



# Navy Cash Training System Operational Procedures Unit 2



# Objectives

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

- Describe the cluster server and node management.
- Describe the servers and Overland Storage.
- State the reasons why weekly maintenance is performed on the Navy Cash system.

# Node Management

# Node Management

- Each node (Member Server (MS)) has a Virtual Machine (Domain Controller (DC)).
- The Microsoft Failover Cluster Manager Application resides only on the Member Server on each node.
- Active Directory and other administrative functions can be accessed on either the MSs or DCs.

# Node Management (cont)

- Each node is attached to the Overland Storage unit.
- Each Overland 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 Failover Cluster Manager Application.

# 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 of Nodes by pressing the “1” button on the KVM for Node 1, “2” button for Node 2.



# Failover Cluster Manager

- Failover Cluster Manager is a Windows application used to control and manage all Navy Cash resources. This resides on the Member Server (MS) on each node.
- All Navy Cash 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.

# Failover Cluster Manager (cont)

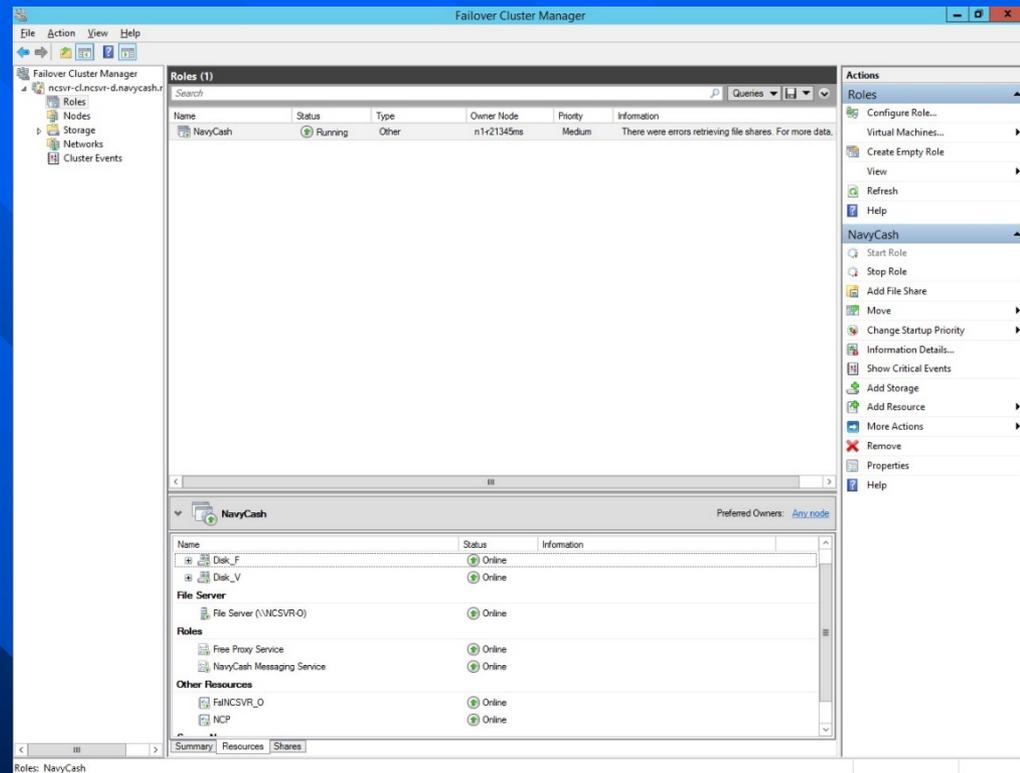
- Failover Cluster Manager allows you to monitor the status of the cluster and check for fail-over or loss of ownership activities.
- Fail-over can occur either as an entire node failure or a resource on a node fails. Node failure is easily identified in Failover Cluster Manager.

# Verifying Ownership of Cluster

## ■ Step 1: Open Failover Cluster Manager

Start → Programs →  
Administrative Tools →  
Failover Cluster Manager.

## ■ Step 2: Under Failover Cluster Manager, expand ncsvr-cl.ncsvr-d.navycash.navy.mil. Then click on Roles.



# Verifying Ownership of Cluster (cont)

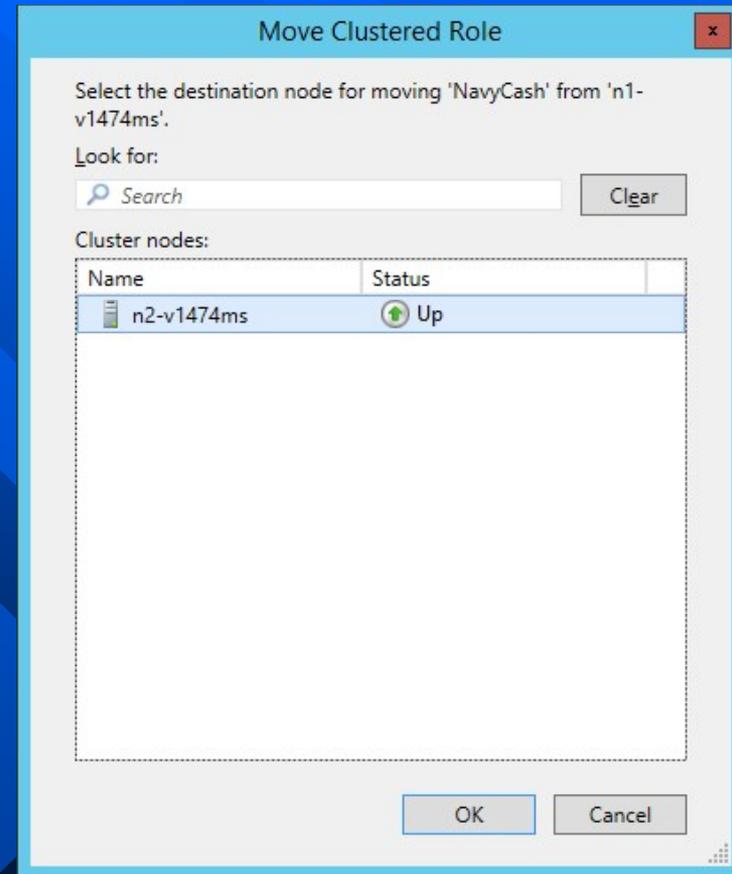
- **Step 3:** Click on Navy Cash. In the middle window you will see which node is in control next to ‘Current Owner’.
- **Step 4:** At the bottom of the middle pane, click on the Resources Tab to see the individual resources.

The screenshot displays the Failover Cluster Manager interface. The main window shows the 'Roles (1)' tab with a table listing the 'NavyCash' role. The role is in a 'Running' status, owned by node 'n1-r21345ms', and has a 'Medium' priority. Below this, the 'Resources' tab is selected, showing a list of resources for the 'NavyCash' role. The resources are categorized into 'File Server', 'Roles', and 'Other Resources'. The 'File Server' section includes 'Disk\_F' and 'Disk\_V', both in 'Online' status. The 'Roles' section includes 'Free Proxy Service' and 'NavyCash Messaging Service', both in 'Online' status. The 'Other Resources' section includes 'FailNCSVR\_O' and 'NCP', both in 'Online' status. The 'Preferred Owners' are listed as 'Any node'.

Name	Status	Information
Disk_F	Online	
Disk_V	Online	
<b>File Server</b>		
File Server (\NCSVR-O)	Online	
<b>Roles</b>		
Free Proxy Service	Online	
NavyCash Messaging Service	Online	
<b>Other Resources</b>		
FailNCSVR_O	Online	
NCP	Online	

# Moving Ownership of Cluster

- **Step 1:** Open Failover Cluster Manager Start → Programs → Administrative Tools → Failover Cluster Manager.
- **Step 2:** Right-click on Navy Cash, select Move, then click on Select Node.
- **Step 3:** Note that the other node is selected. Click OK.



# File System Management

- The F:\, 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 Overland Storage Unit.

- The information contained on each drive is:

F:\ navy.cfg file

F:\ Oracle\NCP

F:\ Data base and Live Update

V:\ Backup Files and Logs

Z:\ Microsoft Clustering Service

# Log File Verification

- Ensure there is communications between the shipboard Navy Cash server and the shore Navy Cash SFTP server by utilizing the following. On either Node from an elevated command prompt type: telnet  
gppfts.navycash.fiscal.treasury.gov 22 (shore Navy Cash FTP Server IP Addresses port 22) to establish and confirm communications between the shipboard Navy Cash server and the shore Navy Cash FTP server. If the result states 'SSH-2.0-OpenSSH\_4.3' then you have good SFTP communications.

# Daily Backups

# Daily Backups

- Backups are done on hard drives and are located on the servers and Overland Storage Device.
- Backup Logs can be found at V:\logs.
- The backup job is called Daily Backup (Scheduled Tasks) and runs at 0400 GMT. This backup includes the Windows File System Backup, Oracle Backup (former expncp.dmp).
- Daily backups are CRITICAL:
  - If a backup fails, it must be addressed and corrected, or log files may fill the drive, and eventually crash the server.
  - Completed backups will purge these log files.

# Weekly Maintenance

# Weekly Maintenance Tasks

- Weekly maintenance tasks are performed to maintain system resources at optimal level:
  - Ensure that drives F:\ and V\ have at minimum 10-20% free space.
    - » If these drives do not have free space, this is an indication that backups may not have been successfully completed.

# 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  
F:\files\navydata\error\UIC\_batchID.yyyymmdd directory.
  - **Step 2:** Check the  
“F:\files\navydata\log\UIC\_batchID.yyyymmdd directory: directory for presence of new  
“process\_ship2shorepost.yyyymmdd.hhmiss.log” files.
  - The summary file indicates if the round trip was successful or not.

# Verify Batch Processing (cont)

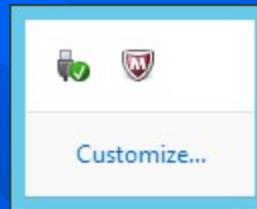
- **Step 3:** Step 6 of the summary file may fail several times until the file info has been processed on the shore side and the database has been updated.
- A failure at any other step might be an indication of an issue. Troubleshoot those various other steps and if you are unable to find the cause of the failure then the Navy Cash Central Support Unit (CSU) should be contacted immediately.

# McAfee Anti Virus

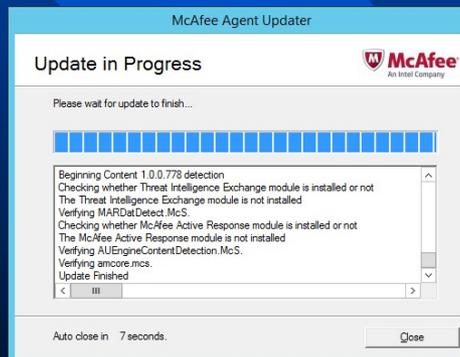
- Updates are automated, but can be done manually.
- McAfee provides antivirus definition updates. These updates protect the system from the most current web security threats. Updates are done automatically to the servers, workstation(s), and laptop(s), provided that a user is logged on.

# McAfee Anti Virus (cont)

- Click on the arrow to the bottom right of the screen, the below will pop up.



- To manually update AV definitions, right click the McAfee icon and select Update Security. Follow the prompts. It will automatically close when done.



# Update Spare Workstation

If the spare workstation is not used on a daily basis, it should be plugged into a Navy Cash drop and logged onto to manually run the Anti-virus program at least once a week. Additionally, the spare workstation should be left plugged in to a Navy Cash drop and left logged on for a minimum of 24 hours to allow all security updates to be downloaded and installed.

# ACAS Scanning

- Scans are to be done on the Navy Cash Member Servers, Navy Cash Domain Controllers, and all Navy Cash Workstations.
- Instructions to accomplish ACAS Scans are provided to ship's force upon completion of installation of the Navy Cash System.

# Weekly Tasks

- Verify that anti-virus definitions on the Navy Cash servers and workstations are up to date.

# Summary

- Daily and weekly tasks mainly consist of verification of EOD and ship to shore files processing.
- Do not change the computer name of the servers or workstation.
- Do not change the computer time from GMT.
- Do not re-assign the drive letters of the system disks on the server or workstations.

# Questions

