Reporting

1.34.1 SMART Report

Each Monday the team have to submit their updates for the previous week into SMART. The SMART system is a Placemat report is generated and is made available to senior management.

These reports detail the achievements and major work in progress for the team that occurred in the previous week.

Every Monday before close of Business, EMEA NAS Infrastructure team need to update SMART with any updates that need to be included in this report. The ENI Manager then collates this and submits this to the Product Support Report within SMART. Access to the SMART report can be found by click the link below

<http://ukctidrsd24/RTO/SmartReport>

People/ Team Recognition

Team or team members to be highlighted for recognition.

Details of any Achievements

Details of any achievements by the team.

Details of any Significant Problems / Issues / Risks

Details of any problems / issues / risks requiring notification.

Project/Initiative Update

Updates for any projects or highlight any initiatives.

Operational Update

Any operation updates to be reported.

Planned Tasks/Activities

Any planned tasks / activities / meetings planned for the near future.

1.34.2 Lever 9 Storage Metrics Report

As part of the Greenbook/Lever initiatives, the team has been tasked with collecting consistent Global metrics for Lever 9 - SAN, NAS and Mainframe. A template has been created by North America, which then needs to be completed by the specific Regional Teams.



"Lever 9 storage
metrics - NAS & MF E

This report is due the last week of every month and saved on the Teams Drive H:\Reporting\Level 9 folder. The report should also be uploaded directly onto The Global Storage Teams Collaboration Sharepoint Site

<https://catecollaboration.citigroup.net/domains/platstor/gdse/products/globalstorage/ProjectTracking/Forms/AllItems.aspx>

Alternatively (If no access to this Sharepoint Site) this report can be emailed to the following recipients

To Robert Small
CC'ing Paul McInerney; Michael Styles; Garry Battersby; *CATE Storage Engineering and Architecture

Information Security

For the NAS platform, EMEA NAS Infrastructure follows the generic change management processes and procedures, as defined in Section 0 of this document.

1.35 Information Security

For the NAS platform, EMEA NAS Infrastructure follows the NAS build specifications provided by Global Distributed Storage Engineering. This document includes mandatory system configuration settings, and includes a special security related configuration section.

OnTap Solution Guide and Release Notes can be found on the GDSE site below:

<http://catecollaboration.citigroup.net/domains/platstor/gdse/products/techstdshmpgs/netappfiler.aspx>

1.35.1 Virtual Threat Management (VTM) Process

The VTM process for NAS is similar to the Wintel VTM process. Global Distributed Storage Engineering (GDSE) owns the product owner relationship with the vendor (NetApp). As such NetApp informs GDSE on a weekly basis of any new issues with current internally approved Citigroup Data OnTap releases. Where necessary these issues are escalated to the Global Security Engineering group for peer review. If certified as a bona fide vulnerability, Security and Storage Engineering will initiate a case number in the VTM database.

All Global NAS representatives will be notified via email from Global Storage Engineering (the list of stakeholders is maintained in the Engineering PCM). In addition to this, notification will also be sent out via the weekly global NetApp case review call: where the topic will be listed in the agenda, minutes, and discussed during the call.

The remediation cycle for VTM is as follows:

- Vulnerabilities with a HIGH rating should be patched / resolved within 60 days of a certified solution being provided by GDSE
- Vulnerabilities with a MEDIUM rating should be patched / resolved within 180 days of a certified solution being provided by GDSE
- GDSE can also assign a completion date for a particular fix to be applied.

Once a solution is provided ENI should use an appropriate tracking mechanism to ensure all affected devices are identified and the remediation cycle is tracked accordingly (for example a spreadsheet matrix). All remediation activities must be covered under the change management processes.

As remediation of NAS devices does not automatically feed into the VTM database, reporting of completed remediation is done manually (via email) to regional NAS representatives, and to the audience on the global NetApp weekly case review call.

1.36 NAS Infrastructure Rights

To perform the day-to-day functions required for the role as a EMEA NAS Infrastructure SA the individual team members require the following rights at a minimum:

1.36.1 Changes to Rights

Before any changes to the ENI team members rights are made, the following process needs to be followed:

- Raise a Virtual Tech ticket explaining what rights are required and the justification, and place this in the EMEA NAS Infrastructure MAC queue
- Send an e-mail to the ENI Team manager requesting approval for the Rights.
- ENI Team manager to respond to the e-mail, with either an approval or denial.
- ENI Team manager to update the VT ticket with the appropriate response.
- The requester needs to upload the e-mail confirmation into the VT ticket.
- Once the rights have been approved these can be implemented.

Exceptions to the above:

- If the request is to create a domain level functional account for the use by ENI, then an additional approval from the Wintel Infrastructure Operations manager is required prior to the creation of the accounts and to follow the EMEA functional account request process via the Wintel Account Request Tracking System.

These approvals need to be added to the VT ticket as per the above procedure.

1.36.2 Network Appliance Filer

The group is currently responsible for all the Network Appliance NAS installations for EMEA with some exceptions. As such each of the team member has full administrator rights to each of the filers including the disaster recovery filers.

1.36.3 Monitoring Servers

The group currently maintains two monitoring servers, production and disaster recovery. Each team member requires administrator rights over each of these servers.

1.36.4 Applications

There are various web based application that each team member requires to perform their day to day role. Examples of these are WebAdmin, Whitepages, TAS, etc. A complete list of these can be found on the groups shared drive:

1.37 Entitlement Reviews

1.37.1 Overview

This document will cover the process for retrieving current entitlements for all relevant systems and the remediation process involved. It will also cover the procedure in place for requesting additional entitlements. Preceding all system reviews will be an EMEA NAS Infrastructure team listing review.

1.37.2 Non EERS Entitlements

This relates to current systems where it is not possible to feed the entitlements in to the EERS system for manager reviews.

These include:

- Operations Manager – Web based NAS Filer monitoring tool
- NAS Filer Local Accounts – Used to administer the NAS Filer environment
- Departmental Drive Access – Access to the Teams Group Drive

Due to the sensitivity of the above applications it has been decided to perform these reviews on a monthly basis rather than bi-yearly. These reviews are controlled via VCC and the required evidence is uploaded as required. The process for performing these reviews is detailed in the EMEA NAS Infrastructure CVS step by step guide.

1.37.3 EERS Entitlements

This relates to systems that automatically feed entitlements directly in to the EERS system and the EMEA NAS Infrastructure manager reviews and approves them on a bi-annual basis.

1.38 Joiners & Leavers

When a new person joins the group, they should not by default be given the above rights. These should be phased in over a period of time and only after the relevant training has been given and awareness of the level of responsibility required has been imparted and the EMEA NTSA groups have been made aware of the change.

1.38.1.1 New Starter Training Process

When a new person joins the EMEA NAS Infrastructure group, they will be expected to undergo an initial training and orientation process before they commence any work on servers or systems. This will involve reviewing all relevant process material, such as this PCM, EUR Operational standards etc, and also having various procedures demonstrated. All of this will be

tracked in a spreadsheet, and signed off by the group manager, or appropriate deputy, prior to the new starter commencing work.

The document is stored on the H drive,

<H:\Doc Control Sys\Documentation\New Starter\ENI New Starter Guide.xls>

This document has the name of the new starter added as a new column to track their progress.

Similarly for any leavers from the group these elevated rights should be removed prior to the member starting in their new role, or if the person is leaving the company then his account should be disabled within 24 hours of leaving and then subsequently all rights removed. Additionally the passwords on any privileged accounts should be changed including and halves of the dual controlled passwords.

Any change in group EMEA NAS Infrastructure members rights needs to be pre approved by Paul McInerney.

1.39 Functional Account Management

1.39.1 OVERVIEW

The term functional account refers to an account that is not a standard SOE 'User' account, with a standard SOE 'User' account being an account that is directly linked via RITS etc and is the responsibility of a single named individual, e.g. tl84065.

To comply with the relevant policies, the following procedures in relation to functional account management must be followed for all functional accounts managed / used by EMEA NAS Infrastructure SA. The procedures are detailed below as follows:

Functional Account Categories.

Functional Account Controls.

Functional Account Inventory.

Functional Account Access / Tracking.

1.39.1.1 FUNCTIONAL ACCOUNT CATEGORIES

Each SA within the EMEA region will have an SOE 'User' account within 'EUR'.

Each SOE 'User' account is directly linked to a named individual via RITS etc, who is the sole owner of the account and each SA is therefore responsible and accountable for all aspects of their account. In addition, each SOE 'User' account within the 'Account Domain' is subject to the account policy.

SOE 'User' accounts are not deemed to be functional accounts.

Functional Accounts fall into 2 different categories, these are detailed as follows:

1.39.1.2 Built in Local Administrator Accounts

Each filer has 'Local Administrator' and 'root' accounts that are built in as part of the operating system. These accounts are only used if there are issues with individual SOE accounts or if the business request us to access data the local administrator password can be brought in to use. These accounts have dual controlled passwords and therefore require more than one person to action. As these accounts are only used as a last resort they remain in an unused state until they are needed.

1.39.1.3 Service Accounts

'Service' accounts are accounts that are used to perform system related functions where it is not appropriate for an SA to use their own SOE 'User' account, e.g. starting/running services where running the service as the system context is not suitable, scheduling background jobs etc. Due to the usage of 'Service' accounts, 'Service' accounts are generally in a constant state of use.

1.39.2 FUNCTIONAL ACCOUNT CONTROLS

Until such a time that a single application, e.g. Cyberarc has been defined as the global standard for managing 'Functional' account passwords, the following compensating controls are in place to aid in the management of 'Functional' accounts.

1.39.2.1 Dual Control

1.39.2.1.1 SA SOE 'User' Accounts:

Dual control is not necessary on these accounts, as each SA is responsible for all aspects of their own account and actions tracked. The passwords on these accounts follow the normal account policy rules, including the password expiring and having to be changed frequently, accounts do not get locked out on the current version of OnTap.

1.39.2.1.2 'Local Administrator' Accounts:

For the majority of systems administrative actions, the SA's are able to perform 'Local Administrator' activities using their own SOE 'User' account and as such the 'Local Administrator' / 'root' accounts are not in constant use and not widely needed. As these accounts are not linked directly to one individual, any actions made using this account are therefore not traceable to any individual and therefore compensating controls are needed until such a time as a product, e.g. Cyberarc has been identified, reviewed, approved and implemented to manage such accounts. As such, 'Local Administrator' and 'root' accounts must be placed under 'Dual Control', so the password is unknown to any one individual. Members of the NAS SA group who are responsible for the server should know and hold 'Half A' and a member of a separate group who do not report into the same line manager as the SA group should know and hold 'Half B'. In doing so, there should always be staff available from each group, who can dual key the password as needed and therefore the full password should never need to be known by a single individual.

1.39.2.1.3 'Service' Accounts:

As all 'Service' account cannot be linked to one individual, any actions made using this account are therefore not traceable to any one individual and therefore compensating controls are needed. As such, all 'Service' accounts must be placed under 'Dual Control', so the password is unknown to any one individual. Members of the NAS SA group who are responsible for the 'Service' account should know and hold 'Half A' and a member of a separate group who do not report into the same line manager as the SA group should know and hold 'Half B'. In doing so, there should always be staff available from each group, who can dual key the password as needed and therefore the full password should never need to be known by a single individual.

1.39.2.2 Password Changes / Password Not Expire

The controls detailed below must be reviewed regularly (minimally semi-annually) to identify any weaknesses and improve the process.

1.39.2.2.1 SA SOE 'User' Accounts:

As these accounts must reside in the 'EUR' domain, they are affected by the account policy set on the 'Account Domains' and as such, each SA will be forced to change their password by the 'Maximum Password Age' setting. In addition, these accounts must not be set to 'Password Never Expire' (PNE). NAS Filer local SA SOE accounts mirror the domain accounts by name and are tracked via the compensating control which checks the password age for these accounts on a daily basis. This process is detailed in section 1.18.4.

1.39.2.2.2 Local Administrator' Accounts:

Each time the 'Local Administrator and Root' password is reset then the date that this occurred must be recorded in the 'Inventory' tab of the functional account inventory and the actual password change event must be recorded in the 'Usage Tracking' tab of the event log collection inventory.

However, the 'Local Administrator' / 'root' passwords, must be reset under dual control in any of the following instances:

If a member of staff leaves who has access to either 'Half A' or 'Half B'.
If either 'Half A' and/or 'Half B' are believed to be compromised.
At least once every 365 days.

1.39.2.2.3 'Service' Accounts:

Each time the 'Service' account password is reset then the date that this occurred must be recorded in the 'Inventory' tab of the functional account inventory and the actual password change event must be recorded in the 'Usage Tracking' tab of the event log collection inventory.

However, 'Service' account passwords, must be reset under dual control in any of the following instances:

If a member of staff leaves who has access to either 'Half A' or 'Half B'.
If either 'Half A' and/or 'Half B' are believed to be compromised.
At least once every 365 days.

1.39.3 Functional Account Inventory

All new domain functional accounts must be requested via EMEA Wintel Infrastructure in accordance with the EMEA Wintel Infrastructure Operational Standards found on the EMEA Wintel Infrastructure website. Only once the request has been approved, should the account be created. All local new functional accounts are requested via the EMEA NAS Infrastructure manager to provide approval for use of the new account.

It is the responsibility of the EMEA NAS Infrastructure SA group to maintain a functional account inventory of their functional accounts and other information related to such accounts. A functional account inventory template is used to track this.

The functional account inventory for EMEA NAS Infrastructure can be located at

<H:\Audit\ENI Tracking\Functional Account Inventory - EMEA NAS Infrastructure.xls>

It is the responsibility of each ENI team member and ultimately the group manager to ensure their functional account inventory is always maintained and that all changes to functional accounts e.g. additions, removals and changes are recorded to ensure their inventory always reflects the correct status of all functional accounts.

1.39.4 Functional Account Creation

Detailed below are the steps that must be completed by the NAS SA group when a new functional account is created to ensure that they maintain an inventory of their own specific 'Functional' accounts:

- Update the 'Inventory' tab within the functional account inventory, to record the relevant details of the newly created functional account.
- Update the 'Revision History' tab within the functional account inventory, to record the changes made to the functional account inventory.

The above actions must be completed as follows:

Within the 'Inventory' tab, go to the next empty row and add a new record, as follows:

Domain/Local Machine Name – Type '*Domain*', where '*Domain*' is the actual name of the domain in which the newly created functional account resides e.g. EUR or type '*Local Machine Name*', where '*Local Machine Name*' is the actual name of the local machine on which the newly created functional account resides e.g. LDNCTINAS201A.

Account Name - Type '*Account Name*', where '*Account Name*' is the actual name of the newly created functional account e.g. Administrator.

Account Description / Purpose – Type '*Account Description / Purpose*', where '*Account Description / Purpose*' is a descriptive of the purpose of the account e.g. Built-in Account for Domain Administration.

Status – Type **Active** to confirm the functional account is active.

PNE – Type **Yes** or **No** to detail if the functional account is 'Set to Never Expire'.

Access / Rights – Type **Domain Admin** and/or **Account Operator** and/or **Domain User** to detail the rights that the functional account has been granted. Note, any other rights or permissions should also be detailed.

Privileged - Type **Yes** or **No** to detail if the functional account is deemed privileged. Any rights other than standard Domain User rights must be deemed privileged.

Dual Controlled - Type **Yes** or **No** to detail if the password for the functional account has been set as dual control. Dual control being where the password has been keyed in by two separate person(s), with each person(s) only knowing their half of the password and therefore the password is not known by any single individual.

Date DC'd – Type '*Date DC'd*', where '*Date DC'd*' is the actual date (DD/MM/YYYY) when the functional account was originally set as dual controlled.

Holder Half A - Type '*Holder Half A*', where '*Holder Half A*' is the actual SOE Id's of any staff who have knowledge of the first half of the dual controlled password.

Holder Half B- Type '*Holder Half B*', where '*Holder Half B*' is the actual SOE Id's of any staff who have knowledge of the second half of the dual controlled password.

Date PW Last Changed - Type '*Date PW Last Changed*', where '*Date PW Last Changed*' is the actual date (DD/MM/YYYY) when the password for the functional account was last changed.

Justification – Type '*Justification*', where '*Justification*' is a descriptive of what the functional account needs to exist, e.g. This is a built in account and as such cannot be removed. Each SA uses their own SOE account, which has domain admin rights but this account is kept as the master domain administration account.

Comment - Type '*Comment*', where '*Comment*' is a field for any relevant comments, e.g., This account is to be retired.

Within the 'Revision History' tab, go to the next empty row and add a new record to reflect the changes above as follows:

Updated by - Type '*SOE ID*', where '*SOE ID*' is the actual SOE ID of the SA that made the above changes to the spreadsheet.

Date – Type '*Date*', where '*Date*' is the actual date (DD/MM/YYYY) when the above changes were made.

Domain/Local Machine Name – Type '*Domain*', where '*Domain*' is the actual name of the domain that the account resides in e.g. EUR or type '*Local Machine Name*', where '*Local Machine Name*' is the actual name of the local machine on which the newly created functional account resides e.g. LDNCTINAS201A.

Account Name – Type '*Account Name*', where '*Account Name*' is the actual name of the account that has been added e.g. Administrator.

Change Details – Type '*Change Details*' where '*Change Details*' are the details of what has been changed, e.g. a newly created functional account has been added to the functional account inventory.

1.39.5 Functional Account Creation for EMEA NAS Infrastructure

EMEA NAS Infrastructure are required to follow the full process defined in [Functional Account Creation](#).

Approval has to be sought and approved from EMEA NAS Infrastructure Operations management (Paul Mcinerney or Michael Styles). In any instance that ENI management are not available for a duration then EISS should be asked to approve the functional account process, however ENI management must be cc'd on the request to EISS requesting approval.

Under no circumstances can a Functional account be created without this approval.

Once this approval is received, if e-mail approval then this must be uploaded into a VT, which is used to process the functional account request by ENI.

1.39.6 FUNCTIONAL ACCOUNT ACCESS / TRACKING

The following procedures below must be followed in relation to the functional accounts access:

1.39.6.1 'Local Administrator' Accounts

As each ENI Team member's SA SOE 'User' Account has 'Local Administrator' rights on the servers / Filers for which they are responsible, the 'Domain Administrator' and 'Local Administrator' accounts should rarely be needed.

In addition, as the 'Local Administrator' accounts are not linked directly to one individual, any actions made using these accounts are therefore not traceable to any one individual and therefore compensating controls are needed. As such, the 'Local Administrator' passwords must be placed under 'Dual Control', so the passwords are unknown to any one individual and the passwords must be split into two halves, with members of the NAS SA group who are responsible for the Server / Filer knowing 'Half A' and a member of a separate group who do not report into the same line manager as the SA group knowing 'Half B'.

In doing so, there should always be staff available from each group, who can key in the passwords as needed and therefore the full passwords should never need to be known by a single individual.

As such, in the event that the 'Local Administrator' account is needed, a member of the NAS SA group who are responsible for the servers should coordinate the process detailed below:

1.39.6.1.1 Break/Fix

The ENI Team member holding 'Half A' of the password must ensure that a valid Virtual Tech ticket exists that details the actions that need to be carried out using the 'Local Administrator' account. If a ticket does not exist, then the ENI Team member must arrange for a ticket to be created including full details.

Once a valid Virtual Tech ticket has been created, the ENI Team member should consult the functional account inventory to ascertain which other staff members have access to 'Half B' of the password.

The ENI Team member would then contact the ENI Team manager, using the standard call out procedures to obtain authorisation to proceed with the use of the 'Local Administrator' account. If the ENI Team manager or his deputy cannot be contacted within a 15-minute period and the issue of a critical nature, then the ENI Team member can proceed, as written notification of the use of the 'Local Administrator' account is mandatory in the later stages of process.

The ENI Team member should then contact a staff member holding 'Half B' of the password and must provide an overview of the issue to justify the need to use the 'Local Administrator' account. If the event that the first staff member is not unavailable then attempts should be made to contact the other holders of 'Half B'.

The ENI Team member must then assign the Virtual Tech ticket to the staff member who has been contacted who has access to 'Half B' of the password.

The staff member holding 'Half B' of the password must then review the Virtual Tech ticket to ensure that sufficient justification is included.

Once the justification has been reviewed and confirmed the staff member holding 'Half B' of the password should proceed to key in his/her half of the password. The staff member must then update the Virtual Tech ticket to confirm that 'Half B' of the 'Local Administrator' password was keyed in and re-assign the ticket back to the ENI Team member.

The ENI Team member should carry out only the actions as detailed / justified in the Virtual Tech ticket and ensure the account is logged out. The Virtual Tech this must then be updated to confirm what actions were taken and the ticket should be closed.

The ENI Team member must record the actual bringing together of 'Half A' and 'Half B' of the 'Local Administrator' password in the 'Usage Tracking' tab of the functional account inventory. All details in relation to the actions made using the 'Local Administrator' account must be recorded in the 'Usage Tracking' tab of the event log collection inventory.

1.39.6.1.2 Staff Members holding 'Half B' not available or unable to remotely key in the password

If the issue is such that 'Half B' of the password is not available due to all staff members holding 'Half B' not being contactable or they are unable to key in the password, e.g. no remote access, then ENI Team member should assess if the issue of a critical nature, in which case, they should contact the Head of Datacentre Product Support or their ENI Manager to provide an overview of the situation and seek approval to reset the password for the 'Local Administrator' account.

Once this has been approved, the Virtual Tech ticket should be updated to reflect that the 'Local Administrator' password has been reset and hence is no longer under dual control and also to detail that the 'Local Administrator' password must be reset within the next 24 hours. The Virtual Tech ticket must not be closed until the password has been changed and reset under dual control. The ENI Team Manager must ensure that this takes place. Note – This action will also be flagged in the Event Log Review process and hence any unjustified password resets would be highlighted.

Each time the 'Local Administrator' password is reset then the date that this occurred must be recorded in the 'Inventory' tab of the functional account inventory and the actual password change event must be recorded in the 'Usage Tracking' tab of the event log collection inventory.

1.39.6.1.3 Change

The ENI Team member holding 'Half A' of the password must ensure that a valid Virtual Change ticket exists that details the actions that need to be carried out using the 'Local Administrator' account. If a ticket does not exist, then the ENI Team member must arrange for a ticket to be created including full details.

Once a valid Virtual Change ticket has been created and approved, the ENI Team member should consult the functional account inventory to ascertain which other staff members have access to 'Half B' of password.

The ENI Team member does not need to contact the ENI Team manager to obtain authorisation to proceed, as the ENI Team manager must have already approved the Virtual Change ticket.

The ENI Team member should then contact a staff member holding 'Half B' of the password and must provide an overview of the change to justify the need to use the 'Local Administrator' account.

The staff member holding 'Half B' of the password should proceed to key in his/her half of the password.

The ENI Team member should carry out only the actions as detailed / justified in the Virtual Change ticket and ensure the account is logged out. The Virtual Change ticket must then be updated to confirm what actions were taken and the ticket should be closed.

The ENI Team member must record the actual bringing together of 'Half A' and 'Half B' of the 'Local Administrator' password in the 'Usage Tracking' tab of the functional account inventory.

All details in relation to the actions made using the 'Local Administrator' account must be recorded in the 'Usage Tracking' tab of the event log collection inventory.

As the Virtual Change must be planned, there should not be a situation that requires the 'Local Administrator' password to be reset due to a staff member holding 'Half B' of the password not being available or not able to remotely key in 'Half B' of the password.

1.39.6.2 'Service' Accounts

As 'Service' accounts are not linked directly to one individual, any actions made using these accounts are therefore not traceable to any one individual and therefore compensating controls are needed. As such, 'Service' account passwords must be placed under 'Dual Control', so the password is unknown to any one individual and the password must be split into two halves, with members of the ENI Team who are responsible for the 'Service' accounts knowing 'Half A' and a member of a separate group who do not report into the same line manager as the SA group knowing 'Half B'.

In doing so, there should always be staff available from each group, who can dual key the password as needed and therefore the full password should never need to be known by a single individual. Once a 'Service' account has been configured, the password would only need to be keyed infrequently, e.g. If a new instance of the service was required due to the existing server being rebuilt etc.

As such, in the event that 'Service' account passwords are needed to be keyed into a scheduled job, a member of the NAS SA group who are responsible for the 'Service' account should coordinate the process detailed below:

Note – 'Service' accounts differ from 'Local Administrator' accounts in that 'Local Administrator' remain in an unused state, where as 'Service' accounts are generally configured to run scheduled background jobs and therefore are in constant state of use. In addition, 'Service'

accounts passwords are generally only required to configure the scheduled job and are actually not used to login to a workstation or NAS Filer.

1.39.6.2.1 Break/Fix

The ENI Team member holding 'Half A' of the password must ensure that a valid Virtual Tech ticket exists that details the 'Service' account that needs to be configured along with the justification. If a ticket does not exist, then the ENI Team member must arrange for a ticket to be created including full details.

Once a valid Virtual Tech ticket has been created, the ENI Team member should consult the functional account inventory to ascertain which staff members have access to 'Half B' of the password.

The ENI Team member should then contact a staff member holding 'Half B' of the password and must provide an overview of the issue to justify the need to the need to key in the 'Service' account password. In the event the first staff member is unavailable then attempts should be made to contact the other holders of 'Half B'.

The ENI Team member must then assign the Virtual Tech ticket to the staff member who has been contacted who has access to Half B of the password.

The staff member holding Half B of the password must then review the Virtual Tech ticket to ensure that sufficient justification is included.

Once the justification has been reviewed and confirmed the staff member holding Half B of the password should proceed to key in his/her half of the password. The staff member must then update the Virtual Tech ticket to confirm that Half B of the 'Service' account password was keyed in and re-assign the ticket back to the ENI Team member.

The ENI Team member must update the Virtual Tech ticket to confirm the details that had the 'Service' account password keyed in and close the ticket.

The ENI Team member must record the actual bringing together of 'Half A' and 'Half B' of the 'Service' account password in the 'Usage Tracking' tab of the functional account inventory.

If the issue is such that 'Half B' is not available or a physical presence is required then the ENI Team member should assess if the issue is of a critical nature, in which case, they should proceed to key their own SA SOE 'User' account password.

The Virtual Tech ticket should be updated to reflect that the resolution included entering their own SA SOE 'User' account and password, and the reason for this. The Virtual Tech ticket must not be closed until the 'Service' account and dual controlled password is entered as required. The ENI Team Manager must ensure that this takes place.

1.39.6.2.2 Change

The ENI Team member holding Half A of the password must ensure that a valid Virtual Change ticket exists that details the details of the 'Service' account that needs to be configured along with justification. If a ticket does not exist, then the ENI Team member must arrange for a ticket to be created including full details.

Once a valid Virtual Change ticket has been created, the ENI Team member should consult the functional account inventory to ascertain which other staff members have access to 'Half B' of the password.

The ENI Team member should then contact a staff member holding 'Half B' of the password and must provide an overview of the issue to justify the need to key in the 'Service' account password.

The staff member holding 'Half B' of the 'Service' account password should proceed to key in his/her half of the password.

The ENI Team member should update the Virtual Change ticket to confirm that the change was implemented correctly with the service account and the ticket should be closed.

The ENI Team member must record the actual bringing together of 'Half A' and 'Half B' of the 'Service' account password in the 'Usage Tracking' tab of the functional account inventory.

As the Virtual Change must be planned, there should not be a situation that requires a 'Service' account password to be reset due to a staff member holding 'Half B' of the 'Service' account password not being available or able to remotely key in the 'Service' account password.

1.39.6.3 Functional Accounts Not Owned by ENI

The ENI team assist the SAN team by holding part B of the dual controlled password to the local administrator accounts, and the Mainframe Storage Team on the following system types:

- Centera
- Cisco
- HDS
- IBM VTS

The SAN team have documented their functional account process in the document "EMEA DS SAN Highly Privileged Dual Control Process v1.0.doc" of which will be followed if the local administrator account is required to be used, and details are included in the Mainframe Storage Management PCM. If access to the dual controlled passwords is required the SAN team will have the appropriate problem / change ticket assigned and contact the ENI team as required.

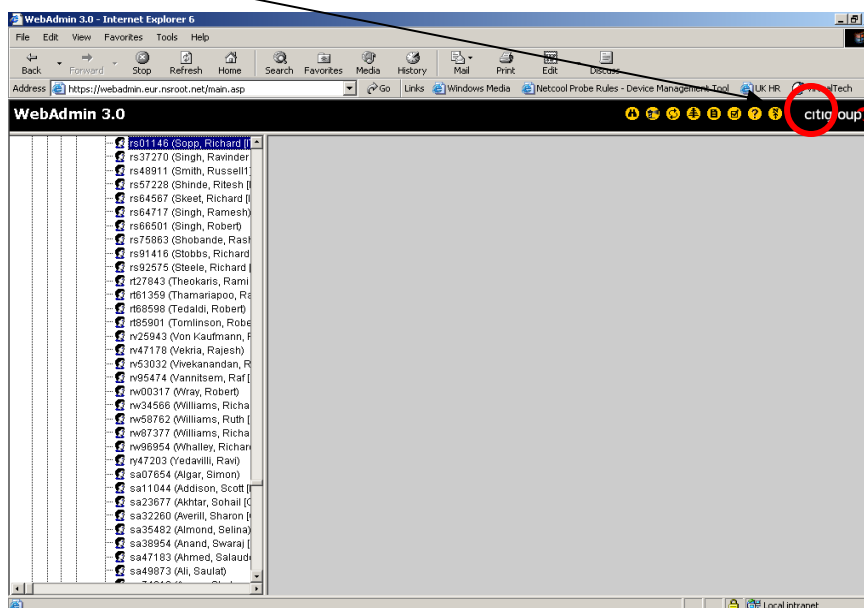
1.40 TEARS EVENT JUSTIFICATION AND REVIEWS

1.40.1 Overview

To comply with the audit and compliance policies, all the NAS SA's must follow the following procedures in relation to justifying events from Server logs via TEARS. TEARS can be accessed via the following URL

<https://tears.nj.smb.com/Tears/Scripts/EventJustification.aspx>,

or by clicking on the Audit Check button in Webadmin, then selecting Event Justification Website.



Each SA group must also ensure that an independent review of the event log from each server that they manage is performed.

In order to achieve this, the TEARS tool has been developed to collect logs from servers, and highlight actions that require justification. This tool also contains a feature to allow reviews of justified actions to take place, which can be performed by an independent group. Finally the tool has reporting capabilities to enable reports to be run weekly identifying events that are still unjustified, have been justified, and justified events that accepted or reject following the independent review. This enables group to ensure all events are being addressed. Each group must achieve 95% reconciliation of their events, in order to satisfy their audit requirements.

This document will detail the technical part of the process, for justification and reviewing part of the process, including Managers' responsibilities.

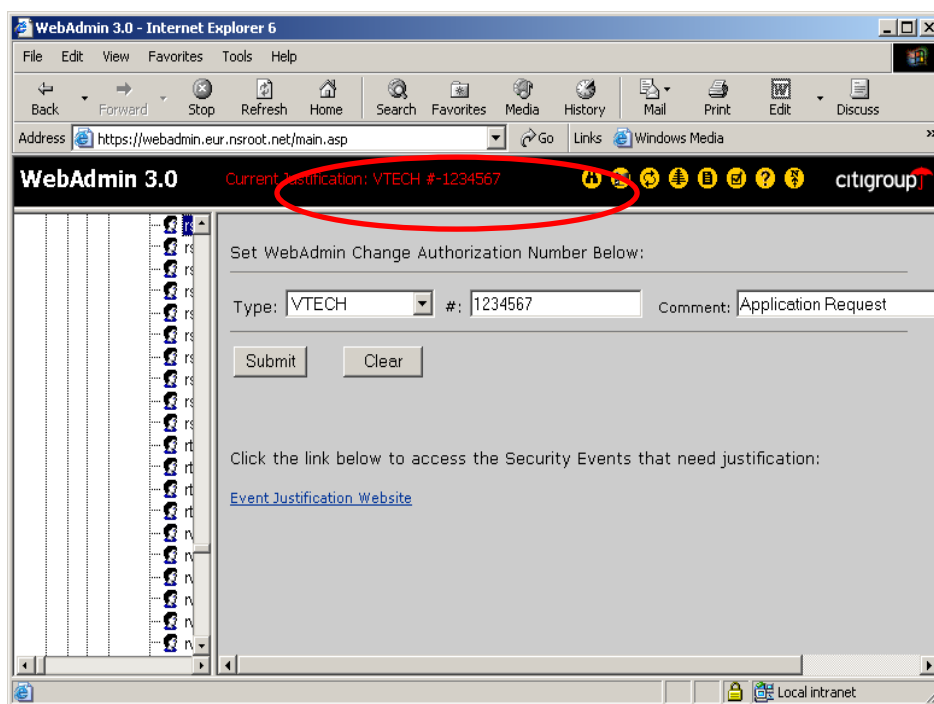
Filer logs are not collated by TEARS. The Filer audit logs are collated and reviewed on a daily basis by a third party team as to comply with the related Citi policy.

1.40.2 Justifying Events

Each SA is expected to justify their events within a maximum of 24 hours from the time the action occurred. After 24 hours, the independent review team will need to review justifications. There are two methods of justification; the first is to use the pre-justification utility within Webadmin, and the second is to wait until the event appears in TEARS and providing the justification after the event. It is always recommended to use the pre-justification tool, as this will ensure you don't have to remember to go back and justify later. Unfortunately this only is available when working in Webadmin, so activity on others servers will have to be justified later.

1.40.3 Pre-justifying events

Pre-justification is only available when performing activity in Webadmin only. In order to Pre-justify an event, the SA should select the Audit Check button in Webadmin before commencing activity. The in the Type field, the should select the System for the source of the justifying ticket (e.g. VTECH, INFOMAN, etc), then the ticket number, plus a comment on the activity about to be performed. Then click the submit button. On the Frame you should now seen in red the details of the ticket justifying all work about to be performed in Webadmin.



Once the activity has been finished, click on the Clear button, and this will stop justifying events against the specified ticket number.

1.40.4 Post-justifying events

When an SA performs activity on a server or within Webadmin that was not pre-justified, they should then visit the TEARS site in Webadmin and justify the event. This should form part of any process of change or activity. As a safety net, each SA should review TEARS for any unjustified events against them at least twice per day, when they first log on, and prior to going home. This should mean all events are justified within the required 24 hours.

As each Manager is responsible for ensuring their teams justify all their events, they should also check TEARS for unjustified events in their teams, also at least twice per day, when they first log on, and prior to going home.

1.40.5 Independent Reviews

All justified events need to be reviewed by an independent group in order to ensure that the activity performed is matched to the ticket or other referenced justification.

The EISS ICU team will provide the independent review service, which will take the form as follows:

- EISS ICU will review events from the previous day for each group, ensuring the justification supplied accurately matches the event performed.
- Where events have sufficient justification, the event will be 'Accepted'.
- If the event justification is not sufficient, or the justification does not match up with the event, then the event will be 'Rejected'. An e-mail will be sent to the SA, and their Manager, detailing the event that has been rejected, and seeking that the event be updated with a fuller, or more accurate justification. The SA will then have 24 hours within which they should respond to advise the event has been updated.
- If any event has not been justified, an e-mail will be sent to the SA, and their Manager, detailing the event(s) that have not been justified, and seeking that the event be justified. The SA will then have 24 hours within which they should respond to advise the event has been updated.
- If the SA does not respond within the required further 24 hours, then the EISS ICU team will escalate a potential issue to the SAs manager, who will need to take appropriate action to have the event properly justified, or determine if a SIRT incident needs to be raised.

EISS ICU will retain all e-mail chases, responses and weekly reports for 1 year for RCSA and Audit purposes.

1.40.6 Review Report

Each week the EISS ICU group will send out a report for each group to the group DL, detailing all events justified, unjustified, accepted and rejected. The group manager is cc'd on the email to be able to track unjustified events.

1.40.6.1 Escalations

Any machines that cannot be traced should be escalated to CTAC. The Virtual Tech ticket should be re-assigned to CTAC.

1.41 Information Systems Inventory

Each business will ensure that an inventory is maintained of all Information Systems (TI applications only) and Processes under their control. The inventory will specifically identify the Information Owner, Information Classification, Criticality level, Risk level and Infrastructure Security Classification.

1.41.1 Core Processes

To ensure compliance with the CITMP requirements for classification of all core processes under the control and management of the EMEA NAS Infrastructure team, the following needs to be adhered to each time there is a significant change in the environment that the team supports. At the minimum this needs to be reviewed annually when the COB processes are reviewed.

The spreadsheet containing the significant core processes needs to be revised and updated to reflect these changes. This spreadsheet is located in the following location:

<H:\Doc Control Sys\01 Current Documents\AllCoreProcesses-ENI.xls>

If required any COB changes are to be made within COBTrac and reviews are completed on a regular basis by the BCS team.

1.42 Vulnerability and Threat Patch Management

New versions of OnTap are certified by the GDSE team in the US, and dates are set on when the deployment of the standard version is to be completed. The OS upgrades contain the required patches to resolve any vulnerabilities highlighted. Announcements of this nature are made

during the weekly call and OS versions are tracked regularly via the quarterly CVS check, NetApp Filer revisions.

Continuity of Business

1.43 Contingency Requirements

Continuity of Business (COB) supports our contingency. In the event of contingency being called, staff will be expected to respond and get to their respective sites as quickly as possible, whether this is within the working day or outside it.

Full details of COB plans can be found in COB Trac:

<https://cobtrac.nj.ssmb.com/siteminderagent/forms/login.fcc>

Implementing / Decommissioning NetApp Filers

1.44 Implementing NetApp Filers

When new devices are required to be implemented, EMEA NAS Infrastructure follow the required procedures as documented by the EMEA Project Office for the duration of the project. During the project the requirements are finalised, ENI reference both the GDSE Solutions Guide and the ENI Operational Filer Installation documents to provide an approved solution. Once the solution has been implemented the project is closed off as requested by the project manager.

1.45 Decommissioning of NetApp Filers Requirements

When devices are no longer required there are a number of tasks to be completed in relation to the decommissioning, and there are also a couple of rules that have to be applied.

The rules are as follows:

- Devices are decommissioned a cluster at the time. This ensures full redundancy is achieved at all times.
- Business support groups are required to remove the data and any shares prior to signing the device off as ready for decommissioning. If this is not possible then the business support group can raise a change request to EMEA NAS Infrastructure to destroy the qtree / volume as required.

The tasks to be completed are listed below with the related tracking tool to be used for each process and the team required to perform the task:

- Data removed and user shares deleted from the system by the business support group
- ENI raise Aperture (Where App is in use) ticket for decommissioning of device
- ENI raise change request for shutdown of the system
- ENI raise VR to remove the device from monitoring
- If ENI are required to physically remove the hardware from the Data Centre a change request is raised to cover this
- ENI shutdown the system under the above approved change request
- ENI set device as decommissioned within Aperture / TAS under the above change request
- Hardware Infrastructure power off and remove all power and network cables
- Hardware Infrastructure remove all hard disk drives and follow required ETM process
- If required ENI physically remove the devices from the Data Centre under the above approved change request, and store in HLF until disposal has been organised
- ENI raise VT ticket to action the following items:
 - Delete computer object from the domain
 - Remove device from DFM
 - Confirm device no longer appears in NAS server list, <http://wintelinfraweb.eur.nsroot.net/ewiservers/nas.asp>. If required delete device from static server list
\\ldnctisw002\d\$\data\data_svr\inetpub\WintelInfraWeb_Virtual_Dirs\ewiservers\nas_static.txt
 - Remove device from required AV scanner folder within ePO. If there are no devices left associated with this folder engage EMEA Wintel Infrastructure to commence a project to decommission the associated AV scanning servers
 - Remove device from device lists used for scheduled scripts
 - Assign the VT to UK Corporate Wintel NT SA to remove device from scripts being executed on our behalf
 - Remove device related details from the qtree database
 - Remove from the supported device list database published on the EMEA Wintel Infrastructure web site
 - Update functional account tracking spreadsheet to show accounts are inactive
- ENI raise VT to the backup team queue "UK Infrastructure Backups" informing them of the device being decommissioned
- ENI login to NOW web site and set the device to decommissioned

- ENI organise with NetApp for the device to be collected
- ENI raise a VT ticket to cover the removal of decommissioned servers from DNS
- Update ENI filer details database to show the device as decommissioned

Internet Management

EMEA NAS Infrastructure do not host any external facing web services. EMEA NAS Infrastructure share an intranet site with EMEA Wintel Infrastructure and is registered with the CWHI.

Contracting and Outsourcing

EMEA NAS Infrastructure are not directly involved in the management of Contracting or Outsource negotiations.

Architecture

EMEA NAS Infrastructure adhere to architecture and infrastructure standards principally defined by Global Distributed Storage Engineering. Details of their standards can be found on their intranet site.

<http://catecollaboration.citigroup.net/domains/platstor/gdse/products/techstdshmpgs/netappfiler.aspx>

Project Management

EMEA NAS Infrastructure do not have any responsibilities with regard to Project Management.

Software Management

EMEA NAS Infrastructure do not have any responsibilities with regard to Software Management or for the deployment of wraps as requested by the business or other support or development groups.