

Navy Cash Training System Operational Procedures

Objectives

At the end of this unit you will be able to:

- Describe the cluster server and node management.
- State the reasons why backups are performed on a daily basis
- State the reasons why weekly maintenance is performed on the Navy Cash system

Node Management

Node Management

- Each node is attached to the cluster storage unit
- The cluster storage unit can be controlled by only one node at any point in time.
 - Ownership of the nodes can be transferred back and forth using the *Microsoft Cluster Administrator Application*

Note: Once every two weeks, shutdown and restart the server. Follow procedures to power down/up the two nodes and the data storage array unit. This maintenance action helps ensure proper system operation and frees up disk space.

Using KVM to Switch Between Nodes

- You will need to verify which node you're viewing before sending commands to the server.
- You can switch viewing by pressing "Scroll Lock" twice then "1" button for Node 1, "2" button for Node 2, and the "3" button for the Workstation, if the Workstation is sharing the KVM switch with the Server.

Cluster Administrator

- *Cluster Administrator* is a Windows application used to control and manage all the Navy Cash groups and resources
- All Navy Cash groups and resources are controlled by one node at a time
- The shared files and drives cannot be viewed if you are not on the controlling node

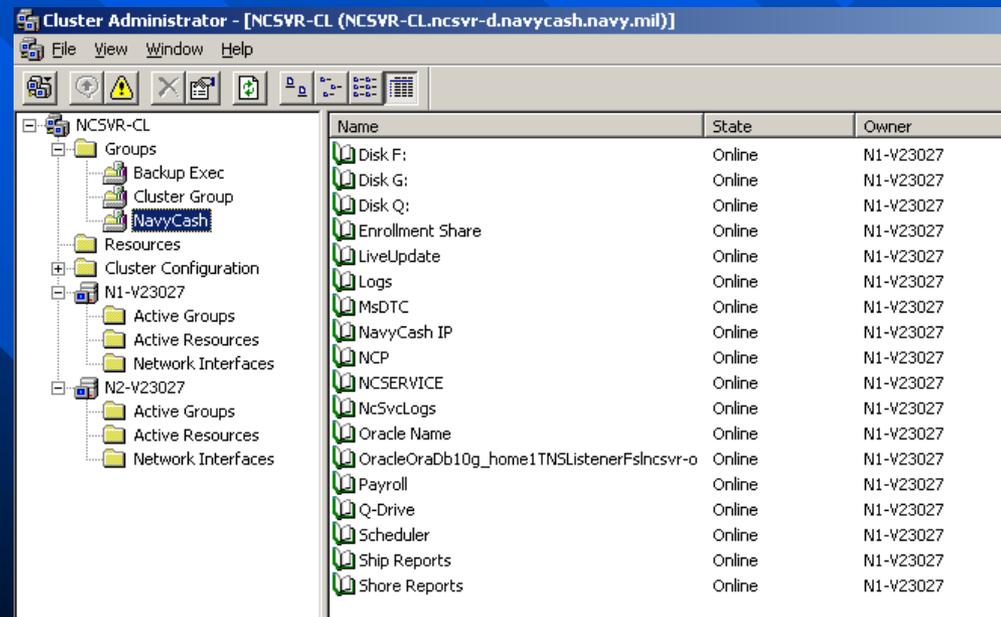
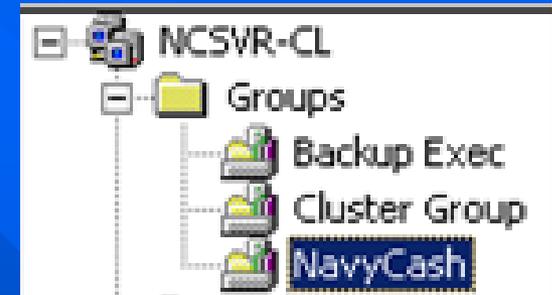


Cluster Administrator (cont)

- *Cluster Administrator* allows you to monitor the status of the cluster and check for fail-over or loss of ownership activities
- Fail-over can occur either as an entire node failure or a resource on a node fails
- Node failure is easily identified in *Cluster Administrator*

Verifying Ownership of Cluster

- **Step 1:** Open *Cluster Administrator*
Start → Programs → Administrative Tools
→ Cluster Administrator
- **Step 2:** Click *Groups* icon to display 4 group resources
- **Step 3:** Click on each resource to verify ownership. Each node is identified under *Owner* column.



Name	State	Owner
Disk F:	Online	N1-V23027
Disk G:	Online	N1-V23027
Disk Q:	Online	N1-V23027
Enrollment Share	Online	N1-V23027
LiveUpdate	Online	N1-V23027
Logs	Online	N1-V23027
MsDTC	Online	N1-V23027
NavyCash IP	Online	N1-V23027
NCP	Online	N1-V23027
NCSERVICE	Online	N1-V23027
NcSvcLogs	Online	N1-V23027
Oracle Name	Online	N1-V23027
OracleOraDb10g_home1TNSListenerFshncsvr-o	Online	N1-V23027
Payroll	Online	N1-V23027
Q-Drive	Online	N1-V23027
Scheduler	Online	N1-V23027
Ship Reports	Online	N1-V23027
Shore Reports	Online	N1-V23027

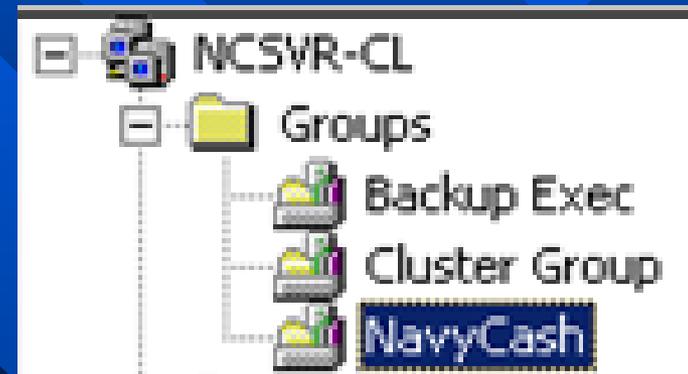
Moving Ownership of Cluster

- **Step 1:** Open *Cluster Administrator*

Start → Programs → Administrative Tools → Cluster Administrator

- **Step 2:** Click on *Groups* icon to display 3 group resources.

- **Step 3:** Right-click each *Group* icon and select “*Move Group*”.



File System Management

- The F:\, G:\, Q:\, V:\ and Z:\ drives are clustered share drives
- Remember, the controlling Node is the only node that can access the share drives and files on the *Cluster Storage Unit*

- The information contained on each drive is:

F:\ navy.cfg file

G:\ Oracle\NCP

Q:\ Data base and Live Update

V:\ Veritas Backup Exec

Z:\ Microsoft Clustering Service

File Verification

The Q:\ drive should be checked to make sure that there are no zipped files in:

Q:\files\navydata\scripts\logxfer\outgoing

After files are processed, the zipped files in these directories are renamed with a *.archive* extension

File Verification (cont)

- If any files are there without the archive extension, it is an indication that the system has lost off-ship communication
 - Tech support should be contacted only after ensuring that there are no other problems with your system

Note: *Shipboard Router ACL* entries must be made during integration, and maintained thereafter, to access the *Shore Navy Cash FTP* server for ship to shore data transmission

Note: *Ship's Configuration files* (navy. cfg file) are on the F drive under *NC Service* which can only be accessed from the controlling Node

Log File Verification (cont)

- Ensure there is communication between the *shipboard* Navy Cash server and the *shore* Navy Cash FTP server by utilizing one of the following FTP server addresses:
 - PACFLT uses 205.56.145.20 and LANTFLT uses 205.56.129.35
- On either Node from a cmd prompt type: ftp 205.56.145.20 or ftp 205.56.129.35 (shore Navy Cash FTP Server IP Addresses)
 - If prompted for a user ID, you have off-ship comms, *but* if it ‘times out’ or displays as ‘error’, you *do not* have off-ship comms

Daily Backups

Daily Backups

- Daily backups are CRITICAL:
 - If a backup fails, it must be addressed and corrected or log files will eventually fill the drive and crash the server
 - Completed backups will purge these logfiles
- Backup tapes are pre-labeled for each day
- Backup jobs run at 2200 and 2230 GMT
 - NSR File System Backup is run to back up Windows
 - NSR Oracle Backup is run to back up the Oracle Database

Performing Daily Backups

- Daily backups are performed automatically using *Backup Exec 11.0*
- It is the System Administrator's responsibility to ensure that the correct tape is in the node that has control of the cluster
- Tapes should be changed once a day
 - The tapes do not have to be used sequentially. If you miss a day ensure you use the current day tape for backups (e.g. if 12th day of the month, use tape numbered '12')
 - The tape number is to be matched to the day of the month

Performing Daily Backups (cont)

- The *Backup Exec* process and logs should be checked after every backup is finished to verify the successful completion of the backups
 - The *Backup Exec* job completion status can be read from the *Backup Exec* history tab
 - The *NSR File System Backup* and the *NSR Oracle Backup* should read “Successful”

Performing Daily Backups (cont)

- If the *NSR File System* fails or the *NSR Oracle Backup* fails without a byte count, check the *Event Logs* for important troubleshooting information

The screenshot displays the Veritas Backup Exec Job Monitor window. The interface includes a menu bar (Session, View, Tools, System, Draw, Help), a toolbar, and a main window with tabs for Backup, Restore, Overview, Job Setup, Job Monitor, Alerts, Reports, Devices, and Media. The Job Monitor tab is active, showing a list of current and historical backup jobs. A red arrow points to a job in the Job History list that failed.

State	Job Name	Device Name	Job Type	Job Status	Priority	Perce...	Start Time	Elapsed Time	B
Scheduled	NSR Oracle Backup	NAVYCASH	Backup	Scheduled	Medium		3/21/2011 10:30 PM		
Scheduled	NSR FILE SYSTEM BACKUP	NAVYCASH	Backup	Scheduled	Medium		3/21/2011 10:00 PM		

Job Name	Device Name	Job Type	Job Status	Percent ...	Start Time	Elapsed Time	
NSR Oracle Backup	HP 1	Backup	Failed		3/20/2011 10:32 PM	0:00:00	
NSR FILE SYSTEM BACKUP	HP 1	Backup	Cancelled	N/A	3/20/2011 10:00 PM	0:31:57	
NSR Oracle Backup	HP 1	Backup	Cancelled	N/A	3/19/2011 10:30 PM	0:01:16	
NSR FILE SYSTEM BACKUP	HP 1	Backup	Cancelled	N/A	3/19/2011 10:00 PM	0:02:27	
NSR Oracle Backup	HP 1	Backup	Cancelled	N/A	3/19/2011 2:21 AM	0:02:50	
NSR FILE SYSTEM BACKUP	HP 1	Backup	Completed ...	100%	3/18/2011 10:00 PM	4:21:06	40,060,87
NSR Oracle Backup	HP 1	Backup	Cancelled	N/A	3/18/2011 2:21 AM	0:03:49	
NSR FILE SYSTEM BACKUP	HP 1	Backup	Completed ...	100%	3/17/2011 10:00 PM	4:21:02	40,048,94
NSR Oracle Backup	HP 1	Backup	Cancelled	N/A	3/17/2011 2:20 AM	0:03:13	
NSR FILE SYSTEM BACKUP	HP 1	Backup	Completed ...	100%	3/16/2011 10:00 PM	4:20:31	40,030,5E
NSR Oracle Backup	HP 1	Backup	Cancelled	N/A	3/16/2011 2:20 AM	0:03:13	
NSR FILE SYSTEM BACKUP	HP 1	Backup	Completed ...	100%	3/15/2011 10:00 PM	4:20:31	39,962,3E
NSR Oracle Backup	HP 1	Backup	Cancelled	N/A	3/15/2011 2:22 AM	1:37:07	
NSR FILE SYSTEM BACKUP	HP 1	Backup	Completed ...	100%	3/14/2011 10:00 PM	4:22:47	39,906,91
NSR Oracle Backup	HP 1	Backup	Cancelled	N/A	3/13/2011 10:30 PM	0:01:17	
NSR FILE SYSTEM BACKUP	HP 1	Backup	Cancelled	N/A	3/13/2011 10:00 PM	0:02:17	
NSR Oracle Backup	HP 1	Backup	Cancelled	N/A	3/13/2011 4:00 AM	0:01:17	
NSR FILE SYSTEM BACKUP	HP 1	Backup	Cancelled	N/A	3/12/2011 10:00 PM	5:59:58	
NSR Oracle Backup	HP 1	Backup	Failed		3/11/2011 10:30 PM	0:29:05	8,397,8E
NSR FILE SYSTEM BACKUP	HP 1	Backup	Failed		3/11/2011 10:00 PM	0:03:27	
NSR Oracle Backup	HP 2	Backup	Cancelled	N/A	3/11/2011 4:01 AM	0:09:08	
NSR FILE SYSTEM BACKUP	HP 2	Backup	Cancelled	N/A	3/10/2011 10:00 PM	6:02:23	

Ver
1.4.6.3

Weekly Maintenance

Weekly Maintenance Tasks

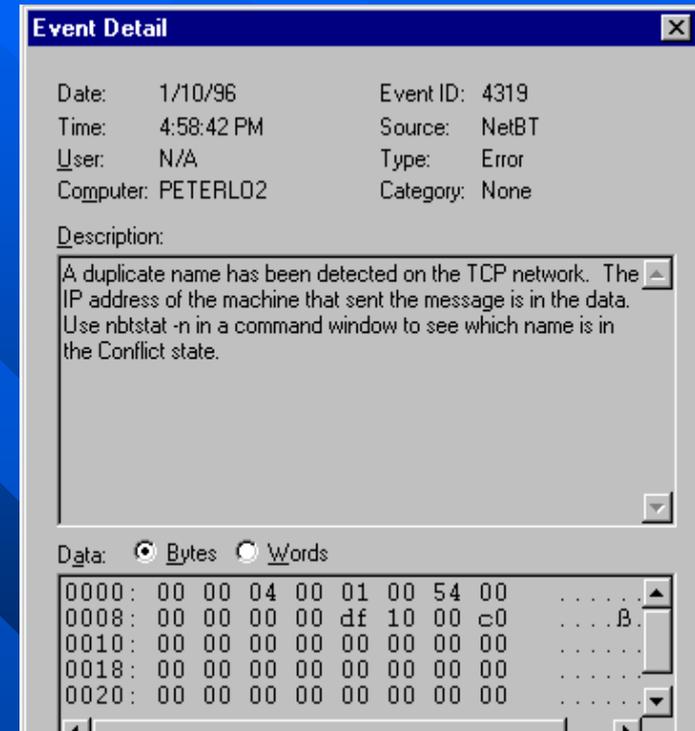
- *Weekly* maintenance tasks are performed to maintain system resources at optimal level:
 - Ensure drives F:\, G:\, Q:\, V:\ have a *minimum* 1GB free space
 - » If these drives do not have free space, this is an indication that backups may not have been successfully completed
 - Launch *Cluster Administrator* and verify that all resources are *online* and on the same Node

Monthly Task

- Clean tape drives
- Clear alerts from *Veritas Backup Exec*
- Connect laptops not being used to a Navy Cash LAN drop and perform a *Live Update* for the Virus definitions
 - less time consuming if done every two weeks
- Verify that Virus definitions on all Navy Cash workstations and laptops are up to date

Verify Event Viewer

- Access *Event Viewer* through the *Start Menu*
 - **Step 1:** Search all event logs for events displaying an error or warning icon
 - **Step 2:** Double-click message to open and view more detail on errors or warnings
 - **Step 3:** Report all errors or warnings to technical support personnel via daily reporting methods



Verify Batch Processing

- Perform the following steps in order to ensure the End of Day (EOD) processed correctly on shore:
 - **Step 1:** On the controlling node, ensure there are no files in directory:
`Q:\files\navydata\error\UIC_batchID.yyyymmdd`
 - **Step 2:** Check `Q:\files\navydata\log:` for presence of new *process_ship2shorepost.yyyymmdd.hhmiss.log* files
- Note:** Review the summary file; it indicates if the round trip was successful or not

Verify Batch Processing (cont)

- **Note:** Step 6 of the summary file will fail several times until the file info has been processed on the shore side and the database has been updated
- A failure at any other step might be an indication of an issue. Troubleshoot those various other steps and if you are unable to find the cause of the failure then the Navy Cash Call Center should be contacted immediately.

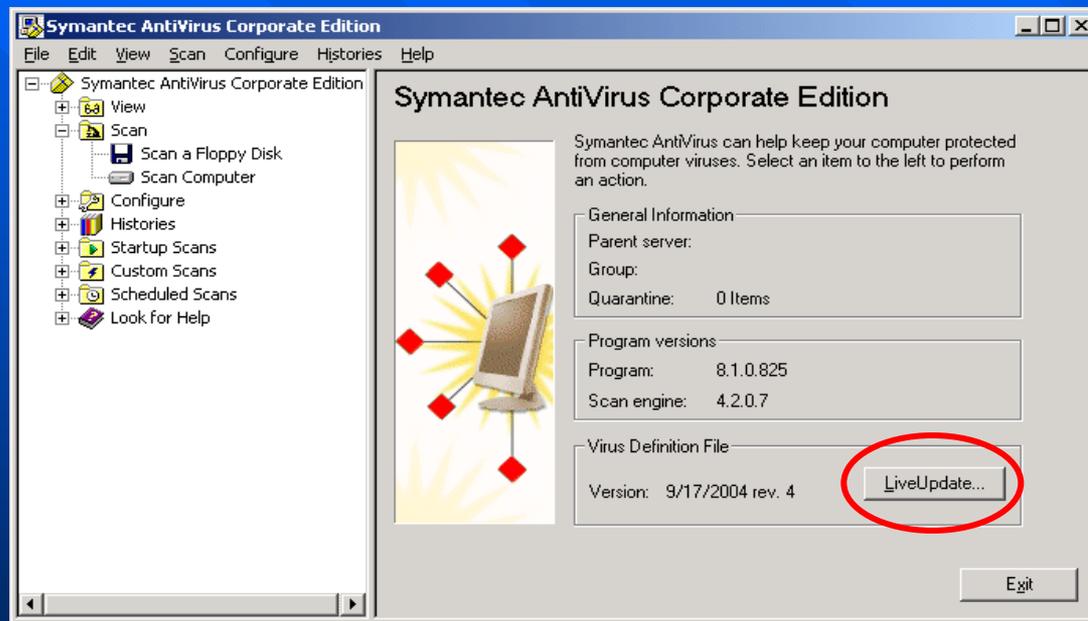
Live Update

- *Live Update* utility provides antivirus definition updates to the server, workstations, and laptops provided that a user is logged on
 - These updates protect the system from the most current web security threats
- To access the software and manually conduct an antivirus update:
 - Log on as ‘nc-admin’
 - Double click the gold shield icon on lower right side of the task bar
 - Click ‘*LiveUpdate*’ to start the process



Live UpDate (cont)

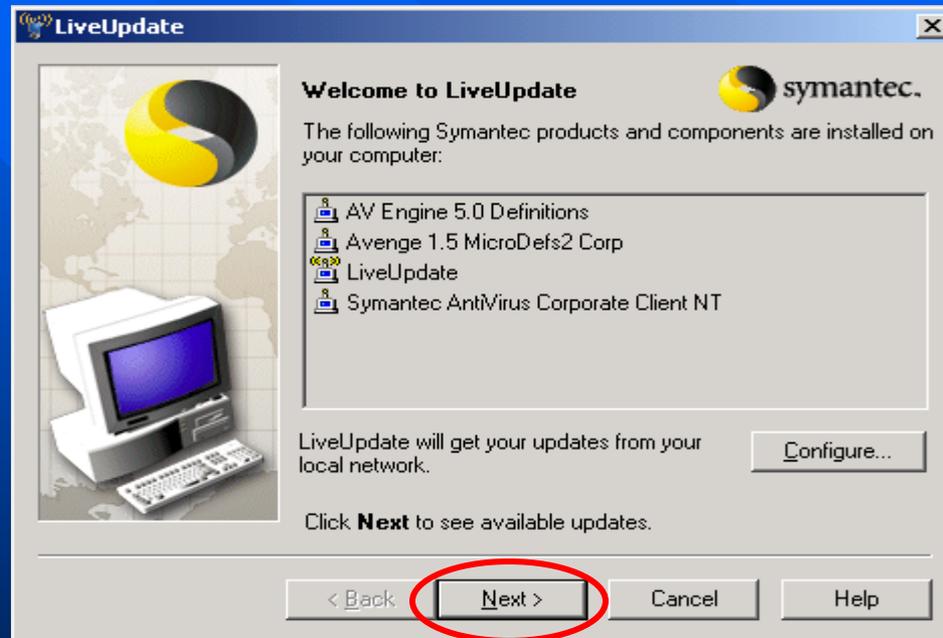
- When the gold shield icon is clicked, the following screen will appear:



- To run LiveUpdate, click *LiveUpdate*

Live UpDate (cont)

- After pressing *LiveUpdate*, the following screen will appear:



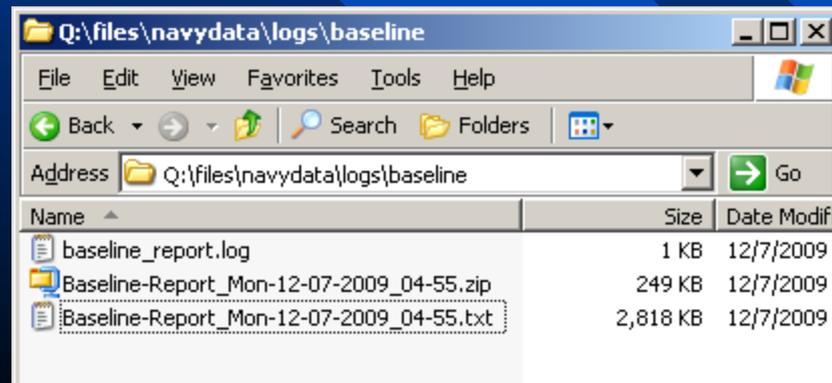
- Click *Next* and the most current virus definitions will be loaded into the system

INFOCON III Requirement ST3-5

- Infocon III Reporting software is installed automatically as part of the image
 - The comparison should be done quarterly.
- Verify that the "Sys Baseline" task is Enabled in the *Scheduled Tasks* window.
- The folder location where the initial baseline dump was generated is Q:\files\navydata\logs\baseline\

Steps to Process INFOCON III Requirement ST3-5

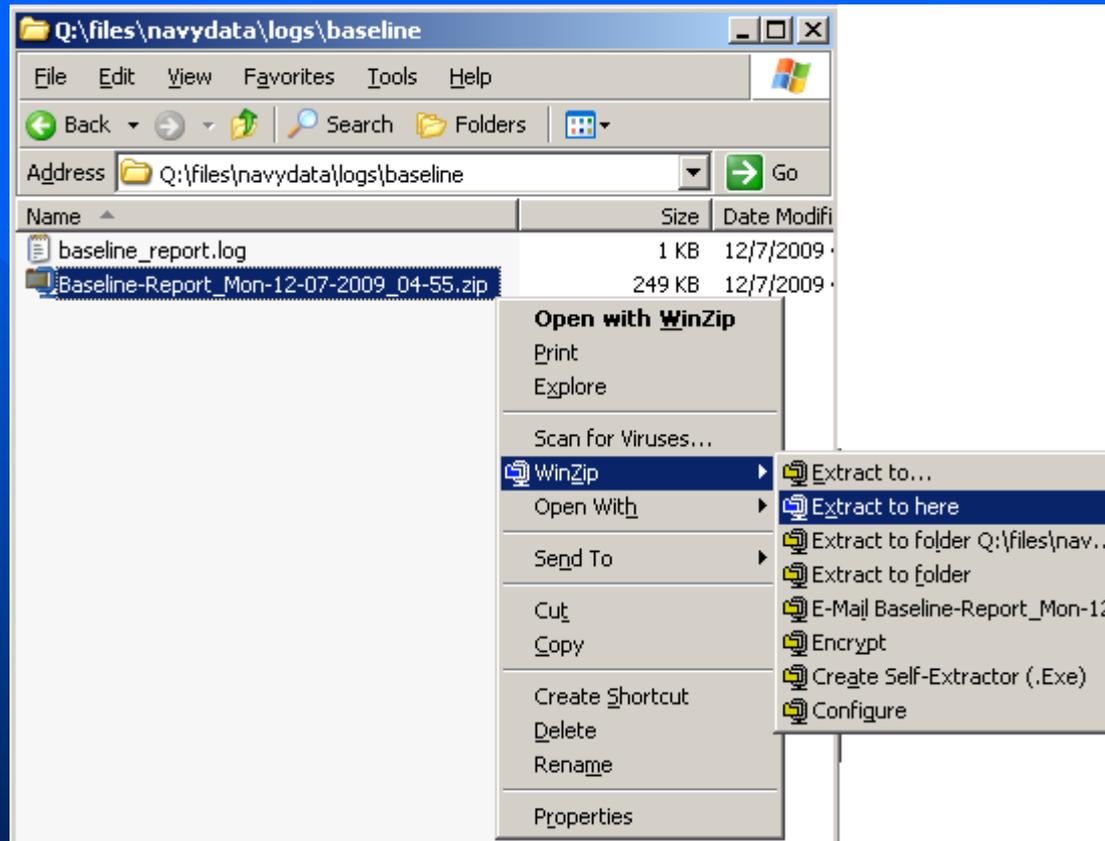
- The following steps must be performed from the Active Node.
- Using *Windows Explorer*, proceed to the folder where the Infocon III dumps reside: Q:\files\navydata\logs\baseline\
 - Dumps are named as "Baseline-Report_ddd-mm-dd-yyyy_hh-mm" where the file's suffix is a timestamp. For example:
Baseline-Report_Fri-04-02-2010_15-00
- Dumps are created as TXT files which are then compressed into ZIP files to conserve disk space. For each unique dump, the TXT and ZIP filenames will be identical, with exception of the file's extension TXT / ZIP.



Steps to Process INFOCON III Requirement ST3-5

- Locate the two Infocon III dumps (ZIP files) that you wish to compare
 - The suggested approach is to compare the most recent dump with the last dump compared
- Right-click the first dump file you chose to compare and select *WinZip > Extract to here* as shown on the next slide:

Steps to Process INFOCON III Requirement ST3-5



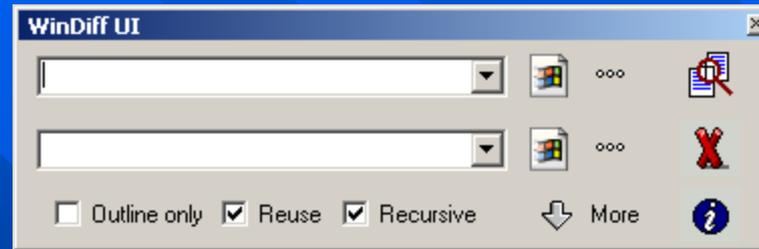
Note: This will extract the dump's TXT file into the same folder as the ZIP file

Steps to Process INFOCON III Requirement ST3-5

- Repeat previous step for the second dump file you chose to compare
- On the active Node's desktop, double-click the *WinDiff* icon:
 - If the icon is missing, the application can be launched manually using *Windows Explorer* and going to *Q:\files\navydata\bin\windiff* then double-clicking *RunWinDiff.exe*
 - Note that *Windiff* is a tool that simplifies comparing differences between two files

Steps to Process INFOCON III Requirement ST3-5

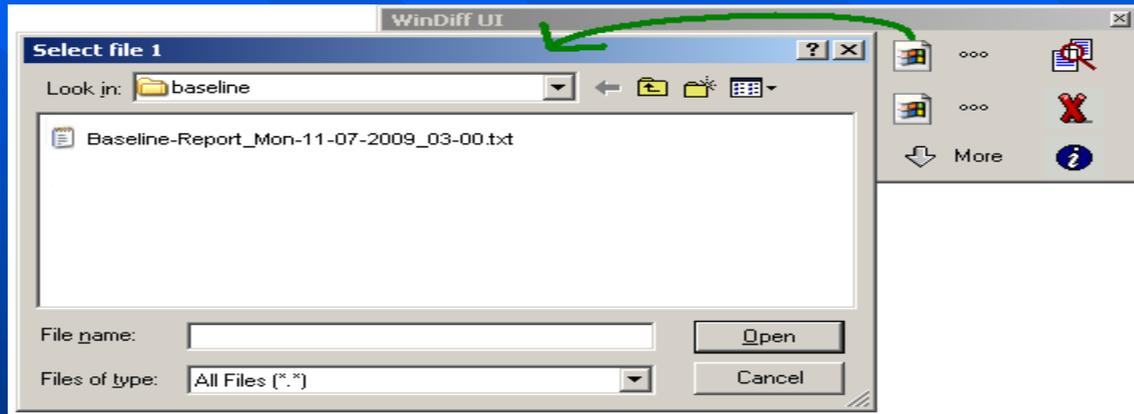
- The following window will appear on the screen:



Note: The first two fields are the *only* selections you need to change. Ensure the other settings remain as shown in the above screenshot.

Steps to Process INFOCON III Requirement ST3-5

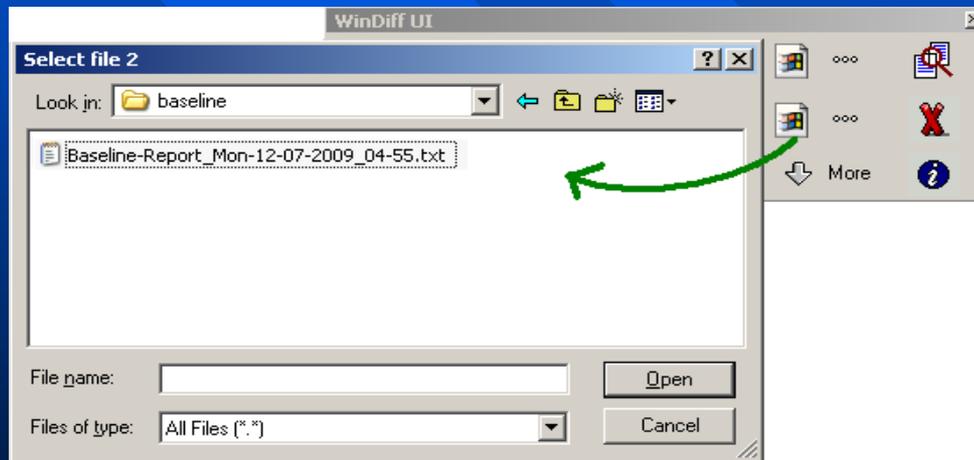
- Select the first dump file to compare by clicking the upper white button as shown here:



Note: This file should be the dump TXT that was generated *previous to* the latest dump

Steps to Process INFOCON III Requirement ST3-5

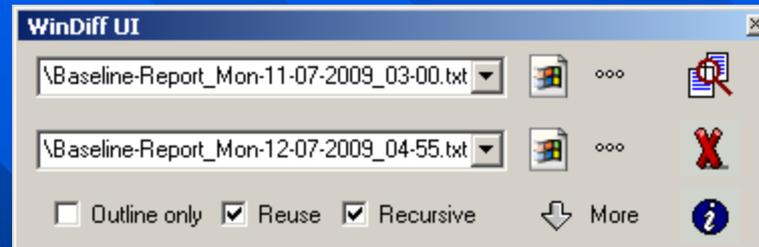
- Single-click the desired TXT file to compare and click *Open*
 - This will place the file's name into the *WinDiff* screen
- Select the second dump file to compare by clicking the lower white button as shown below:



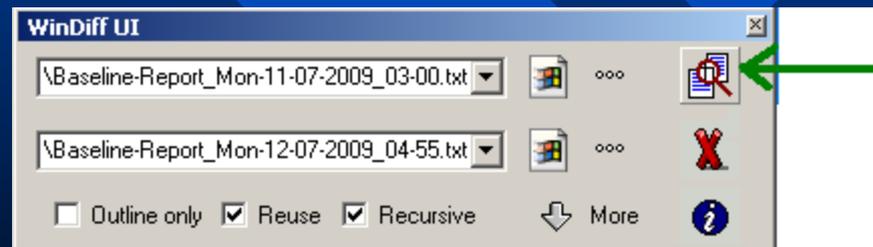
Note: This file should be the dump TXT that was generated more recently

Steps to Process INFOCON III Requirement ST3-5

- Single-click the desire TXT file to compare and click *Open*
 - This will place the file's name into the *WinDiff* screen
- Once both files have been selected, the window should look as follows:

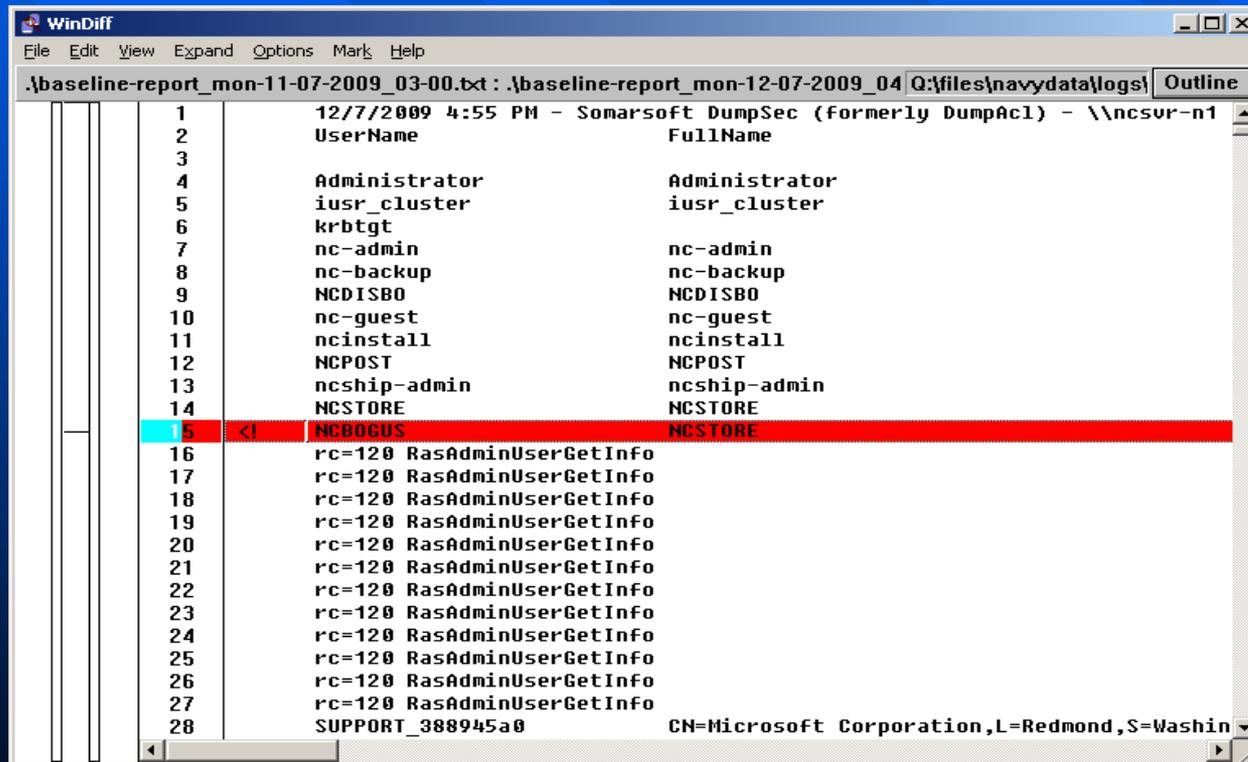


- Click the magnifying-glass icon to begin the comparison:



Steps to Process INFOCON III Requirement ST3-5

- Once *WinDiff* completes the comparison between the two dump files you chose, the *WinDiff* screen will highlight any differences found, as shown in this example:



```
WinDiff
File Edit View Expand Options Mark Help
.\baseline-report_mon-11-07-2009_03-00.txt : .\baseline-report_mon-12-07-2009_04 Q:\files\navydata\logs | Outline
1 12/7/2009 4:55 PM - Somarsoft DumpSec (formerly DumpAcl) - \\ncsvr-n1
2  UserName                      FullName
3
4 Administrator                  Administrator
5 iusr_cluster                    iusr_cluster
6 krbtgt
7 nc-admin                        nc-admin
8 nc-backup                       nc-backup
9 NCDISBO                         NCDISBO
10 nc-guest                        nc-guest
11 ncinstall                       ncinstall
12 NCPOST                          NCPOST
13 ncship-admin                    ncship-admin
14 NCSTORE                         NCSTORE
15 <| NCBOGUS                      NCSTORE
16 rc=120 RasAdminUserGetInfo
17 rc=120 RasAdminUserGetInfo
18 rc=120 RasAdminUserGetInfo
19 rc=120 RasAdminUserGetInfo
20 rc=120 RasAdminUserGetInfo
21 rc=120 RasAdminUserGetInfo
22 rc=120 RasAdminUserGetInfo
23 rc=120 RasAdminUserGetInfo
24 rc=120 RasAdminUserGetInfo
25 rc=120 RasAdminUserGetInfo
26 rc=120 RasAdminUserGetInfo
27 rc=120 RasAdminUserGetInfo
28 SUPPORT_388945a0              CN=Microsoft Corporation,L=Redmond,S=Washin
```

Steps to Process INFOCON III Requirement ST3-5

- Some helpful tips:
 - Click *Options* from the menu bar and locate "Show Identical Lines". When unchecked, it will only show the differences found by omitting identical data
 - Lines found only in the **top** file are shown on a red background
 - Lines found only in the **bottom** file are shown on a yellow background
 - Lines common to both files are shown on a white background
 - To skip from one difference to the next, press F8 (move forward) or F7 (move reverse)

Steps to Process INFOCON III Requirement ST3-5

- If differences are present which the IAO has previously outlined as unacceptable:
 - Provide to the IAO the INFOCON III Report for further analysis and the ZIP files of the two dumps that you compared
- Any approved differences must be added to the last “known good” baseline dump TXT file
- To keep the Infocon III dump folder clean, please delete the *TXT* files that you previously extracted using WinZip
- Make certain *NOT* to delete any *.ZIP* files from this folder

Summary

- Utilize *Cluster Administrator* to ensure only one Node is the owner of all cluster resources within each cluster group at any given time, and ensure an *online* status
- Daily and weekly tasks mainly consist of backup data verification, switching of backup tapes, verification of EOD and ship to shore files processing
- View the *Event Viewer* for any errors that may have occurred on Node 1 and /or Node 2

Summary (cont)

- Do not change the computer name of a cluster Node
- Do not change the computer time from GMT [syncs ship and shore data]
- Do not re-assign the drive letters of the system disks on the Nodes
- Verify that all cluster nodes can detect one another over the network utilizing the *Ping* command
- Check all Event logs on both nodes for any error messages