COLUMBIA GORGE
COMMUNITY COLLEGE

Information Technology Services

Disaster Procedures and Recovery Manual

Bill Bohn
Chief Technology Officer

Adam Gietl
Manager of Network Services

Created: August 2010
Last Modified: May 2013, Nov 2017

OVERVIEW OF THIS DOCUMENT

This document outlines the disaster preparedness, planned activities for during a disaster and disaster recovery procedures as they apply to CGCC's Information Technology Services Data Center. The procedures include detailed specifics of what is performed, at what location, and by whom. Included with the procedures, are lists outlining the required equipment, software, user names and required passwords.

Due to the network access level necessary to perform these tasks, this document should be considered highly confidential. Draft copies will NOT include password information.

This document is broken down into 10 sections: Page

1.0 Introduction 4
2.0 Contact Information 5
3.0 Disaster Preparation 7
3.1 Alert Notification 8
3.2 Electrical Power Supply to the Data Center and Wire Closets 9
3.2.1 Uninterrupted Power Supply (UPS) 9
3.2.2 American Power Conversions (APC) Edge Units (Wire Closets) 12
3.2.3 Generator 14
3.3 Data Protection 15
3.3.1 Offsite (cloud) Backup 15
3.3.2 Tape Backup System 15
3.3.3 Storage Area Network (SAN) Snapshot & DR Unit 19
3.3.3.1 Windows/Netware SAN Volume Recovery in VMWare 20
3.3.3.2 Microsoft Windows Server Data (D:\) Volume Recovery 29
3.3.3.3 Novell Netware Server Data (VOL1:\) Volume Recovery 37
3.3.3.4 Windows/Netware OS. Boo Partition & Complete Server Restore 46
3.3.4 VMWare Virtual Server Hosting 58
3.3.5 User Security Redundancy (eDir & Windows domain) 59
3.3.6 Moodle Backup 59
3.4 Hardware & Network Infrastructure Precautions 60
3.4.1 Server Hardware 60
3.4.2 Cisco POE Wire Closet Switches (extra & stored configurations) 61
3.4.3 Core Switch Hardware & Route redundancy 61
3.4.4 Physical Security 62
3.4.5 Environmental Controls 63
3.5 Future Plans 64
4.0 Mid-Disaster Procedures 65
4.1 Activity Checklist 65
4.1.1 Communication 65
4.1.2 Power Outage 66
4.1.3 Environmental Unit Failure (Heat) 66
5.0 Data Center Shutdown Procedures 67

5.1 Partial Shutdown 70
5.2 Complete Graceful Shutdown 71
5.2.1 Process the Shutdown steps as outlined section 5.0 in the following order 72
5.2.2 Phone System Shutdown 74
5.2.3 VMWare Servers 74
5.2.4 SAN 75
5.2.5 APC Shutdown 75
5.2.6 Liebert Units 75
6.0 Emergency (Quick) Shutdown (15 min or less power or over 95 degrees) 76
7.0 Data Center Startup Procedures 78
7.1 Process the STARTUP steps as outlined section 6.0 in the following order 79
8.0 Hood River Indian Creek Campus – Startup & Shutdown 81
9.0 Disaster Recovery 84
10.0 Document Modification Log 85

Each section contains:

- Required Equipment & Software
- Detailed Instructions of activities
  - Primary Lead Person

1.0 INTRODUCTION

Disaster recovery is the process, policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster.

Disaster recovery planning is a subset of a larger process known as business continuity planning and should include planning for resumption of applications, data, hardware, communications (such as networking) and other IT infrastructure. A business continuity plan (BCP) includes planning for non-IT related aspects such as key personnel, facilities, crisis communication and reputation protection, and should refer to the disaster recovery plan (DRP) for IT related infrastructure recovery / continuity. This document focuses on disaster recovery planning as related to IT infrastructure.

Each section begins with basic information regarding the section. This includes a chart for the areas of protection/recover as shown below.
Since some systems are put in place to protect a variety of areas, the following chart accompanies each systems introduction section. An example of a system protecting multiple areas is the use of UPS's. By protecting and providing a consistent power supply, we protect all aspects of BCP. Power keeps the Infrastructure working, power keeps the Hardware working, steady power helps prevent the hardware from corrupting Data, and consistent power reduces application error.

Areas of recovery / protection

Applications	Data	Hardware	Infrastructure	
			Data Center	Edge

2.0 CONTACT INFORMATION

This is followed by the primary & secondary Lead information:

Lead Staff	Name	Home Phone	Mobile Phone
CGCC Primary	Bill Bohn	[redacted]	[redacted]
CGCC Secondary	Adam Gietl	[redacted]	[redacted]
Tech III	Richard Jepson		[redacted]
Online Specialist	Danny Dehaze		[redacted]
Tech I/Lab Aide	Ron Watrus		[redacted]
Vendor	**Name**	**Office**	**Mobile**
Compellent	CoPilot Support Controller ID #'s [redacted], [redacted] Hsn#(same as controller #)	[redacted]	[redacted]
C2ITSystems	Tech Phil Thompson	[redacted]	[redacted]
Dell	Server Support ID# 7 digit TAG Account Rep Pleschette Fontenet	[redacted]	[redacted]
ESD	Internet, Firewall, DNS Eric Harrison, eharrison@mesd.k12.or.us Dan Young, Cody Harmon charmon@cgesd.k12.or.us NOC noc@mesd.k12.or.us noc@cascadetech.org	[redacted]	[redacted]
eThink Education	Claire Machia claire.machia@eThinkEducation.com	[redacted]	
Fire	Fire Dept	[redacted]	[redacted]
HREC	John Gerstenberger Simien HRICC<-to->TDC	[redacted]	[redacted]

	Service from HRICC->HREC		
Insight Web Publishing	Paul Irving		
Integra	ApplicationXtender Tech Support Beau Brazier beau.brazier@integraECM.com Joe Roche joe.roche@integraECM.com	[redacted]	[redacted]
LS Networks	Circuit ID [redacted] CACHE/Columbia Gorge Comm. College, HDRV-THDL Service from HREC->TD Mark Waldo Sr. NOC Engineer mwaldo@lsnetworks.net Lief Hanson	[redacted]	[redacted]
LS Networks	LS Networks 921 SW Washington St., Ste 370 Portland, OR 97205 www.lsnetworks.net	[redacted]	
Matrix	Shoretel Support Techs Jason Bow Krizzia Muehleck Acct Rep: Tim Lopez	[redacted]	
May Technologies	Mike Neeley		
Microsoft	Technical Support Server OS Support	[redacted]	
NeWest Technologies	RMS – Support [redacted]	[redacted]	
Novacoast	Tech: Rob Aronson Tech: John Walls	[redacted]	[redacted]

	Northwest Rep: PJ Anderson		
Novell	Technical Support	[redacted]	[redacted]
Pacific Office Automation	Copier Support Acct Manager Jeff Simon	[redacted]	[redacted]
Police		[redacted]	[redacted]
Series25 Live	Account Manager Andrew Van Dyk avandyk@collegenet.com	[redacted]	
Symantic Backup Exec	Technical Support ID: [redacted]	[redacted]	[redacted]
SYN-Apps	SA-Announce Tech Greg Banse		[redacted]
VMWare	Virtual environment Acct: helpdesk@cgcc.cc.or.us	[redacted]	[redacted]

3.0 DISASTER PREPARATION

This section reviews the areas of preparedness, the equipment in place, the procedures used on the equipment, and the person(s) responsible for the activities.

3.1 Alert Notification

All of the College's critical systems incorporate an alert notification in case of problems. Each system alert parameters are set based on that system's purpose and monitoring capability. This document outlines each of the systems parameters and recipients.

For ease of future maintenance, all systems send their alert to a single email account:
ZX-CriticalAlerts@cgcc.edu

The ITS Department configures the CriticalAlerts account to recognize what system sent the email, and who to be notified by email &/or text messaging. By using this single, central notification account, modifying the specific recipient list can be done in one place, versus modifying each system when an email or text message address changes.

CriticalAlerts account rule configuration is defined for sending alerts based on: (check CriticalAlerts account for notification list)
Subject of "HVAC" & "Critical"
Subject of "HVAC" & "General"
Or forwarding ANY message submitted

3.2 Electrical Power Supply to the Data Center and Wire Closets

3.2.1 Uninterrupted Power Supply (UPS)

American Power Conversions (APC) Data Center UPS

Areas of recovery / protection

Applications	Data	Hardware	Infrastructure	
			Data Center	Edge
✓	✓	✓	✓	

Primary Contacts:

	Name	Home Phone	Mobile Phone
Primary	Adam	[redacted]	[redacted]
Secondary	Bill Bohn		
Past	Chris McQuade		
Vendor Support	APC		

Description:

The Data Center APC UPS is located in the Data Center. It consists of four different functional units, Batteries, distribution, Management, and Monitoring

The APC UPS functions primarily to provide uninterrupted power for a short period of time. Short period of time means that the unit will provide consistent clean power for power spikes, dips or during an outage until the generator provides emergency power. The system will provide roughly one (1) hour of power once the generator stops.

Scope of protection:

This unit protects all of the electrical equipment inside the black cabinets and mounted on the back set of racks. It does NOT provide power to lights or environment control units.

Parameters of protection:

Provides clean uninterrupted power to the above scope for one (1) hour.

Monitoring/Notification:

There are two monitoring unit hubs, one located in each cabinet row. The front row uses one temperature monitor and one temperature/humidity monitor. The back row uses two temperature monitors and one temperature/humidity monitor. (This is also outlined in the Environment section)

All monitors are set with the following event settings:

- High temperature
- Low temperature
- High humidity
- Low humidity
- Fast short term temperature gain/loss
- Long term temperature gain/loss
- All monitors are set to text and email the following:
  - ZX-CriticalAlerts@cgcc.edu

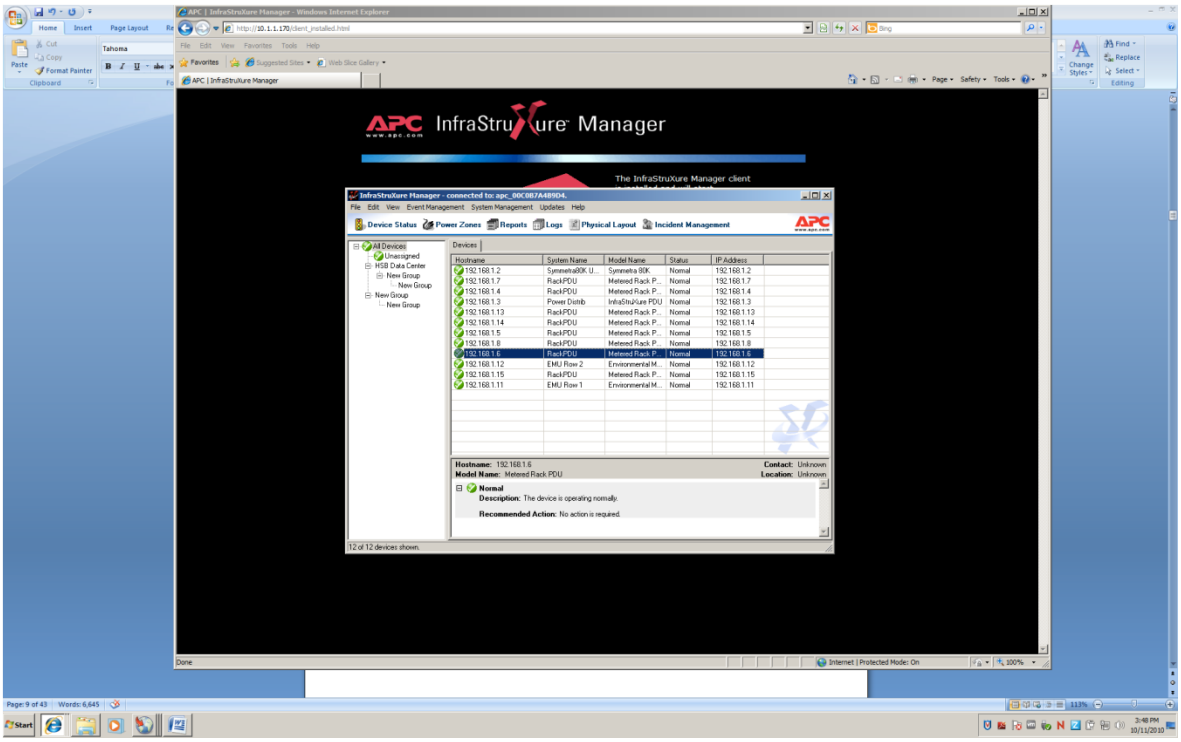
This account forwards the message based on the sender. Recipients for the APC unit include:

- B.Bohn, A.Gietl, J.Austin

#1) Login Instructions for APC-Infrastruxure Server (monitored in Xymon)

This is the Main APC server that monitors the APC, all power and environmental components of the Server Room rack infrastructure. This server sends out an e-mail notification of a power alarm or an environmental alarm conditions in the server room. Prerequisite: User will be prompted to install APC client software from website below. **Highly Recommend using citrix.cgcc.edu to login to APC-Infrastruxure Mgr** Using Internet Explorer, accept and install the InfraStruxure Mgr. Software if you do not already have this software. After software installed, login to [redacted]

To check an alarm state double click on the device that has an alarm condition marked with a Red X. You will then be able to see the alarm conditions and generate log files by drilling into the device.



E-Mail Notifications are listed under the following menu:
System Management->Network->Notification Settings
There you can input the e-mail address for the recipient of an alarm state e-mail. In this case we use ZX-CriticalAlerts@cgcc.edu as our broadcast alarm e-mail.

3.2.2 American Power Conversions (APC) Edge Units (Wire Closets)

Areas of recovery / protection

Applications	Data	Hardware	Infrastructure	
			Data Center	Edge
		✓		✓

Primary Contacts:

	Name	Home Phone	Mobile Phone
Primary	Adam Gietl	[redacted]	[redacted]
Secondary	Bill Bohn	[redacted]	
Past	Chris McQuade	[redacted]	[redacted]
Vendor Support	APC	[redacted]	

Description:
The Edge APC UPSs are located in each wiring closet. The closets provide clean power to network switches that provide services to the end devices (computers, printers, scanners, & phones).

Each closes houses UPS(s) sufficient to power the closets equipment for up to a half an hour. These UPSs function to provide uninterrupted power for a short period of time. Short period of time means that the unit will provide consistent clean power for power spikes, dips or during an outage. The system will provide roughly one half (.5) hour of power.

Scope of protection:
These units protect the electrical switching equipment inside each of the network wiring closets. It does NOT provide power to lights or environment control units. Due to our phones using power over Ethernet (POE), phone units will remain in operation as long as the closet UPS provides power to that closet's switch(s).

Parameters of protection:
Provides clean uninterrupted power to the above scope for one half (.5) hour.

Monitoring/Notification:

#1) UPS-B3F1 (monitored in Xymon)
Bdlg. 3, Floor1 APC 1500 UPS inside the Main Server Room
Used for backup temp probe in core-switch rack and Bdlg. 3 main power. E-mail recipient: ZX-CriticalAlerts@cgcc.edu [redacted]

#2) UPS-B2F2 (monitored in Xymon)
Bdlg. 2, Floor2 APC 1500 UPS in the old server room.
Used for temp probe in switch rack. Monitors Disaster Recovery server room temp and power fluctuations in Bdlg. 2. Also provides monitoring for battery back-up status on our Internet connection. E-mail recipient: zx-criticalalerts@cgcc.edu
[redacted]

#3) UPS-B2B (monitored in Xymon)
Bdlg. 2 APC 1500 UPS in Basement in the Telco Room.
Used for temp probe in B2B switch rack. Internet fiber x-connect room.
E-mail recipient: zx-criticalalerts@cgcc.edu
[redacted]

#4) UPS-B1F3 (monitored in Xymon)
Bdlg. 1 Floor 3 APC 1500 UPS in wiring closet.
Used for temp probe in B1F3 switch rack. Student Lab PCs
E-mail recipient: zx-criticalalerts@cgcc.edu
[redacted]

#5) HRC-UPS (monitored in Xymon)
Bdlg. 1 HRC – APC 1500 UPC in 1st. floor HRC data center.
Used for temp probe in Hood River Campus data center.
Monitors power fluctuations at Hood River Campus.
E-mail recipient: zx-criticalalerts@cgcc.edu
[redacted]

3.2.3 Generator

Areas of recovery / protection

Applications	Data	Hardware	Infrastructure	
			Data Center	Edge
✓	✓	✓	✓	

Primary Contacts:

	Name	Home Phone	Mobile Phone
Primary	Jim Austin		[redacted]
Secondary	Ino Olivan		[redacted]
Vendor Support	*Get Support company* *Get refueling company*	*Support Company*	*Refueling Company*

Description:
The generator is located outside the ITS Department, just west of Building Three. It uses a 100 gallon diesel tank for fuel.

Scope of protection:
What it protects: The generator provides emergency power to the Data Center. Specifically, power to the APC UPS, lights, the Liebert environment control units and the Liebert control computers. It does NOT provide power to any other area of the College.

Parameters of protection:
Provides power to the Data Center computer & Environment Control units for roughly eight (8) hours.

Monitoring/Notification:
None.

3.3 Data Protection

3.3.1 Off Site (cloud) Backup

Areas of recovery / protection

Applications	Data	Hardware	Infrastructure	
			Data Center	Edge
	✓			

Primary Contacts:

	Name	Home Phone	Mobile Phone
Primary	Adam Gietl	[redacted]	[redacted]
Secondary	Bill Bohn	[redacted]	[redacted]
Vendor Support	CrashPlanPro http://www.crashplanpro.com/business/ [redacted]	[redacted]	

Description:
The College subscribes to CrashPlanPro to backup critical data off site. This off site backup fulfills the need to recover from a disaster that removes all on-site recovery options. The off-site data is updated on an hourly basis, so the data is never older than one hour. Recovery options include a menu driven select and recover option, as well as requesting a drive be sent to restore large amounts of data.
The data is encrypted with 448 bit encryption, as well as password protected. Nobody, including the vendor can recover the data without the password.

Data backed up by this method include:

- RogueNet (includes RogueNet and Charters)
- DocImg
- Archive
- Thor
- Isis

Scope of protection:
What it protects: CrashPlanPro backs up data from the core systems listed above. The data is stored offsite to protect against failure of onsite backups. See below for backup schedule.

Parameters of protection:
The schedule is based on the quickest availability of all our current backups. Some backups are done as quickly as 15 minutes. It keeps versioning of files when they are changed. A typical setup is as followed. There are backups and versioning done every 15 minutes. The retention for the last week is every 15 minutes. The retention for the last 90 days is every day. The retention for the last year is every week. The retention for previous years is every month. Beyond that, no files are deleted.

Steps to install CrashPlanPro.
Log onto the CrashPlanPro website and on the left hand side, click on Devices. Near the top is an image of a computer monitor, click on that and then choose the OS that the software will be installed on. Once it is downloaded, copy the installer to the server that CrashPlanPro will be installed on. Follow the steps to install and login using the CrashPlanPro credentials

3.3.2 Tape Backup System

Areas of recovery / protection

Applications	Data	Hardware	Infrastructure	
			Data Center	Edge
✓	✓			

Primary Contacts:

	Name	Home Phone	Mobile Phone
Primary	Adam Gietl	[redacted]	[redacted]
Secondary	Bill Bohn	[redacted]	[redacted]
Past	Chris McQuade	[redacted]	[redacted]
Vendor Support	Dell Power Vault TL2000 Symantec - BackupExec		

Description:
The College uses a robotic tape library system. It uses a single tape drive, and automatically changes tape based on a programmed schedule and configuration. The unit holds up to 23 2.5TB tapes. Backup sets can and do span multiple tapes. The backup unit resides in the Data Center.
Tape drive unit: Dell PowerVault
Tape type: LTO6 – 2.5 TB capacity
Backup Software: Veritas BackupExec

Scope of protection:
What it protects: The tape backup unit backs up all of data stored on all of the Colleges servers. The tape system does NOT backup any data stored on local computer drives.
Please see the below parameters of protection for the backup schedule.

Parameters of protection:
The schedule is based on a two week nightly rotation for Monday through Thursday, and a four week rotation schedule for Friday, and a monthly rotation schedule for monthly backups. Friday is used for the full data backup to allow backup time to run past 8am Saturday morning. Any other day may slow network performance during a regular business day.

Backup schedule:

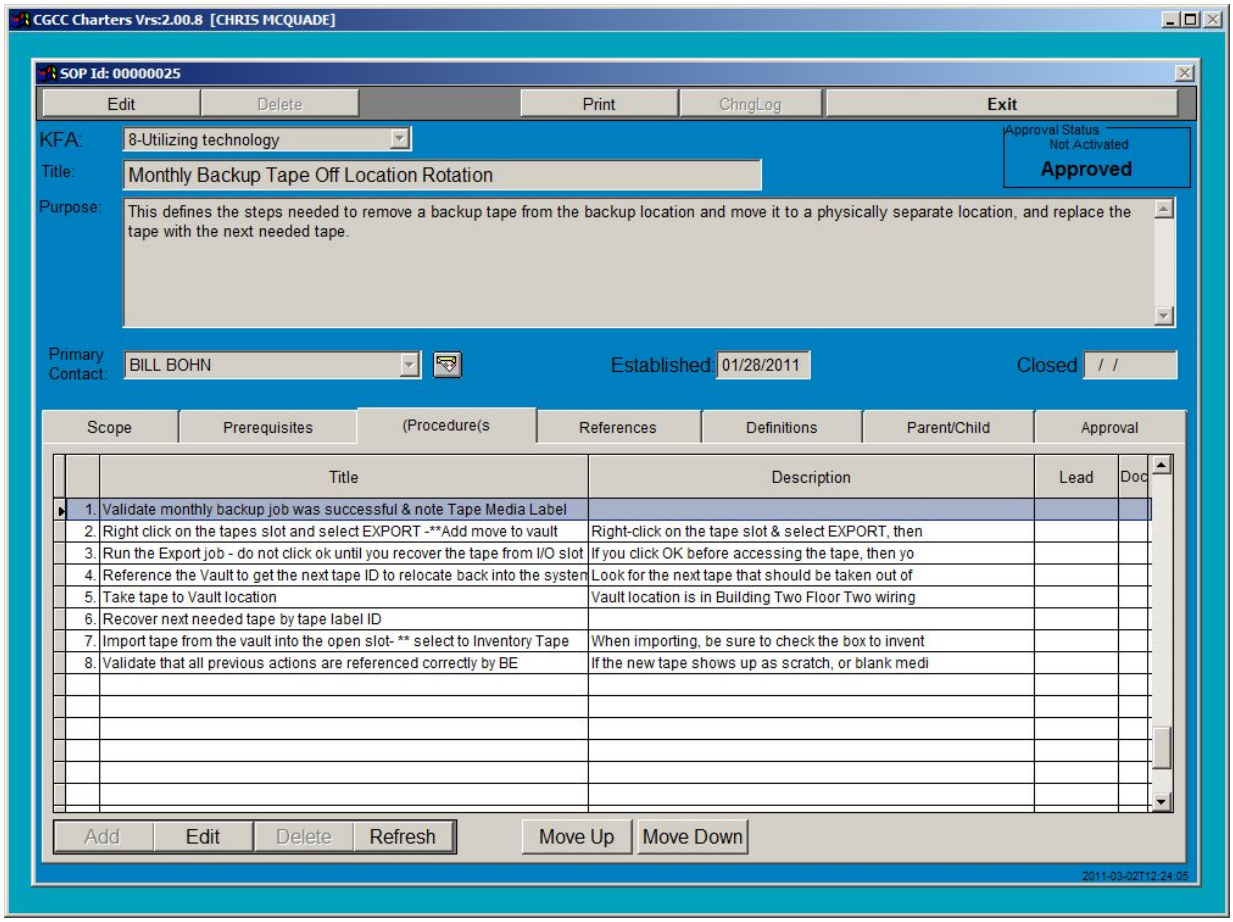
DAY	DESCRIPTION
Friday-1	Full backup of all data.
Monday-1	Full backup of key systems: RogueNet (RN) & GroupWise (GW), and differential of all other data (differential = all files modified since they were last backed up to tape)
Tuesday-1	Full backup of key systems: RN & GW, and differential of all other data
Wednesday-1	Full backup of key systems: RN & GW, and differential of all other data
Thursday-1	Full backup of key systems: RN & GW, and differential of all other data
Friday-2	Full backup of all data.
Monday-2	Full backup of key systems: RN & GW, and differential of all other data
Tuesday-2	Full backup of key systems: RN & GW, and differential of all other data
Wednesday-2	Full backup of key systems: RN & GW, and differential of all other data
Thursday-2	Full backup of key systems: RN & GW, and differential of all other data
Friday-3	Full backup of all data.
Friday-4	Full backup of all data.
Monthly	No data just applications and non-data related files. Manually rotated and stored in same location of Monday tapes.

Job Details:
Friday: Full Backup on two tapes, starts at 11:00PM same day
Monday – Thursday: Differential (only files modified since last backup) on one tape, Full starts at 1:00AM the *next calendar date*, Differential starts at 2:00AM. Differential is written to a network drive first, and then backed up to tape. This saves on wear on the tape drive unit.
Monthly – second Saturday of each month, starts at 7:00PM

Archive Drive Backup (Archive):
Due to the volume of data, the archive data uses a different schedule. A full backup is run every 84 days (every 12 weeks). As of May 2013 it was almost filling two tapes. Differential backups should be scheduled weekly (as of May 2013, this has not been established yet)

Monthly tapes are rotated out of the unit and moved to another building.
***In CGCC Charter System, follow Standard Operating Procedure (SOP) #00025 listed below**

"Monthly Backup Tape Off Location Rotation" -Tested 1/25/11 –CM

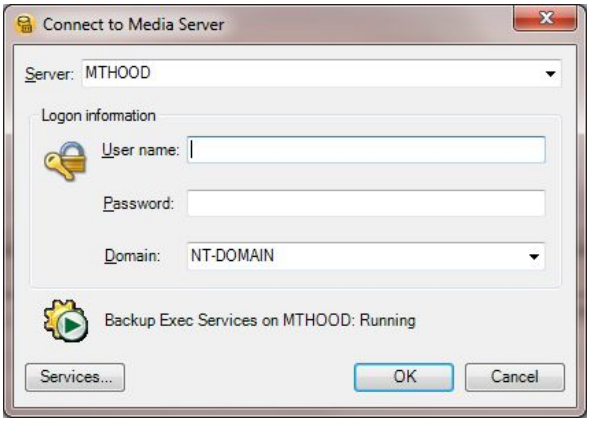


Monitoring/Notification:
Completed job notification emailed to the HelpDesk daily. Job errors are emailed to HelpDesk, A.Gietl and B.Bohn.

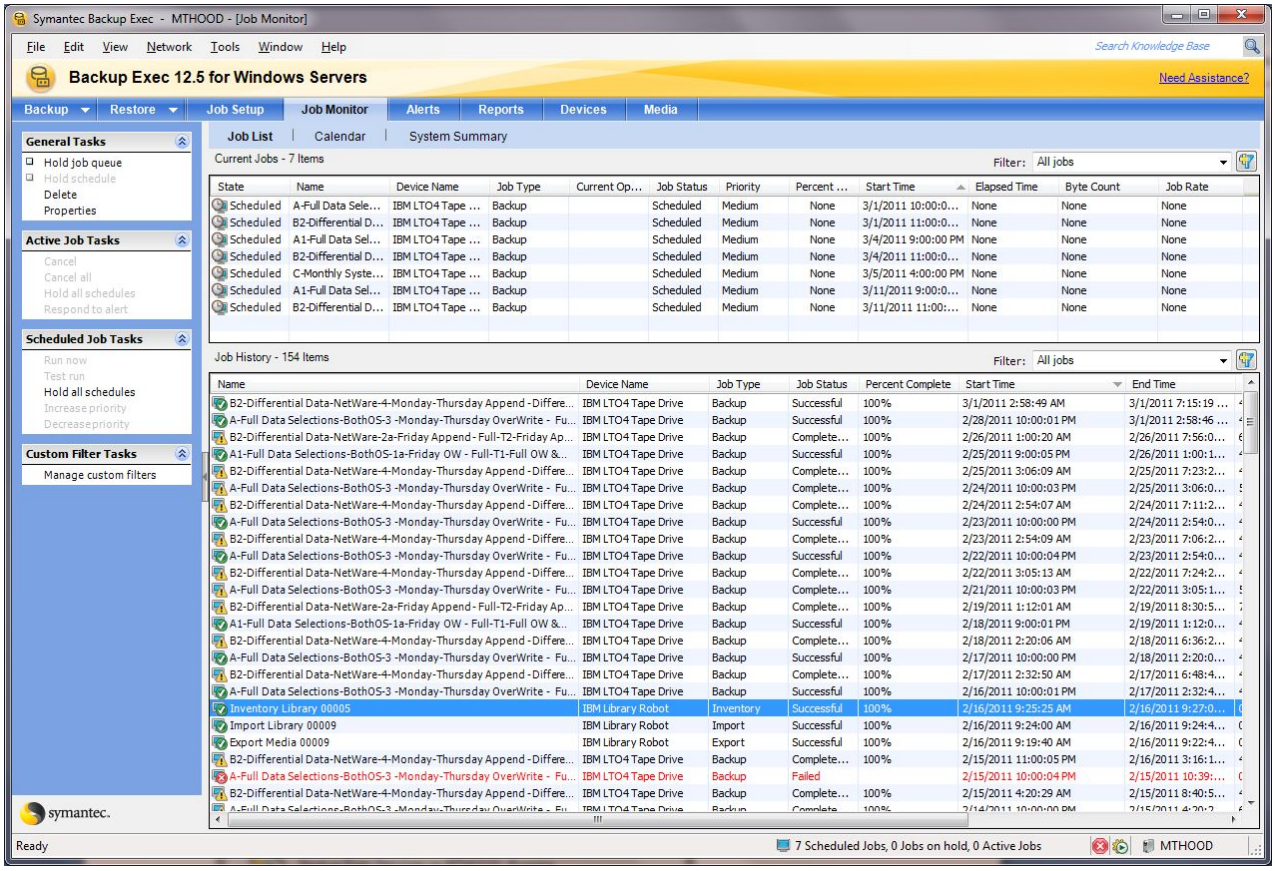
Fundamental Steps for Tape Restore

***Must have access to the Symantec Backup Exec 12.5 for Windows Servers Client on a PC**

***User must have a valid Domain Account.**



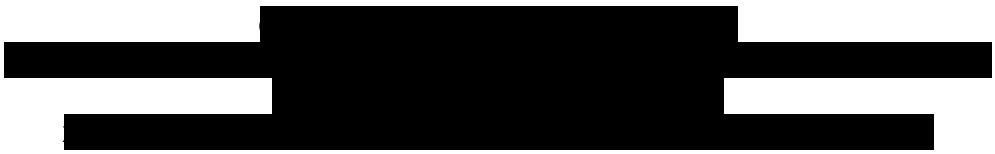
Enter valid Domain User/Pass and Press OK -- You will see the "Job Monitor" window.



Fundamental Steps for Tape Restore (Cont.)

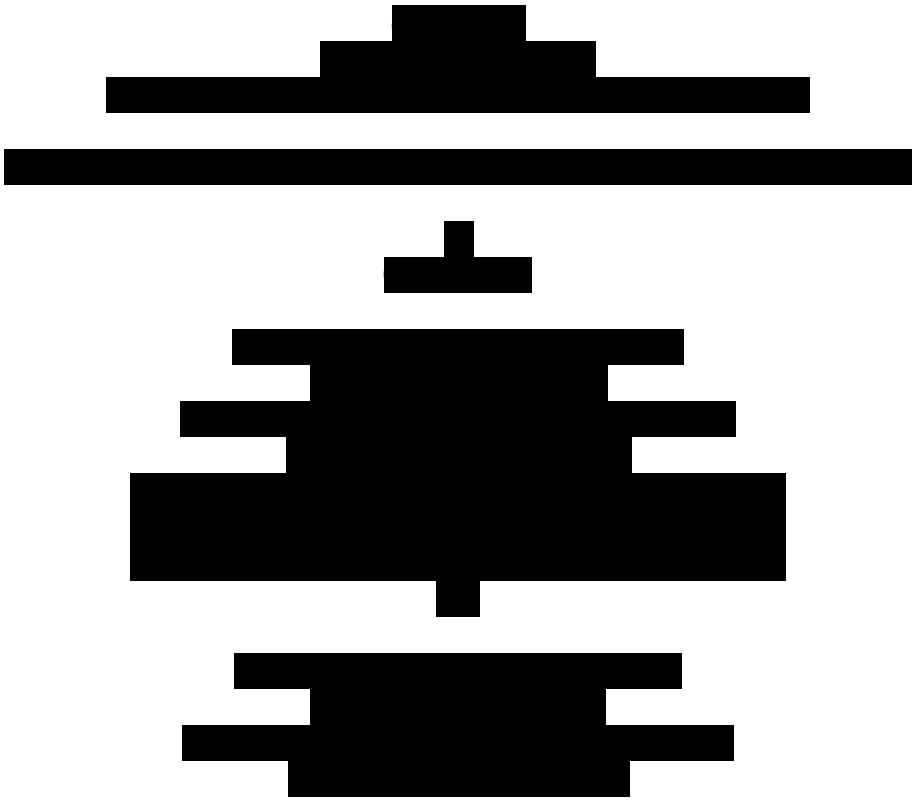
SQL specific information:
Some of the backup data is from SQL databases. This data must be exported out of SQL before it can be backed up to tape. The following describes the process and disk locations.

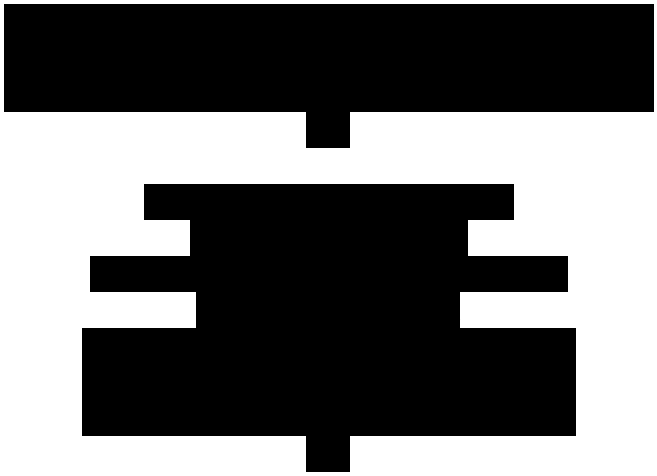
RMS (Retail Management System)
RMS runs of three different servers, each running an instance of SQL. RMS-HQ2, RMS-TDC2, RMS-HRC2
RMS-HQ2 – database name RMS-HQ
RMS-TDC2 – database name CGCCPOS
RMS-HRC2 – database name CGCCPOSHR
Each server runs a scheduled task to run the SQL export to the local “backup” folder.
POSBackup.bat consists of the following commands:



POSBackup.bat removes the 0 (zero) file, exports the local SQL data to a new 0 file, then copies it to the HQ server. RMS-HRC runs at 7:00 PM, RMS-TDC runs at 7:30 PM, RMS-HQ runs at 8:00 PM nightly. The HQ batch file does not do the xcopy since it is going directly to the backup folder.

The RMSIncrement.bat is a scheduled task that runs on the HQ server at 9:00 PM. This program increments the existing backup export files to make a consistent set of three for each server. This batch file consists of the following:





The most current export is the file marked with a 0 (zero) . If the zero file does not exist, then none of the rename commands are run. Otherwise, version 3 is removed, then #2 renamed to #3, and #1 renamed to #2, then #0 renamed to #1. Thus there should always be three version of backups.

All version of all three servers are backed up to tape following the nightly “full data” settings.

3.3.3 Storage Area Network (SAN) SnapShot & DR Unit

Areas of recovery / protection

Applications	Data	Hardware	Infrastructure	
			Data Center	Edge
✓	✓			

Primary Contacts:

	Name	Phone #1	Phone #2
Primary	Adam Gietl	[redacted]	[redacted]
Secondary	Bill Bohn		
Past	Chris McQuade	[redacted]	[redacted]
Vendor Support	Compellent CoPilot Services Customer Id [redacted]	[redacted]	

Description:

The Storage Area Network provides a shared pool of drives (disk space) and related storage handling features. The SAN is used for data storage as well as housing the virtual files from the Colleges virtual servers. Servers can connect to the SAN via CAT6 Ethernet or fiber. This system provides a number of protections to the entire system, as well as having a number of protection system built into its own system.

Since the SAN provides a critical aspect to the entire network operation, the SAN system implements a number of built in fault tolerant features.

The units are identified by a numbering system as follows:

- Controller [redacted] – Primary Data Center Controllers
  - Main Drive array T1 = 12x Seagate 600 GB 15K drives
  - Main Drive array T2 = 16x Seagate 400 GB 10k drives
  - Main Drive array T3 = 6x Seagate 2 TB 7.2K drives
- Controller [redacted] – Disaster Recovery Controller

  DR Drive array = 16 x Seagate 140 GB 10K drives

Scope of protection:

SAN Hardware

- The main drive array houses 12 tier 1, 16 tier 2, and 6 tier 3 hot swappable drives. Up to one drive can fail in each tier and the system will remain in operation.
- The main drive array is accessed via two separate Controller units. Each controller unit provides access for separate sets of servers. If either Controller fails, the services are migrated to the other Controller.
- Each Controller has two processors, either can fail, and the unit will remain operational.
- Each controller has three redundant power supplies.

SAN Software

- Replays - The SAN protects data integrity and user error with Replays. Replays are copies of the volume at a particular moment in time. “Replays” are also known as “SnapShots” on other systems.
- Copy to disaster recovery unit. Key data is migrated in real-time to a disaster recovery unit in Building Two.
  - The DR unit is a duplicate of the main unit, but only runs with a single control unit.

Parameters of protection:
SnapShots are scheduled to make images. These images are also given a period of time to be kept before automatically being discarded. The SnapShot details are as follows:
Snapshot schedule:
GroupWise: Weekly Sat @ 1am – keep for 4 weeks
Daily @ 1am – keep 7 days hrs
Daily 7 am – 7pm once every 3 hrs – keep 12 hrs

RogueNet: Daily @ 1am – keep 2 weeks
Weekly Sat @ 1am – keep 4 weeks
Daily 7am – 7pm once every hour - keep for 12 hrs

VMware Virtual Systems: Monthly – keep for 4 weeks
Lead on SnapShots & DR replication: Adam Gietl

Section 3.3.3.1 – Windows/Netware SAN Volume Recovery in VMWare

NOTE: In the event of server or volume corruption, both the actual server and or attached volumes can be restored from the SAN and connected back to hardware by the same methods listed herein. However, total server recovery is slightly different and requires a few more steps that will be covered.

NOTE2: CGCC SAN volume practices utilize two types of VMWare “Datastores”

- “Shared Storage” - This is a disk that has been mapped to each host the VMWare Cluster formatted as vmfs3. Hence the name “Shared Storage” Virtual Machines (servers) are created and their “Virtual Disk” hard disk 1 (C:\) is typically stored on this “Shared Storage” volume. The volume naming scheme is as follows: “sharedstorage(LUNID)_servername”

- “Mapped Raw LUN” – This is a disk that has been allocated for a Servers’ Data volume (D:\) or (VOL1) It is typically formatted when it gets attached to a server and mounted as a hard disk 2. Recovered “Mapped Raw LUN” disks can only be recovered on a compatible OS. Additionally, because these raw data disks are not formatted as vmfs3 they do not mount in the cluster. In this case the cluster serves as just a pass-through so these “Mapped Raw LUN” disks can be handily mounted directly to the server VM itself. Coincidentally, these volumes are also in a “Shared Storage” failover architecture. If the

VMWare ESX host fails the “Mapped Raw LUN” disk will also auto-migrate with its’ associated server VM.

Monitoring/Notification:
7/24/365 Compellent Central Operations Monitoring, http://xymon.cgcc.cc.or.us,
Email & text notification to B.Bohn & A.Gietl

Prerequisites:

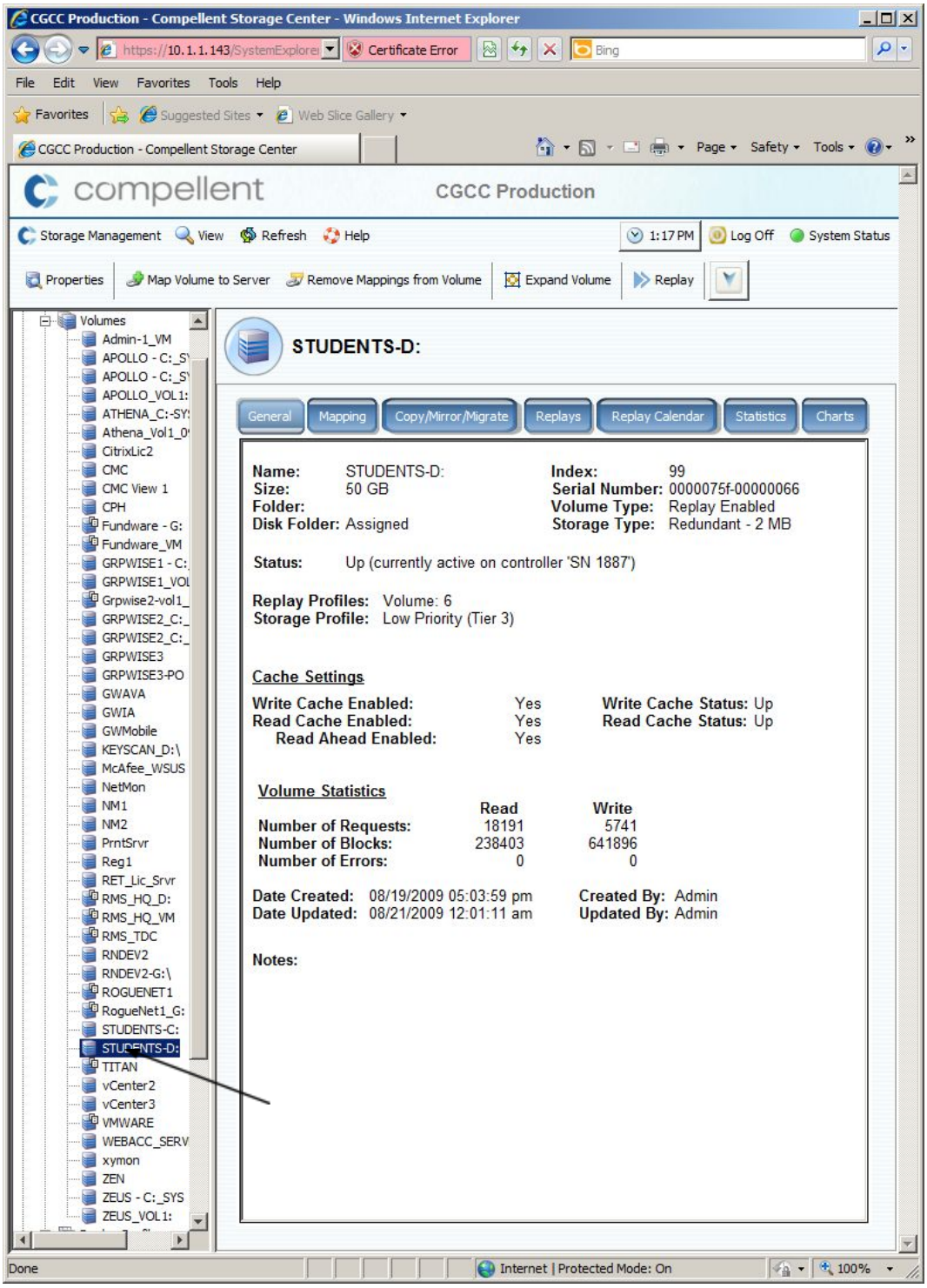
- I/E or Firefox Web - Browser Access from the CGCC LAN or CGCC Citrix Connection if off-campus
  https://citrix.cgcc.edu and the latest version of VMWare vSphere Client is installed
- Familiarity with logging into and navigating in a Virtual Server VMWare (ESX) environment using the vSphere client
- Familiarity with Windows and Netware Server disk mounting operations
- Familiarity with establishing Windows and Netware file system permissions
- NOTE: Windows and Netware file share rights will need to be re-established after mounting a recovered volume

Instructions:

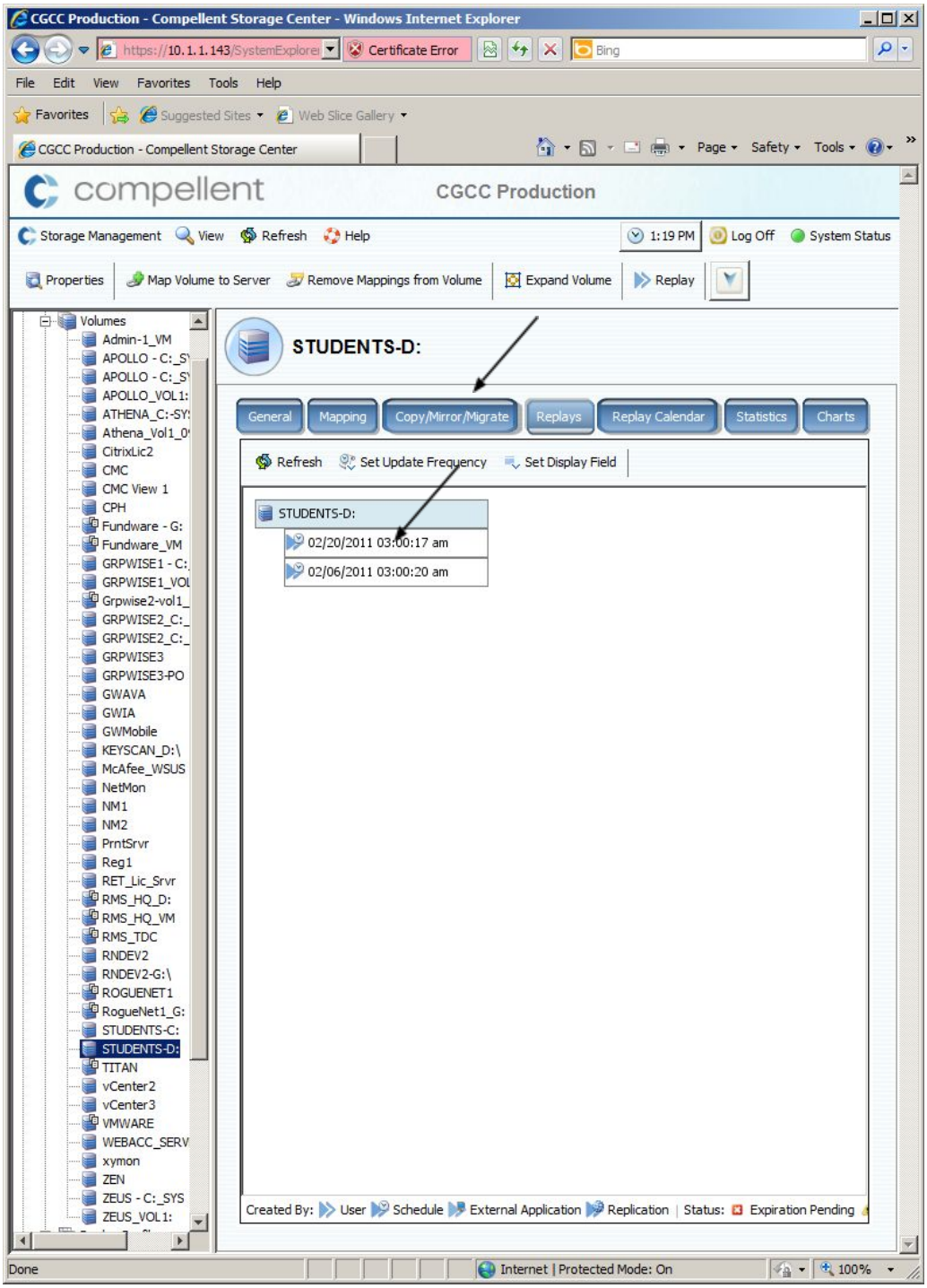
1.) Analyze what volume or server is down or corrupt. Note the name.

2.) Login to Compellent SAN [redacted]

3.) Expand Storage, Expand Volumes and Find the Volume you want to recover and select it by double clicking on the volume. For this example we will do a recover of a server using volume "Students-D" (pic)



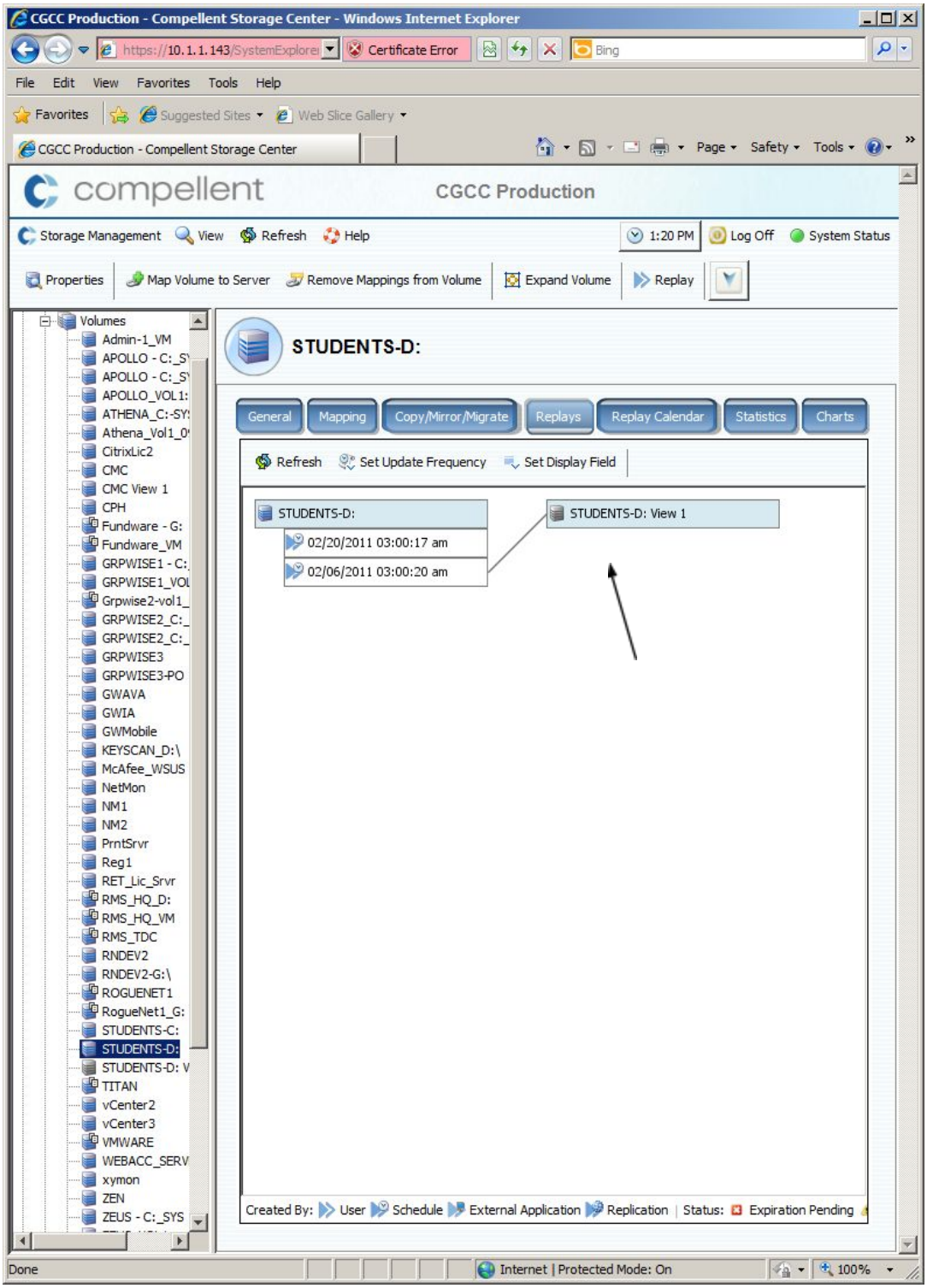
4.) Snapshots in this case are referred to as “Replays” in compellent SAN terminology. In this next step we will select what “Replay” we want to recover. Click the Replay TAB at the top of the Screen. You will see the replays and their respective date the replay was taken. (pic)



5.) ****IMPORTANT***** (pic)

The best scenario for success is to recover the Replay when the “closest date” was taken. In order to recover a replay, rt. Mouse Click the replay and select local recovery. This will generate the

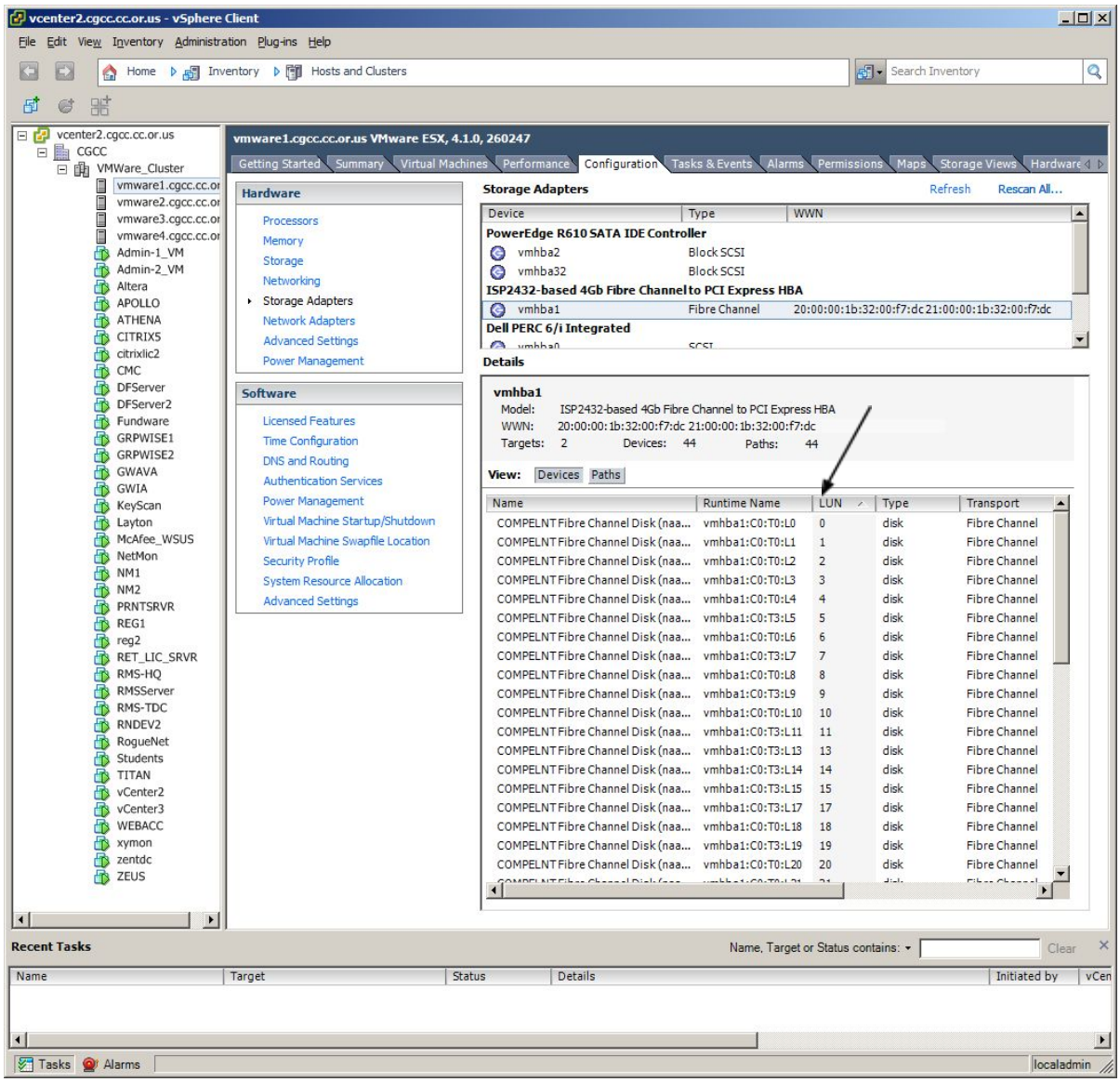
replay that we will restore into the VMWare cluster. You will then be asked to name the recovery volume, i.e. (Students-d: View 1) you can also put a date in here to specify the recovery time. You will then be asked to map the volume to a server. Skip this step and press “Cancel” the volume will be mapped later.



6.) Now that the volume has been recovered in the SAN, the volume must be mounted to the VMWare Cluster. Log in to the “VMware vSphere Client” When prompted to login you can use your standard (NT-DOMAIN) account. just by selecting the checkbox that says “Use Windows session

credentials" then press Login. If unable to log in via this method you can use the default username is [redacted]

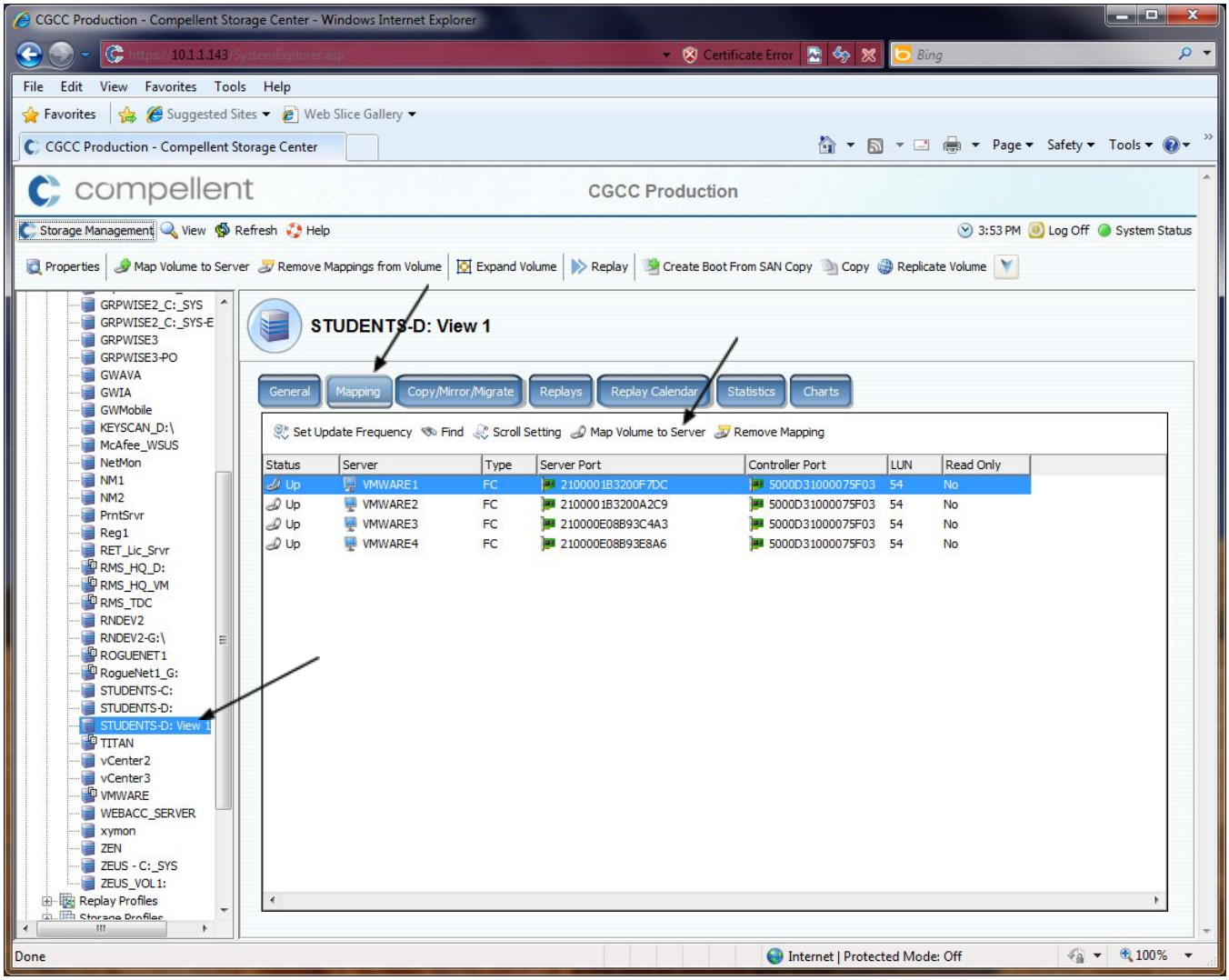
7.) **"Identifying the next LUN avail. to restore the volume to VMWare Cluster."**
After logged in to VMWare vSphere you will see a listing of all VMs running on our network. Select "VMWare12.cgcc.cc.or.us" by highlighting it, then select the Configuration Tab. Then click on Storage Adapters in blue text in the center of the window. (pic)



8.) Locate the next avail. LUN by clicking on the LUN menu arrow this will ascend/descend highest to lowest.
Then scroll down and note the next available LUN. Write it down. Minimize but leave this window open for later access. (pic)

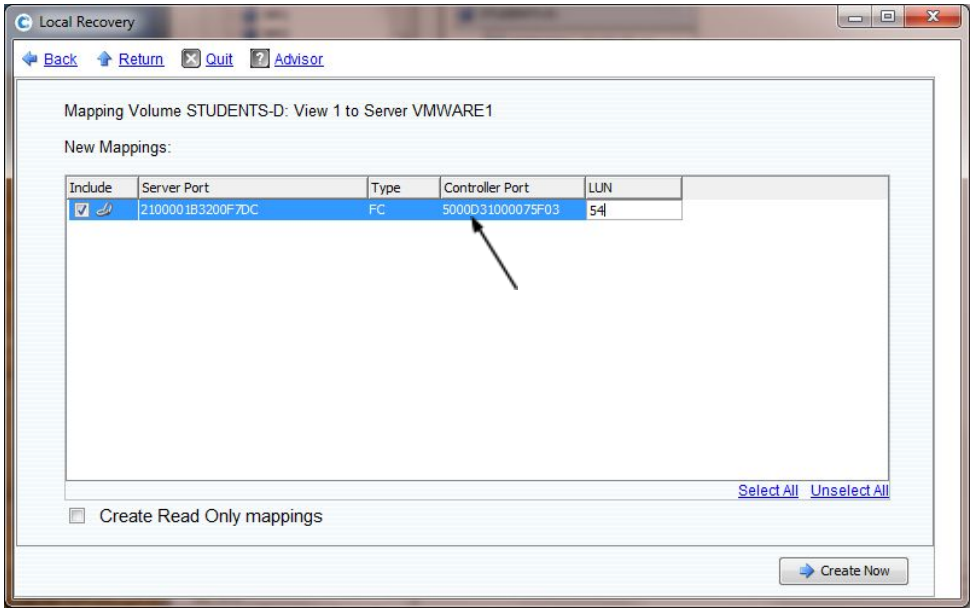
9.) **"Mapping the Recovered Volume to the VMWare Custer" (pic)**
From the Compellent SAN Web-Interface [redacted] Under CGCC Production, expand Storage, expand Volumes. Double click on the volume you wish to map. Click the "Mapping" button. This will show you what servers are mapped to this volume. The volume needs to be mapped to all (4) VMWare Servers in order.

- VMWare12
- VMWare13
- VMWare14
- VMWare15



10.) Map the volume by clicking the “Map Volume to Server” link. (pic)
You will be prompted to name the volume and then select the server you wish to map to. (pic)
In this first instance, we’ll pick VMWare1 as the first server to map to. Continue through by accepting the
default selections for (Fiber/ISCI) click continue, select “YES” – If prompted with a “Read-Only Mapping”
Warning, continue on with pressing “YES” but make sure you do not select “Read-Only Mapping” During this
process, we will establish connectivity for the recovered volume to each VMWare host server in the cluster.

11.) **“Inputting the correct LUN ID in the Map Volume to Server”** wizard. *****IMPORTANT*****
Input the LUN ID here by deleting anything in the box and inputting the next available LUN ID that was noted in Step #7. (pic)



12.) Repeat Steps 10-11, for each server respectively.

- VMWare12
- VMWare13
- VMWare14
- VMWare15

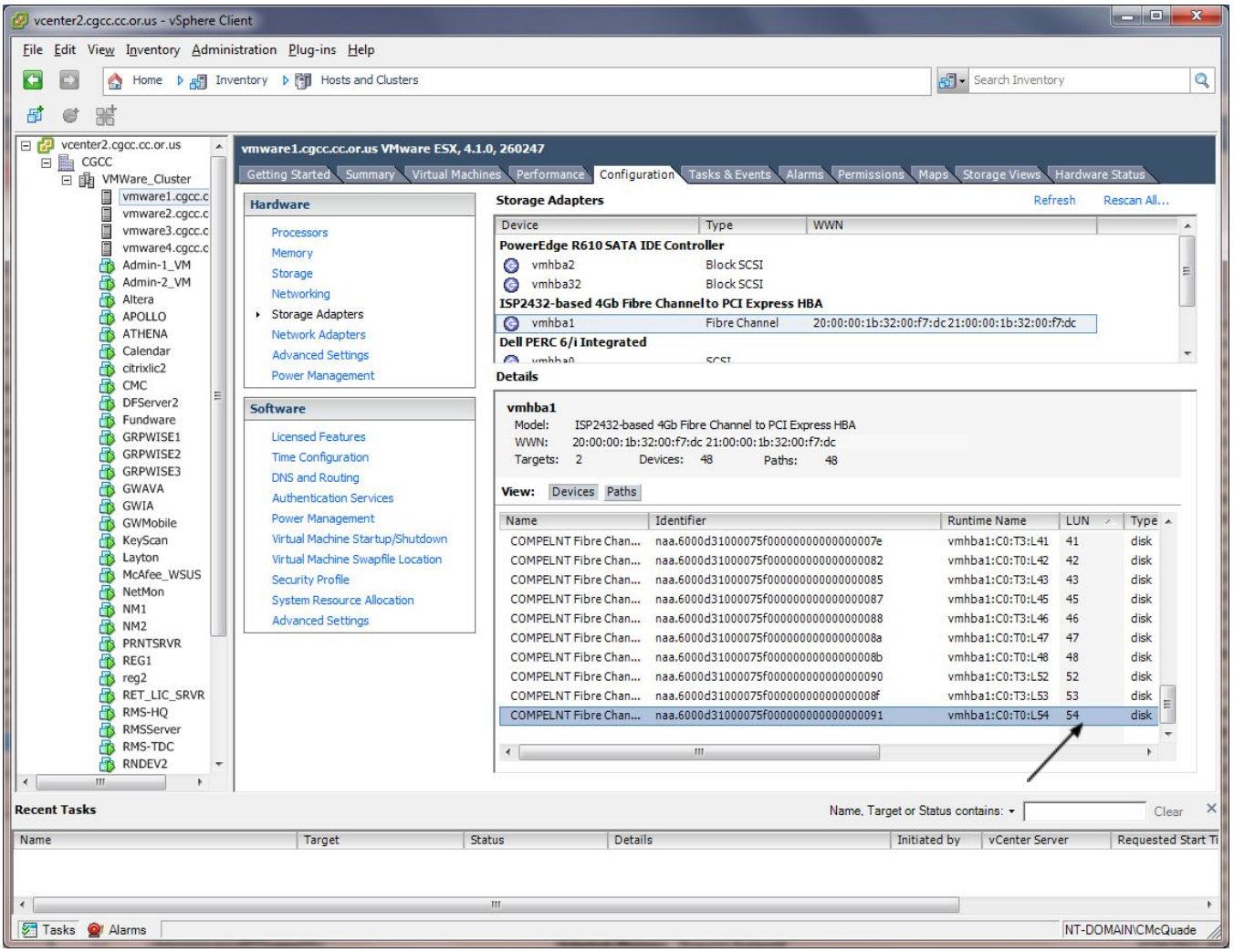
13.) **"Confirming the volume has been properly mapped."** In the VSphere Client Select "VMWare12.cgcc.cc.or.us" by highlighting it, then select the Configuration Tab. Then click on Storage Adapters in blue text in the center of the window. Click the "Rescan All" to see the newly mapped "Storage Adapters." Repeat for each VMWare host. Confirm the newly mapped LUN or "Storage Adapter" is listed, repeat for each VMWare host. ***Very Important***

Section 3.3.3.2 – Microsoft Windows Server Data (D:\) Volume Recovery

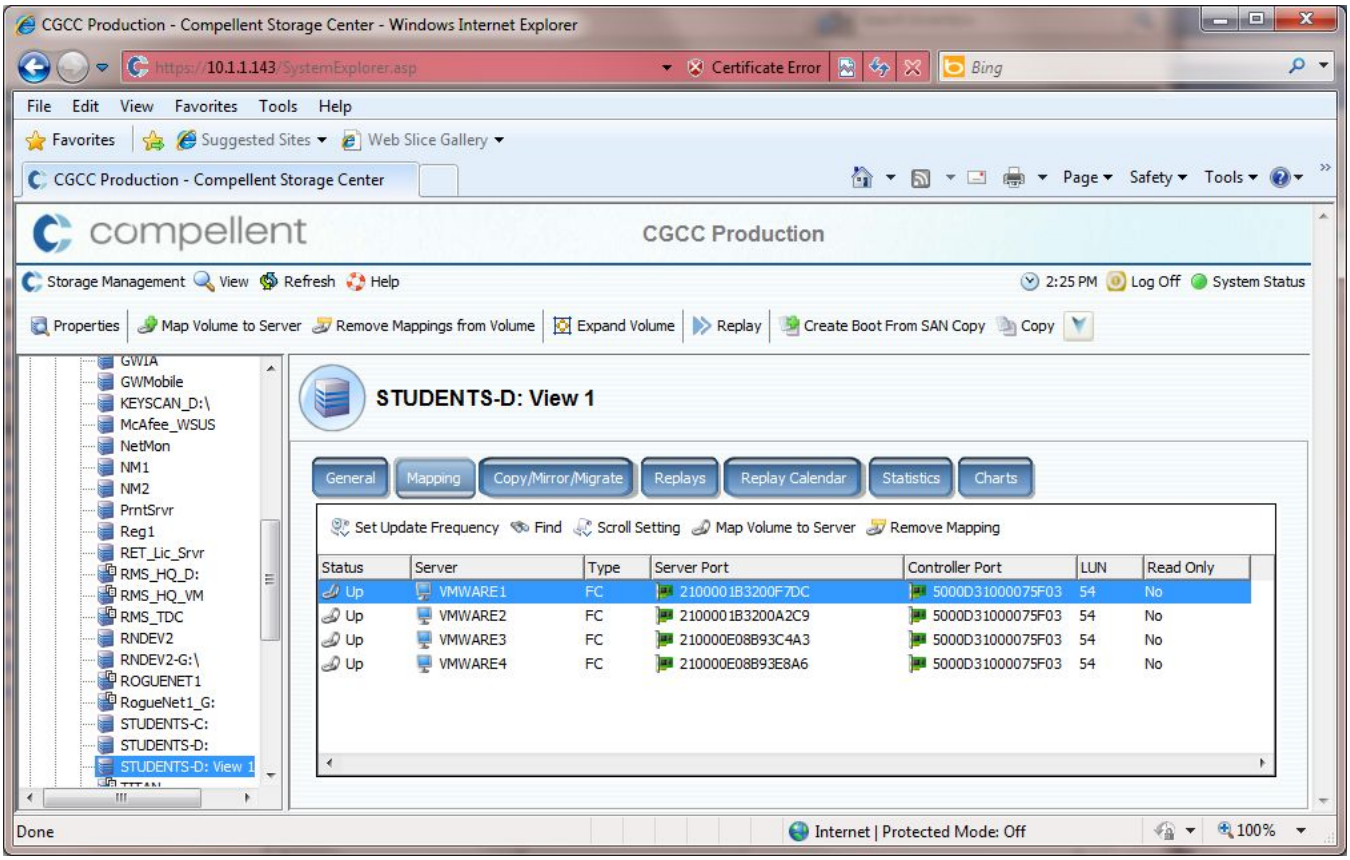
1.) Now that the recovered volume(s) have been restored from the SAN and the disks have been properly mapped to all the hosts in the VMWare cluster. In this process we will define how these

newly recovered Hard Disks and their volumes will be associated to a server OS and ultimately accessed.

2.) Log in to vSphere Client, Go to Home -> Inventory -> Hosts and Clusters, expand vSphere.cgcc.cc.or.us, The Dalles (datacenter) expand TD_PE-R620, highlight host server "vmware12.cgcc.cc.or.us" and select the "Configuration" tab. Click the link "Storage Adapters" and find the storage adapter "8Gb Fibre Channel to PCI Express HBA" highlight "**vmhba2**". Below under "Details" click the "LUN" Menu and sort least to greatest. Note the last LUN number that was created in section 3.2.2.1 you will use this information to mount the new disk. (pic)

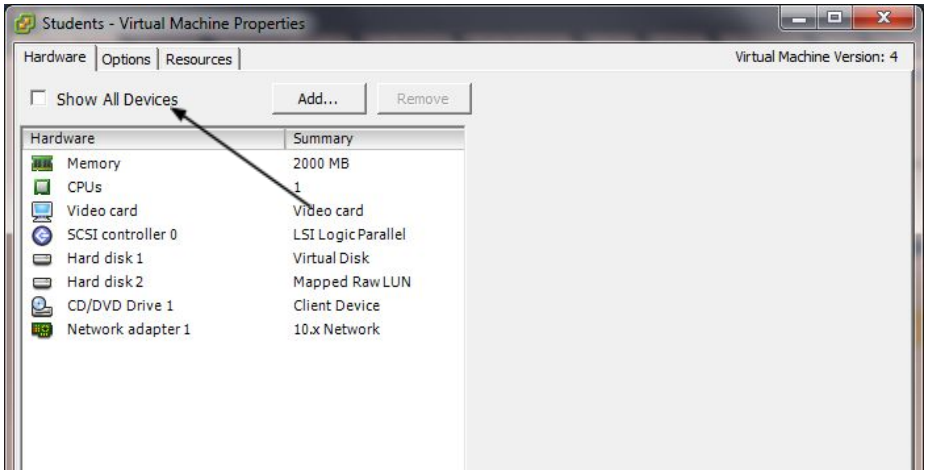


3.) In this example we will add a "Mapped Raw LUN" as a D:\ data volume to a Server "Students" The test volume we are recovering is called "Students-D: View 1" LUN #54. (pic)

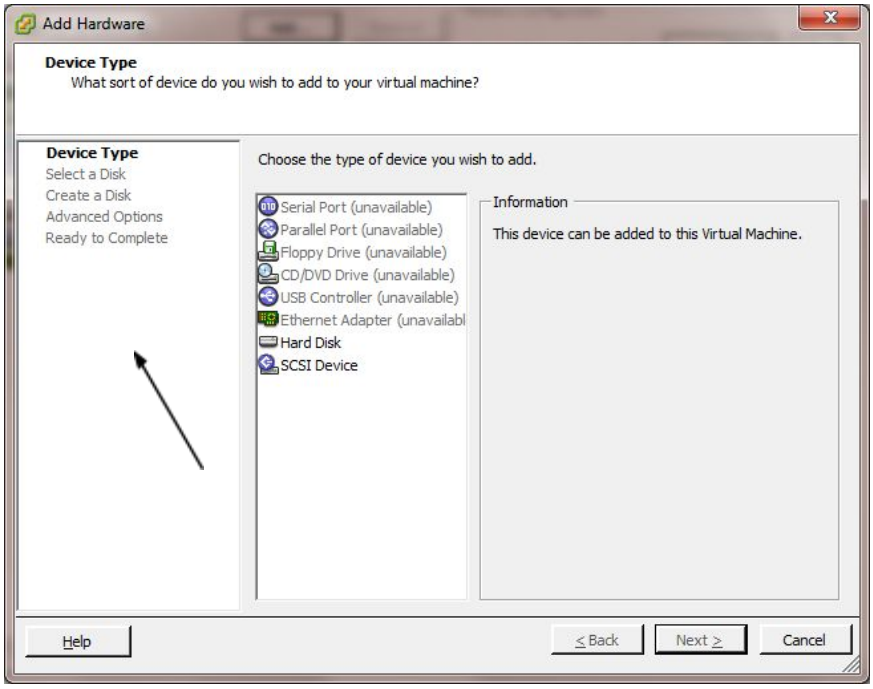


4.) Log in to vSphere Client, Go to Home -> Inventory -> Hosts and Clusters, expand vSphere.cgcc.cc.or.us, The Dalles (datacenter) expand TD_PE-R620, highlight guest VM "Students" by clicking on the VM. Then edit the Virtual Machine settings by clicking "Edit Virtual Machine" link under Basic Tasks:

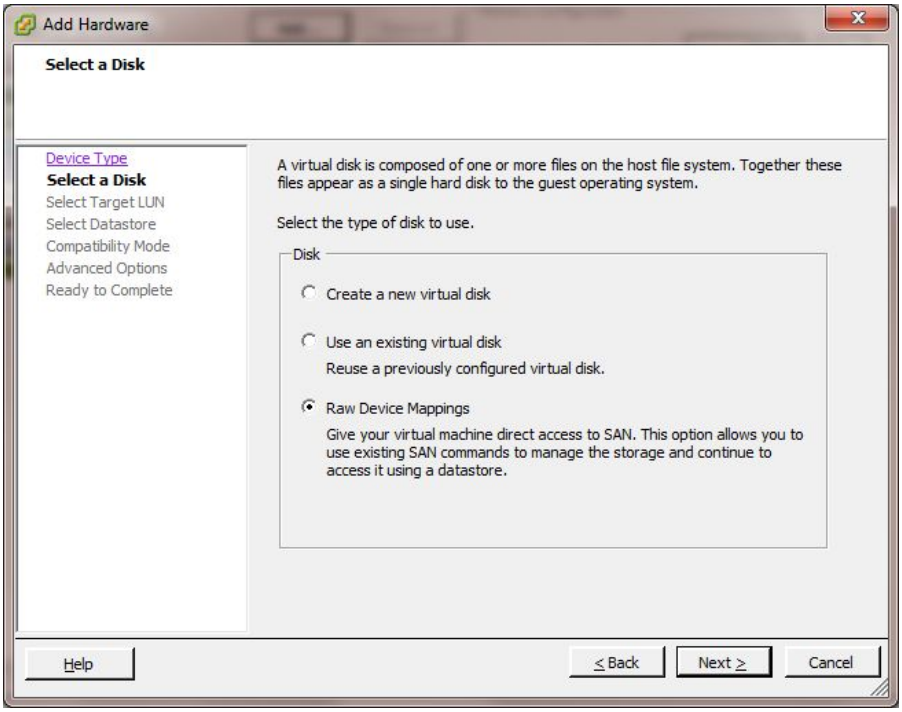
The following screen will appear. Click the Add Button (pic)



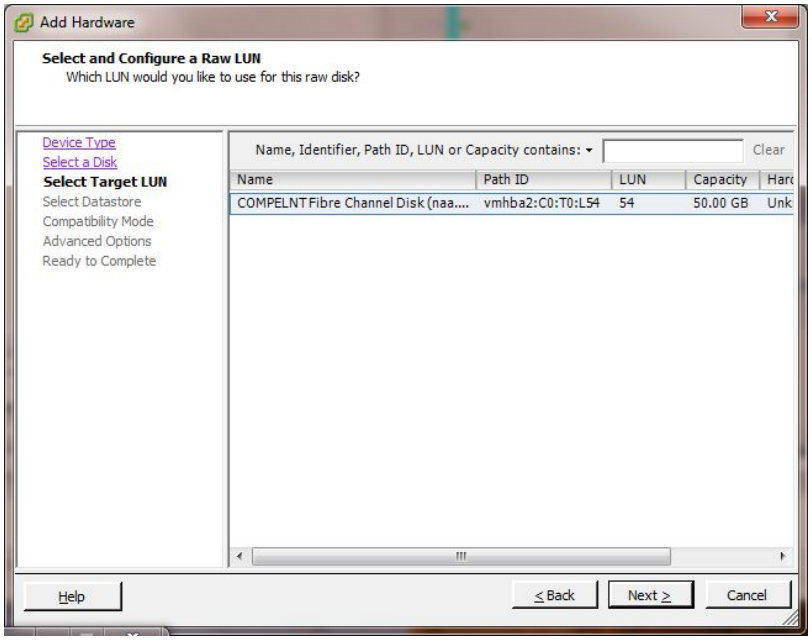
5.) Add a new Hard Disk by selecting it. Click Next. (pic)



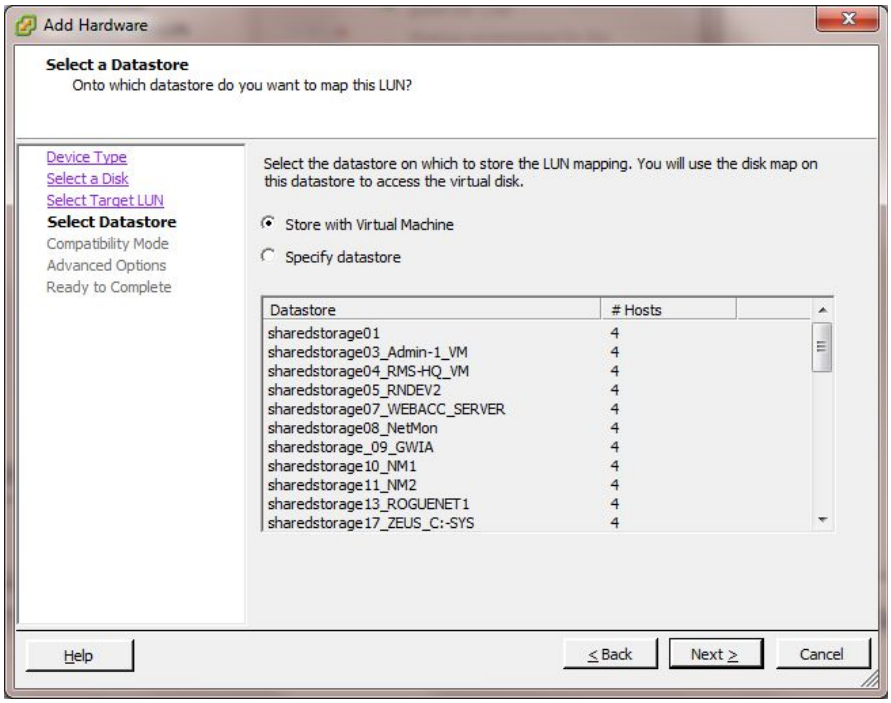
6.) Select “Raw Device Mappings” Click Next. (pic)



7.) This screen should show the recovered volume from Section 3.2.2.1 Note the LUN #ID is the same that was mapped to the cluster for recovery. Select the volume by clicking on it. Click Next. (pic)

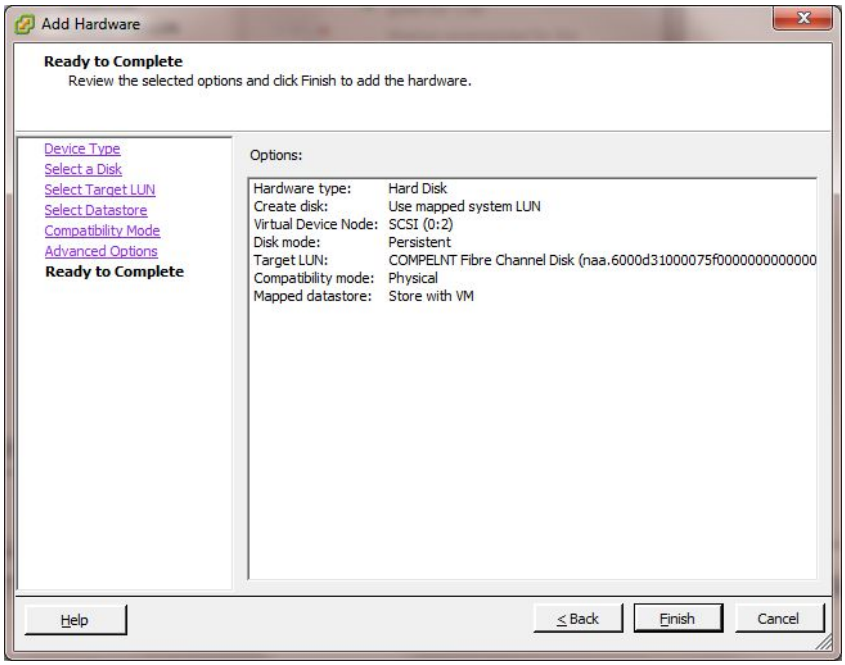


8.) "Select the datastore on which to store the LUN Mapping"
Select "Store with Virtual Machine" This will store the LUN mapping info with the VM itself. Click Next. (pic)

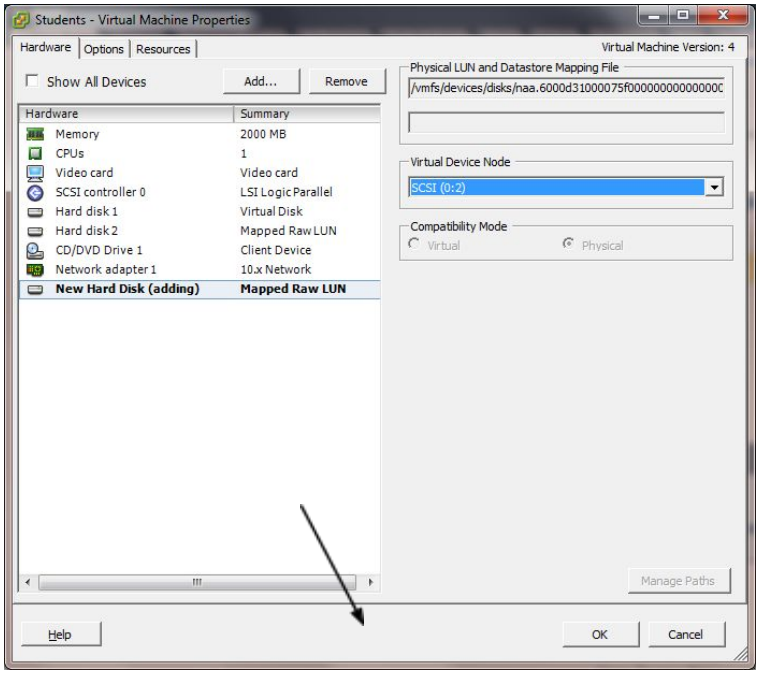


9.) Under the next screen “Select Compatibility Mode” the default setting is “Physical” leave this to the default. Click Next. Under the next screen under “Advanced Options / Virtual Device Node” leave the default setting. Click Next. Ready to finish completing the “Add Hard Disk” Review the settings.

Click Finish. (pic)



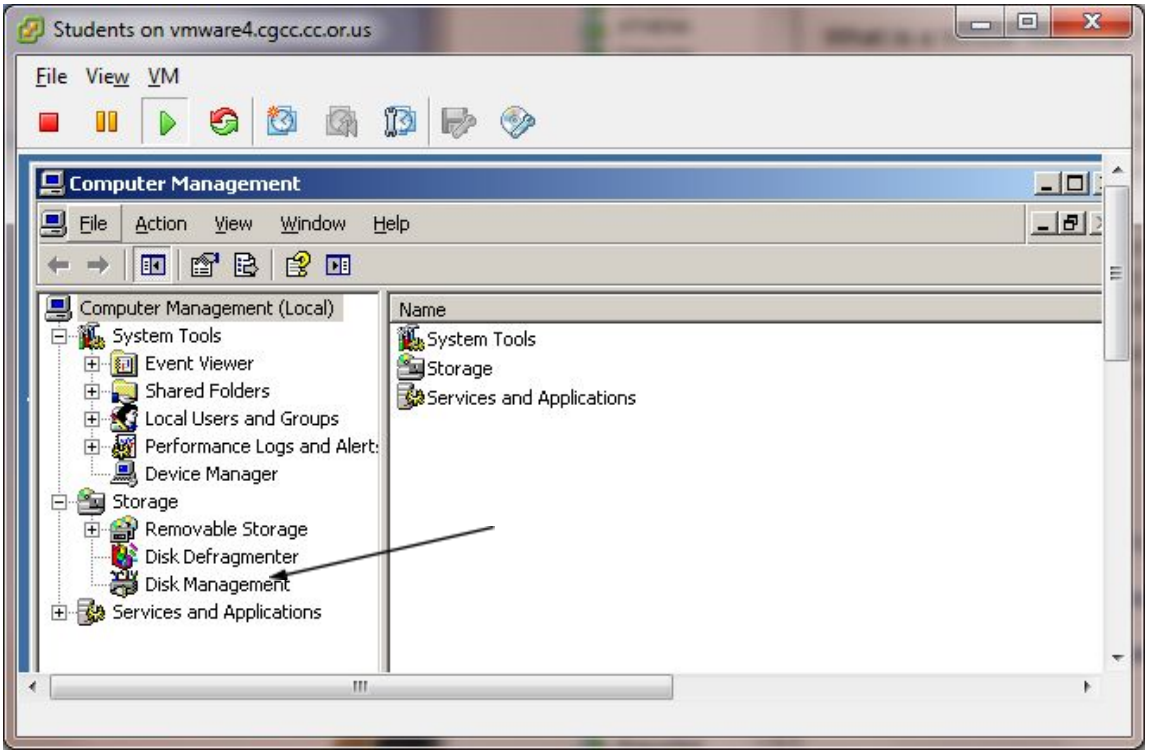
10.) You will now see the new “Hard Disk (adding)” listed in the “Students” – Virtual Machine Properties. Press OK. VMWare will then add the new disk accordingly and respond with a 100% complete. (pic)



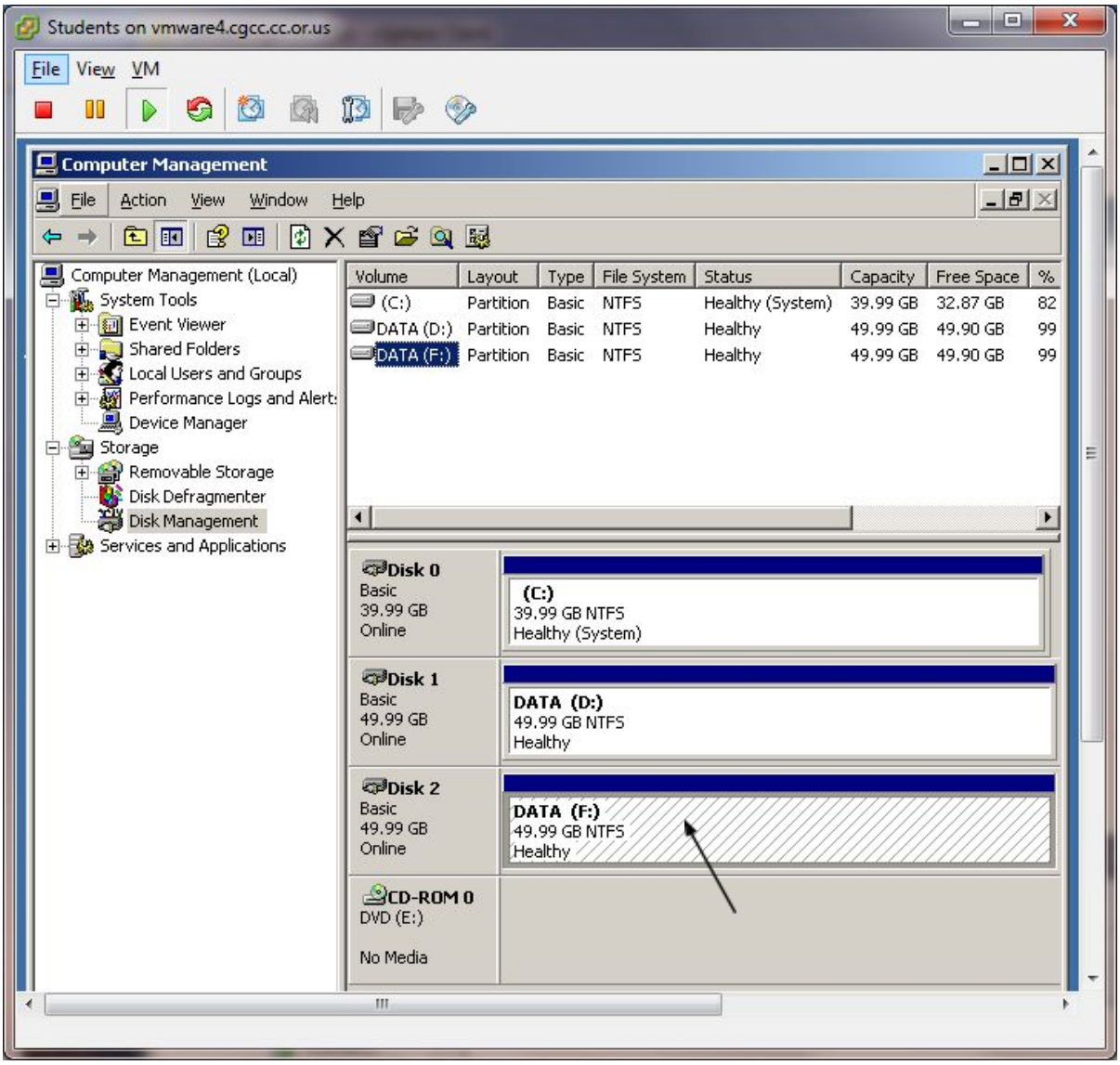
Windows Server 2003 r2 Standard Ed. Volume Mounting Instructions

11.) Log in to vSphere Client, Go to Home -> Inventory -> Hosts and Clusters, expand vSphere.cgcc.cc.or.us, The Dalles (datacenter) expand TD_PE-R620, highlight guest VM "Students" by clicking on the VM. Then open a console to the VM. (rt. Mouse click – Open Console) Log On to the Server "STUDENTS" with [redacted] credentials. *see IP Table for [redacted]

12.) On the "Students" Server, Click Start->My Computer->rt. Mouse click->manage This will bring up the local "Computer Management" window. Select "Disk Management" (pic)

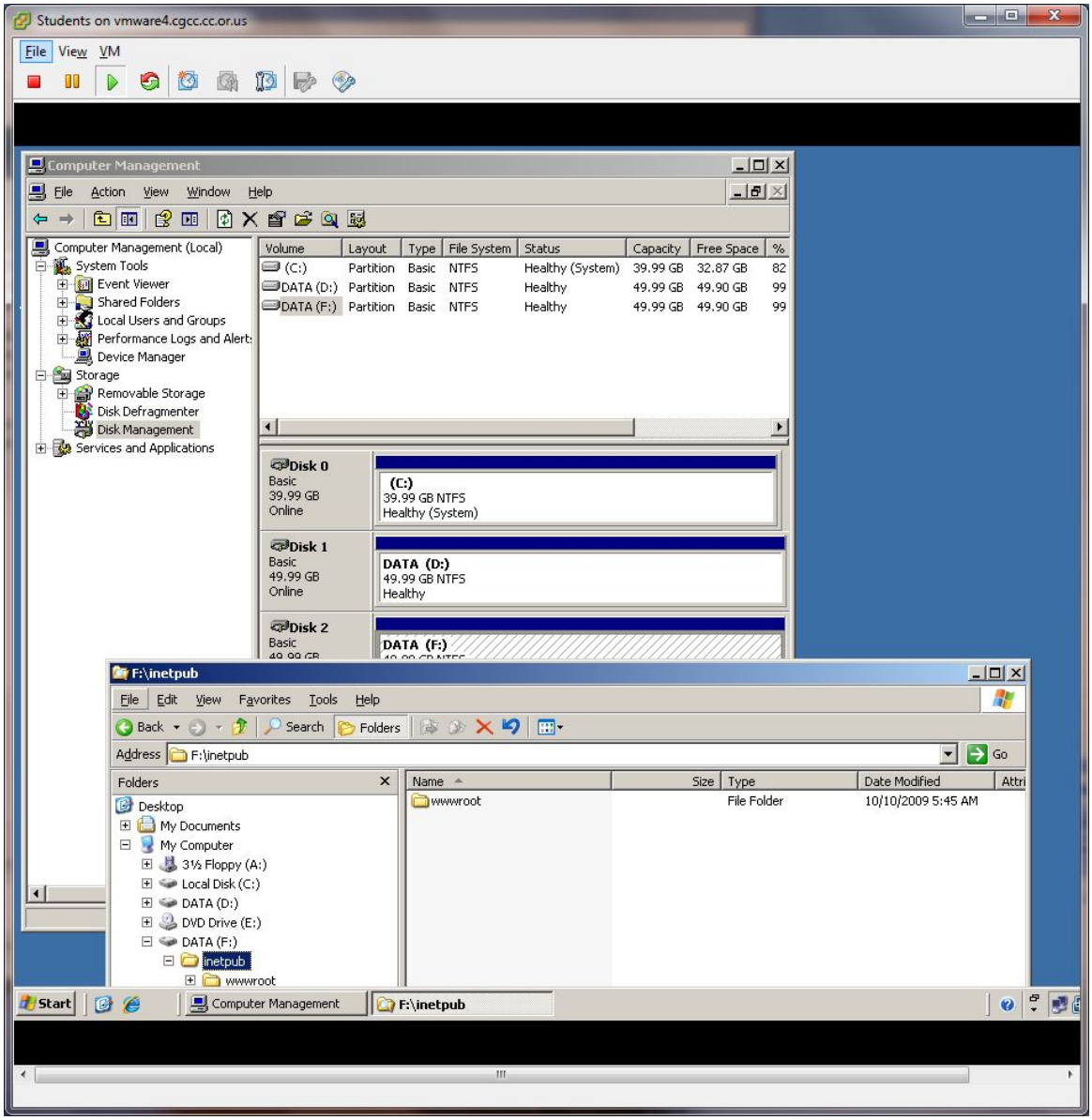


13.) In this window you will see the newly mounted windows volume DATA (F:) (pic)



14.) Browse the volume by rt. Mouse clicking the volume and select “Explore” Recover Data as needed. (pic)

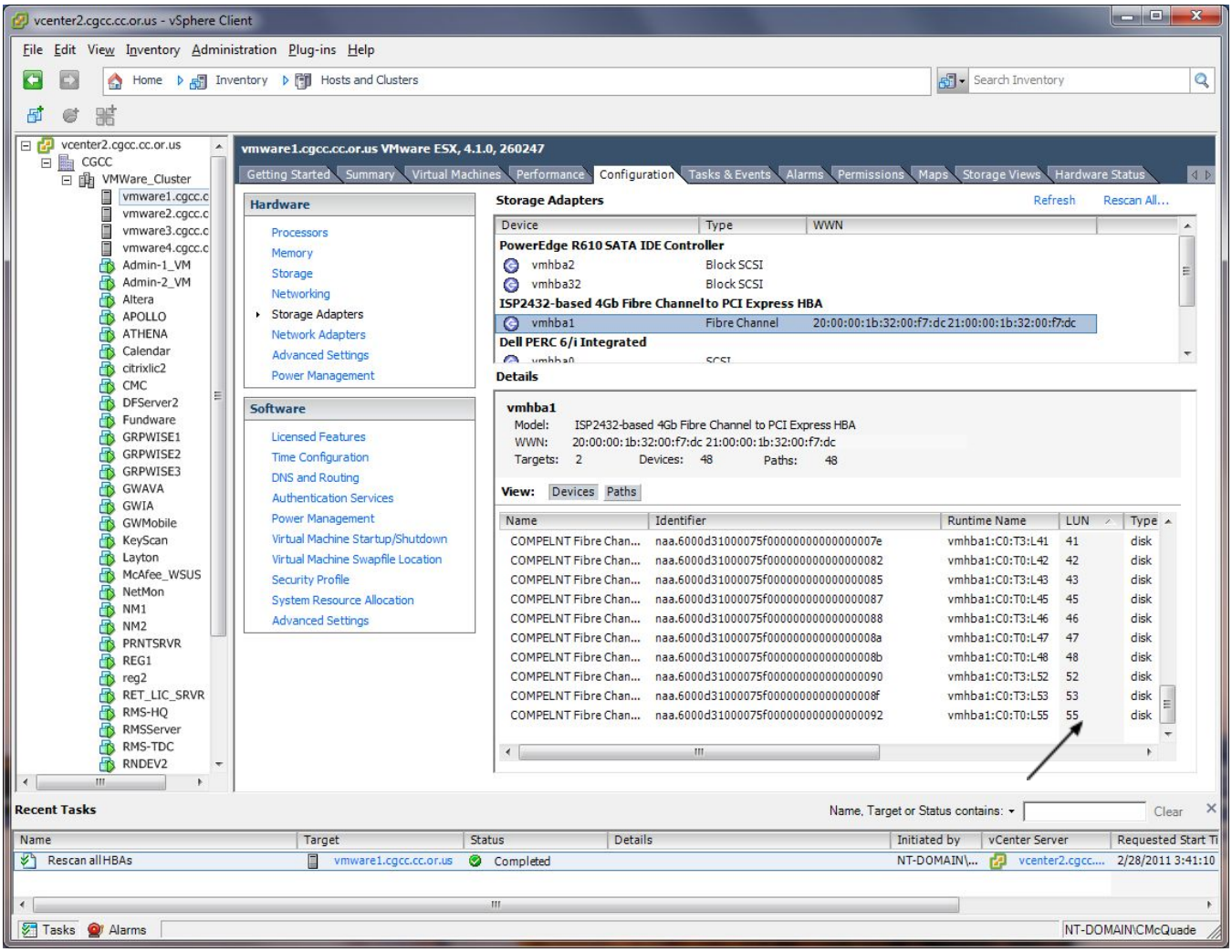
Note: If intending to use this volume for production, Windows File Share Rights and Windows Security Permissions will need to be re-established for this volume.



Section 3.3.3.3 – Novell Netware Server Data (VOL1:\) Volume Recovery

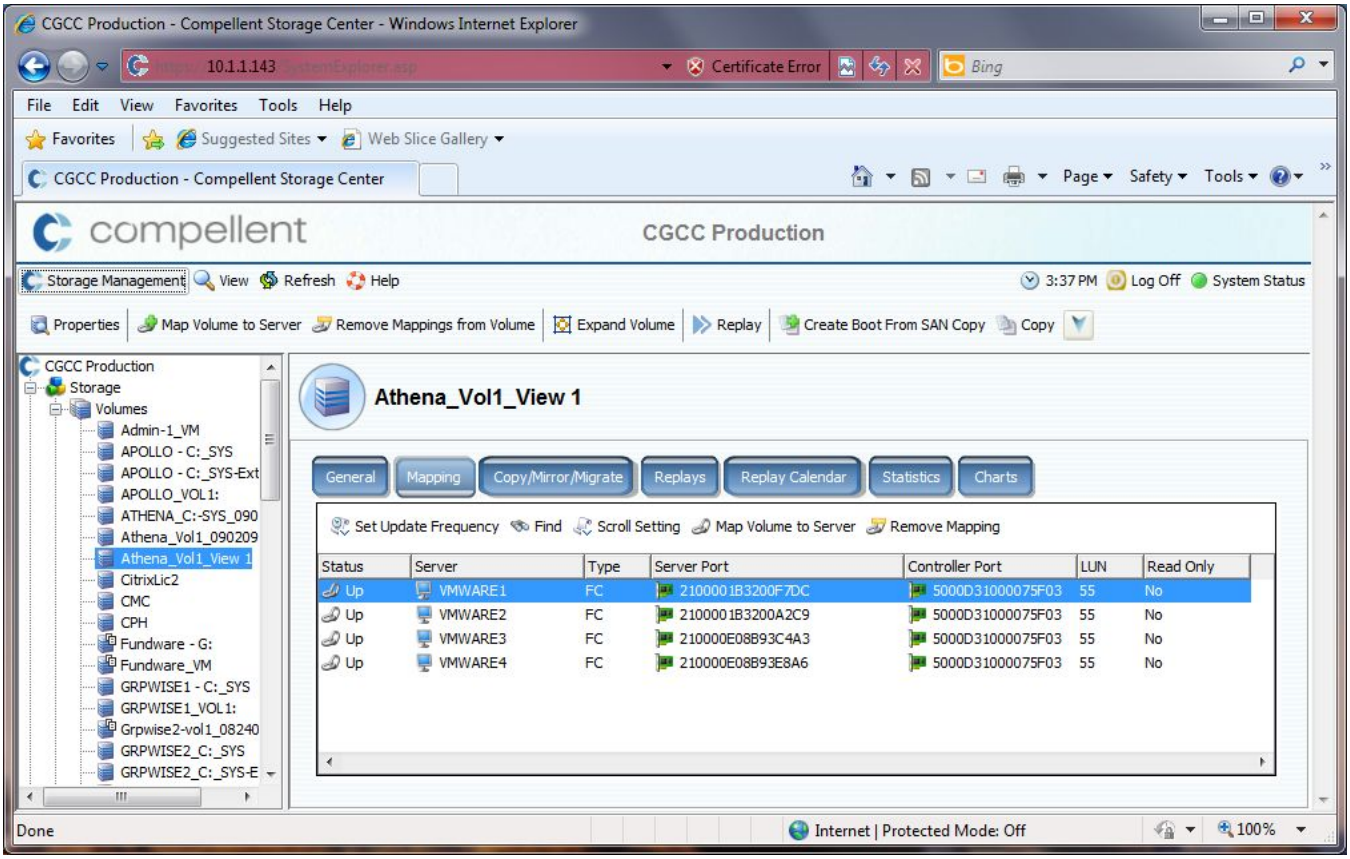
1.) Now that the recovered volume(s) have been restored from the SAN and the disks have been properly mapped to all the hosts in the VMWare cluster. In this process we will define how these newly recovered Hard Disks and their volumes will be associated to a server OS and ultimately accessed.

2.) Log in to vSphere Client, Go to Home -> Inventory -> Hosts and Clusters, expand vSphere2.cgcc.cc.or.us, CGCC (datacenter) expand VMWare_Cluster, highlight host server "vmware1.cgcc.cc.or.us" and select the "Configuration" tab. Click the link "Storage Adapters" and find the storage adapter "4Gb Fibre Channel to PCI Express HBA" highlight "**vmhba1**". Below under "Details" click the "LUN" Menu and sort least to greatest. Note the last LUN number that was created in section 3.2.2.1 you will use this information to mount the new disk. (pic)



3.) In this example we will add a “Mapped Raw LUN” as a VOL1:\ data volume to a Server “ATHENA”

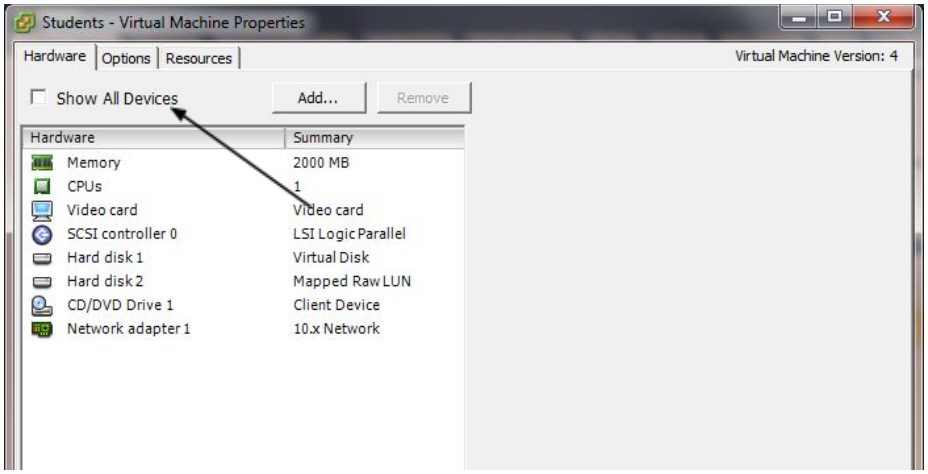
The test volume we are recovering is called “Athena_Vol1_View 1” LUN #55. (pic)



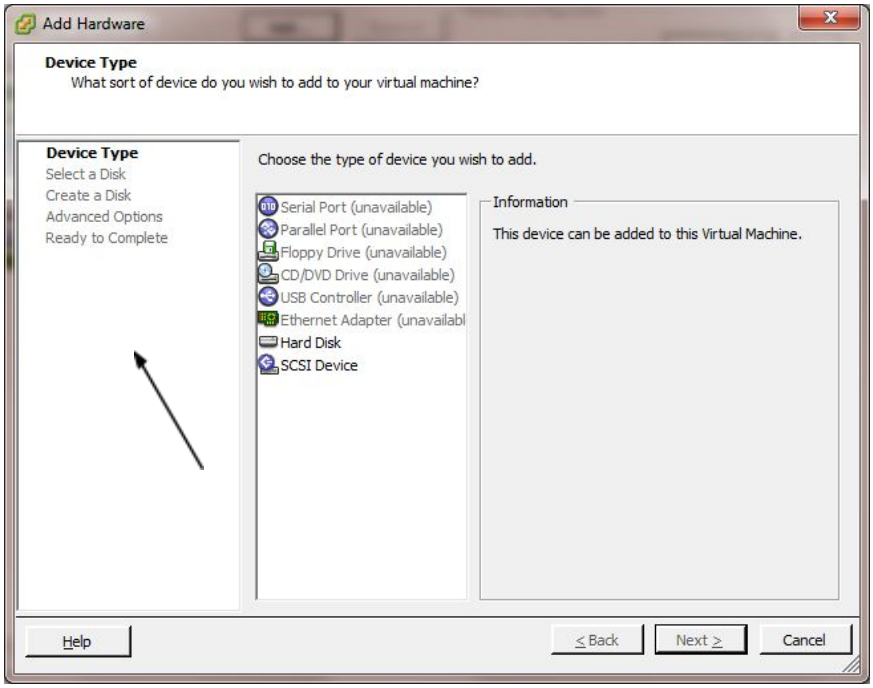
NOTE: Novell Netware volume titles like “VOL1” and “VOL2” are eDirectory specific and can only be mounted on another Novell Netware server that does not have any volumes with the same name. The volume name is embedded in the volume itself. The server must see it at a “VOL1” or “VOL2”

4.) Log in to vSphere Client, Go to Home -> Inventory -> Hosts and Clusters, expand vSphere2.cgcc.cc.or.us, CGCC (datacenter) expand VMWare_Cluster, highlight guest VM “NM2” by clicking on the VM. Then edit the Virtual Machine settings by clicking “Edit Virtual Machine” link under Basic Tasks:

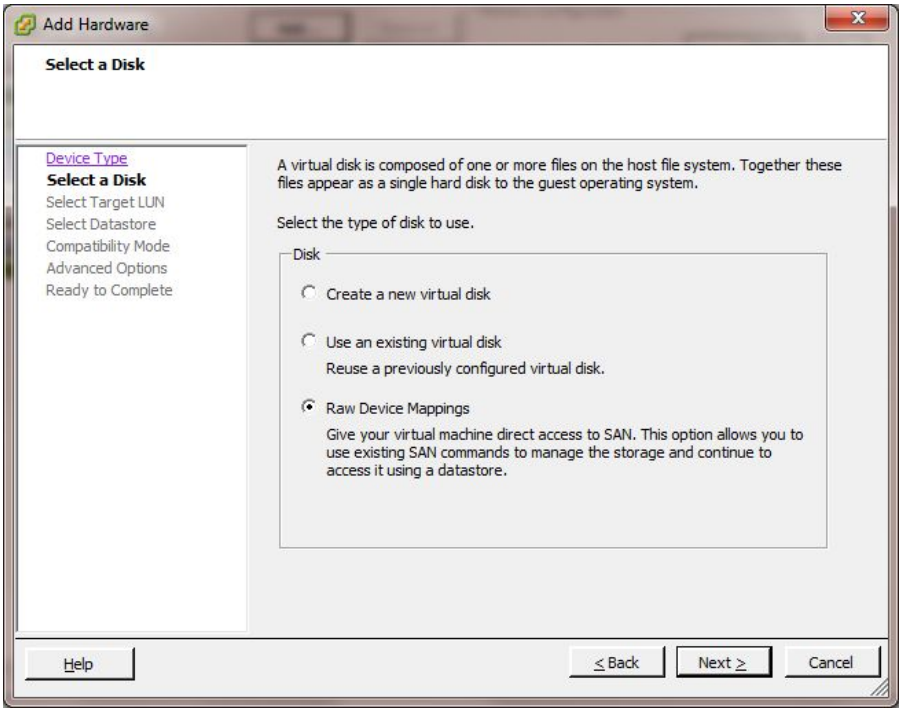
The following screen will appear. Click the Add Button (pic)



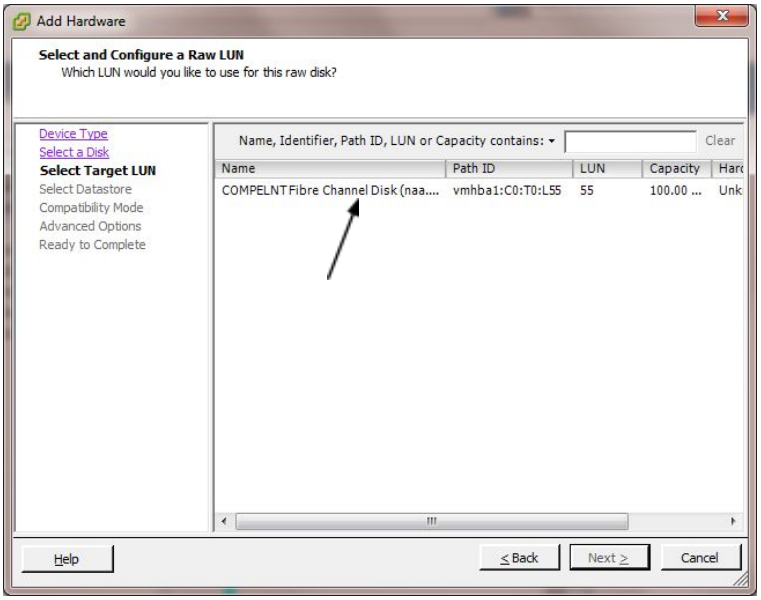
5.) Add a new Hard Disk by selecting it. Click Next. (pic)



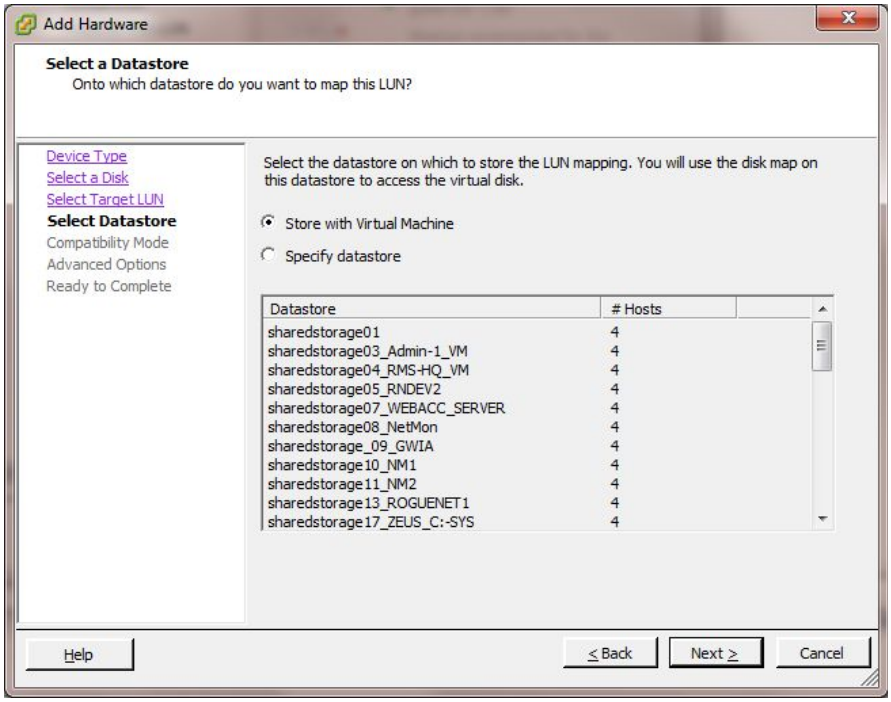
6.) Select “Raw Device Mappings” Click Next. (pic)



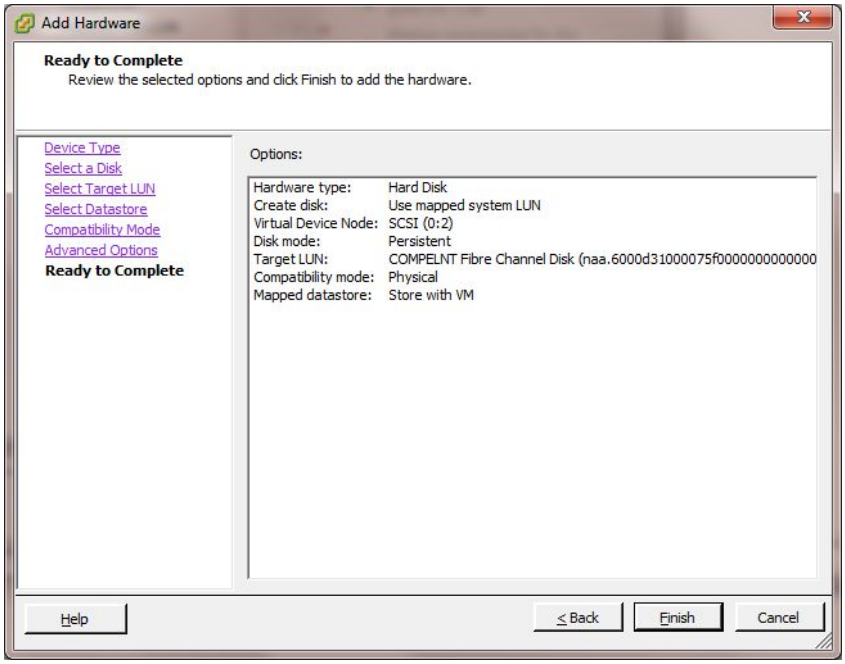
7.) This screen should show the recovered volume from Section 3.2.2.1 Note the LUN #ID is the same that was mapped to the cluster for recovery. Select the volume by clicking on it. Click Next. (pic)



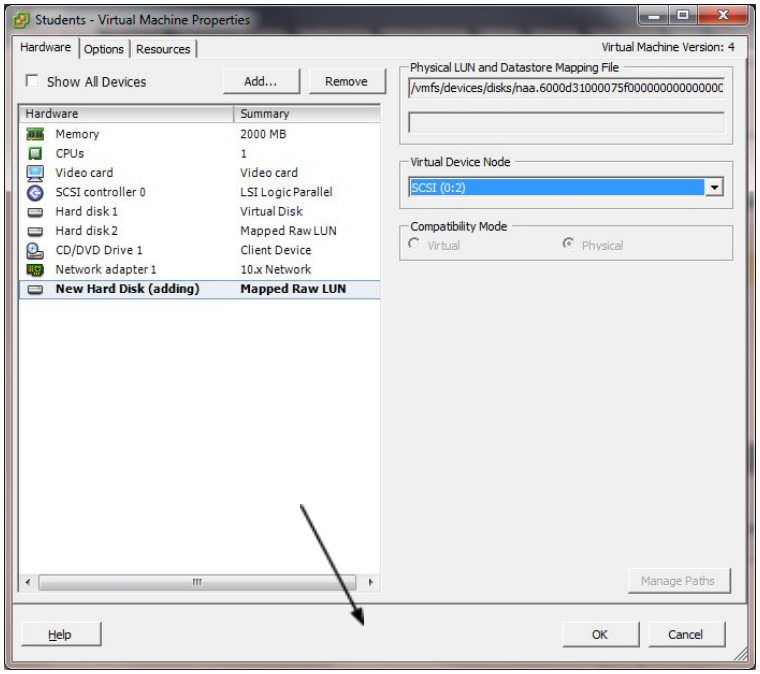
8.) "Select the datastore on which to store the LUN Mapping"
Select "Store with Virtual Machine" This will store the LUN mapping info with the VM itself.
Click Next. (pic)



9.) Under the next screen "Select Compatibility Mode" the default setting is "Physical" leave this to the default. Click Next. Under the next screen under "Advanced Options / Virtual Device Node" leave the default setting. Click Next. Ready to finish completing the "Add Hard Disk" Review the settings.
Click Finish. (pic)



10.) You will now see the new “Hard Disk (adding)” listed in the “Students” – Virtual Machine Properties. Press OK. VMWare will then add the new disk accordingly and respond with a 100% complete. (pic)

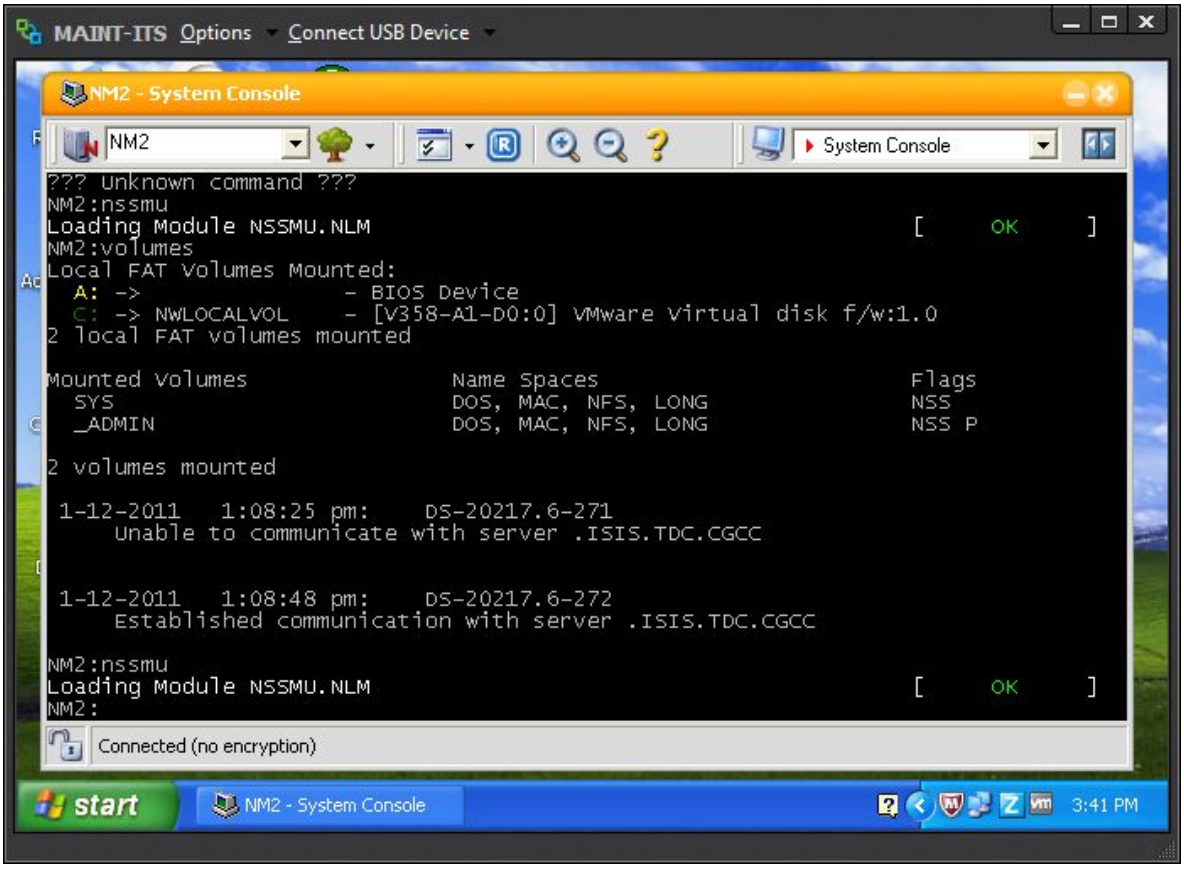


Novell Netware 6.5sp8 NSS Volume Mounting Instructions

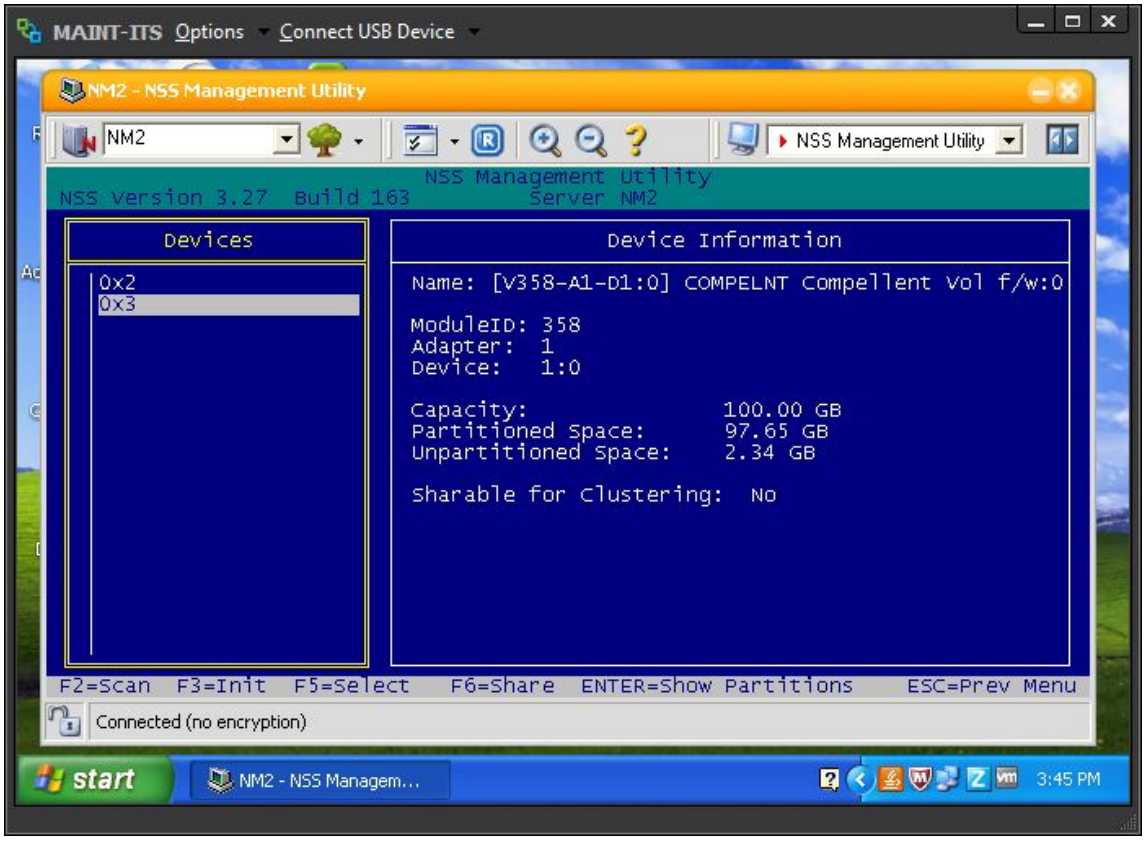
11.) Log in to vSphere Client, Go to Home -> Inventory -> Hosts and Clusters, expand vSphere2.cgcc.cc.or.us, CGCC (datacenter) expand VMWare_Cluster, highlight guest VM "NM2" by clicking on the VM. Then open a console to the VM. (rt. Mouse click – Open Console to the Server "NM2")

11b.) Alternatively, the Novell Netware Server Console can also be accessed via AdRem FreeCon

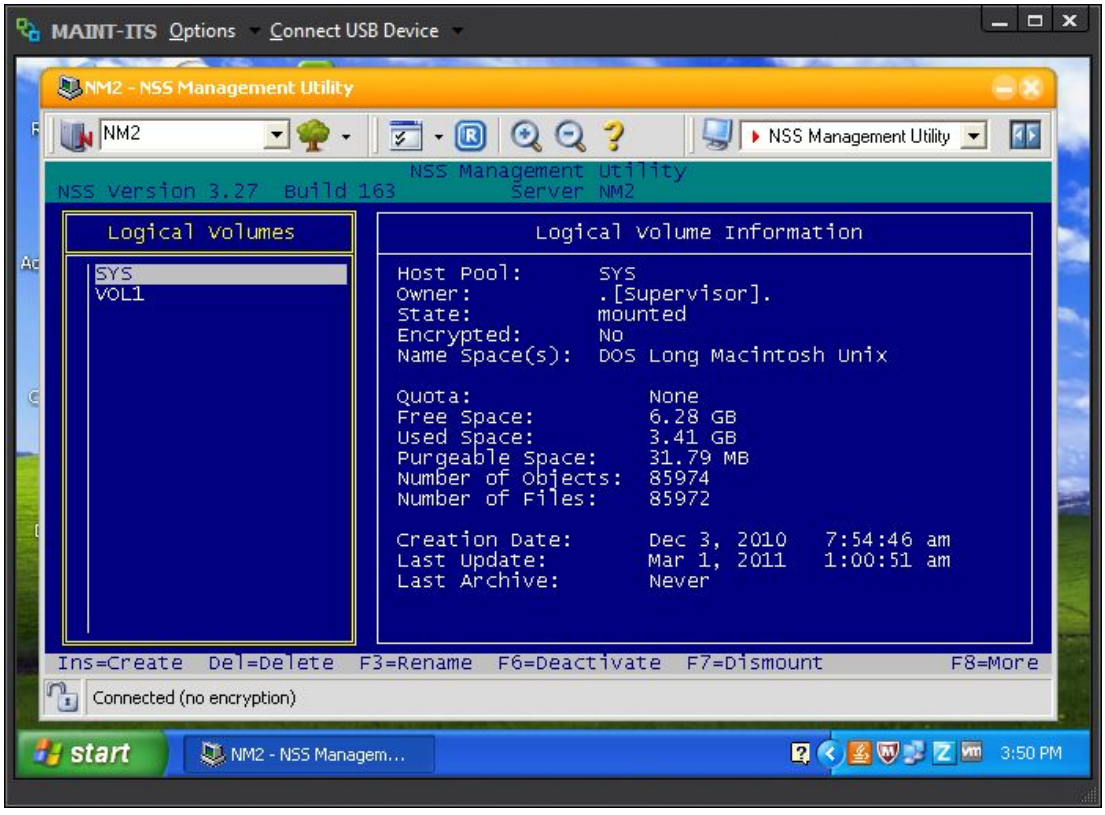
12.) In the Console window of "NM2" type nssmu (pic)



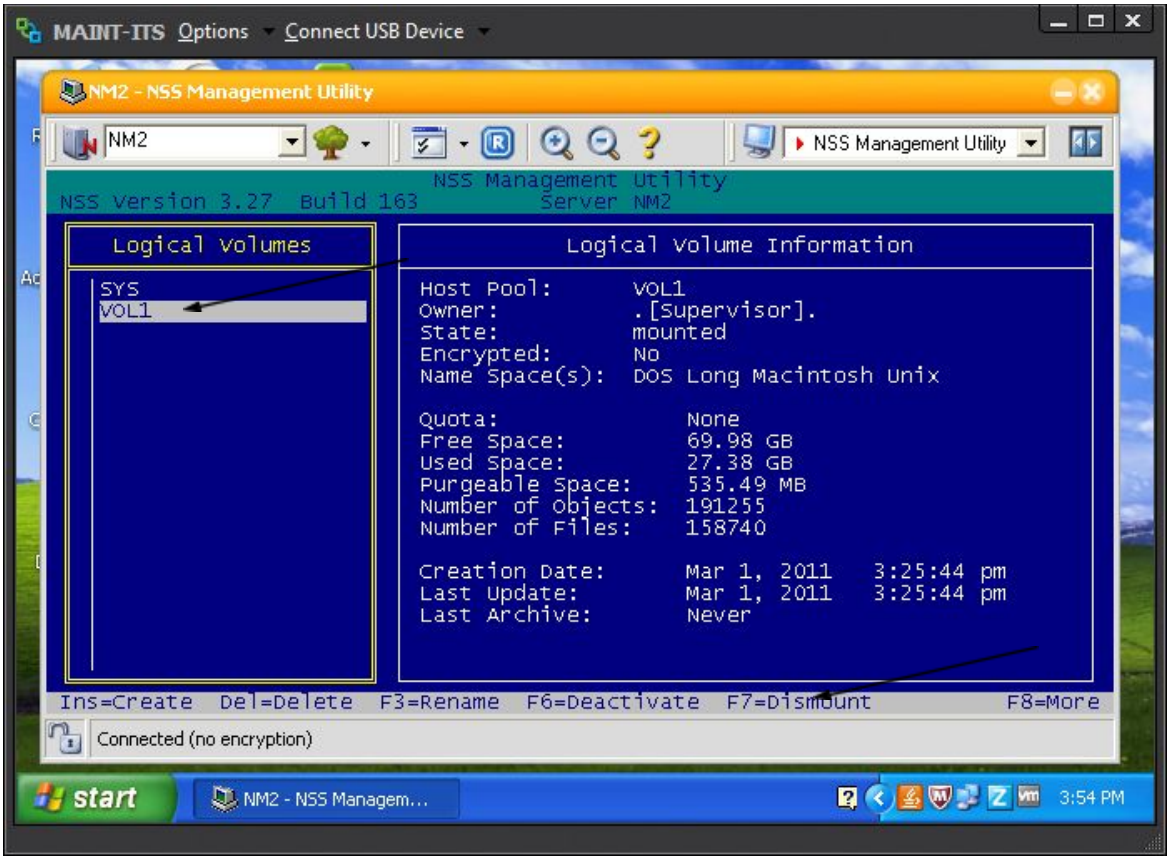
13.) In the NSSMU window, select Devices and press F2 – Scan. Verify that the new device shows up after the scan by highlighting it. Confirm the data volume size is correct. Press ESC (pic)



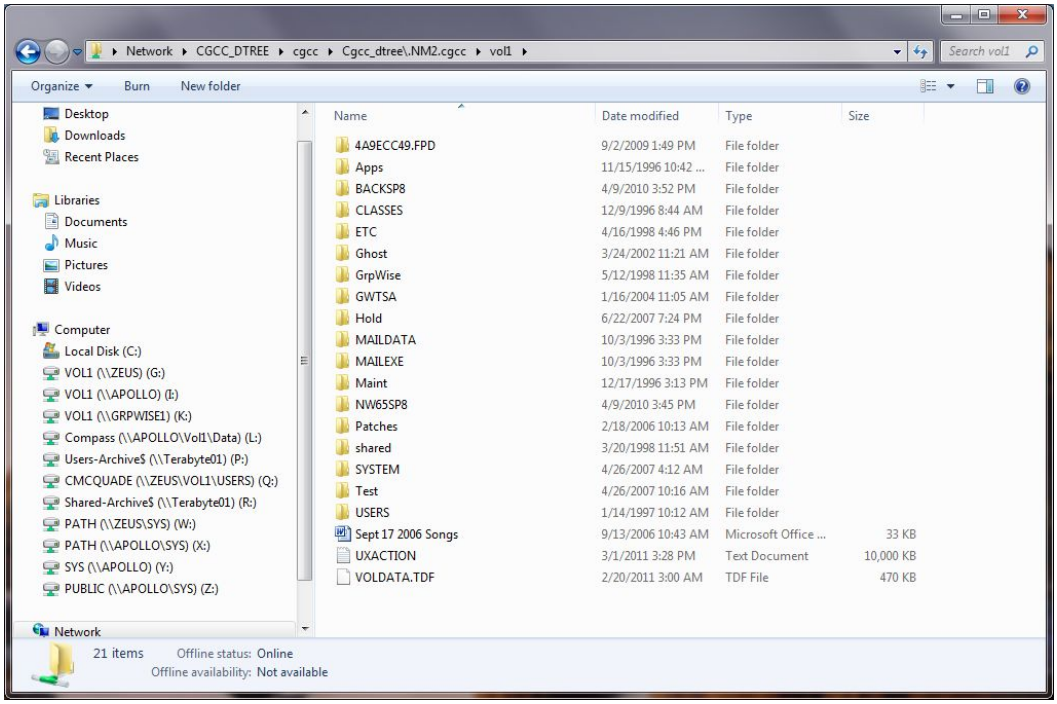
14.) In the NSSMUU select “Volumes” confirm that “VOL1” is listed as a volume. (pic)



15.) To Mount the volume highlight “VOL1” and press F7=mount, this will then mount the volume to the Netware Server. Browse to the newly recovered volume using “Windows Explorer” (pic)



16.) Browse to the newly recovered volume using “Windows Explorer” Recover Data As Needed. (pic)



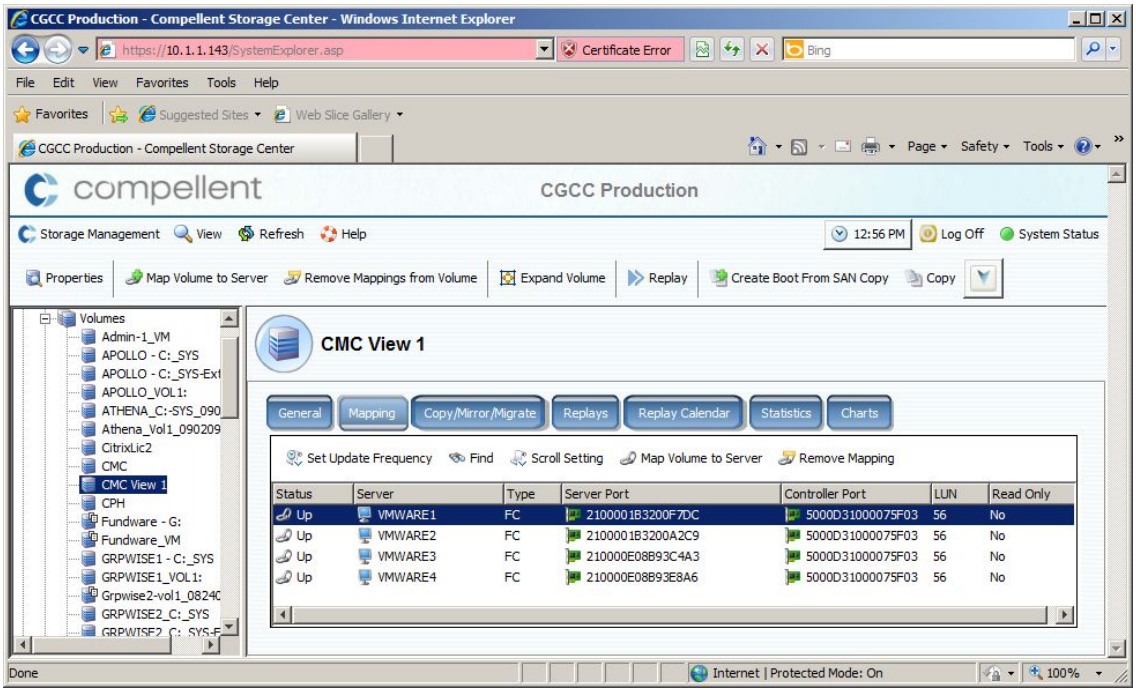
Section 3.3.3.4 – Windows/Netware OS, Boot Partition & Complete Server Restore

Note: Before restoring a complete server, confirm that the bad or corrupt VM (server) you are restoring is powered off.

1.) Log in to vSphere Client, Go to Home -> Inventory -> Hosts and Clusters, expand vSphere.cgcc.cc.or.us, The Dalles (datacenter) expand TD_PE-R620, highlight server “CMC” rt. Mouse Click, select Power, shut down guest OS. If no graceful down then OK to just power off the VM.

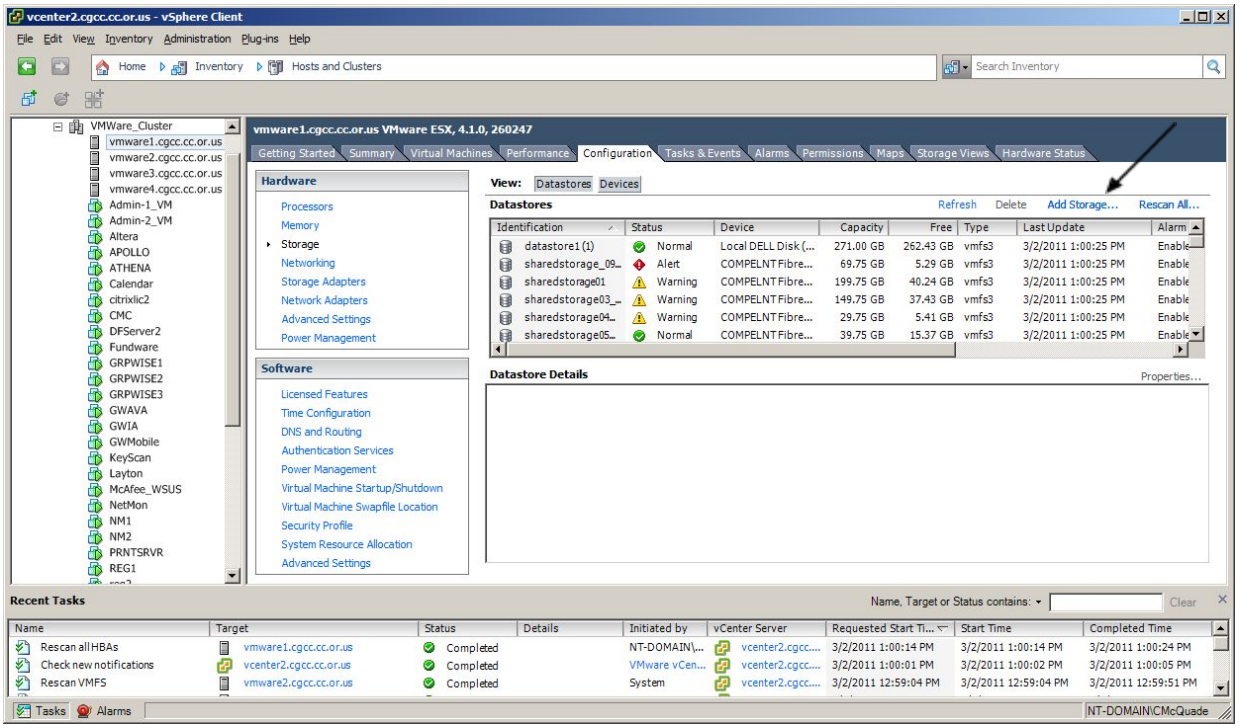
2.) Rt. Mouse click the VM “CMC” and remove from Inventory. This will remove the existing problematic server from VMWare Inventory but will not remove the data or datastore for further analysis later.
Confirm the server has been removed by verifying it is not in existing inventory.

3.) Log into Compellent SAN, create a local recovery of current replay of volume “CMC” map the volume to each server in the VMWare using the next avail. LUN. In this exercise we will create a “Shared Volume” that can be accessed to restore a complete server. (pic)

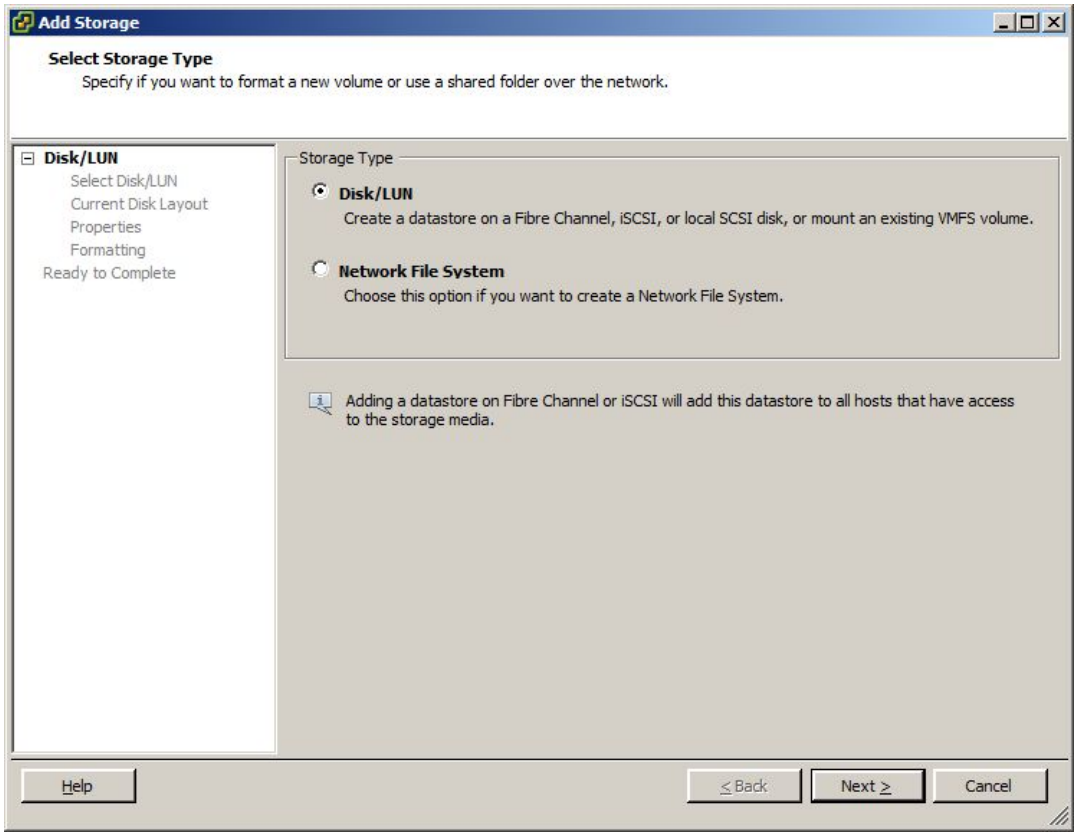


4.) Log in to vSphere Client, Go to Home -> Inventory -> Hosts and Clusters, expand vSphere.cgcc.cc.or.us, The Dalles (datacenter) expand TD_PE-R620, highlight host server "vmware12.cgcc.cc.or.us" and select the "Configuration" tab. Click the link "Storage Adapters" and find the storage adapter "8Gb Fibre Channel to PCI Express HBA" highlight "**vmhba2**". Below under "Details" click the "LUN" Menu and sort least to greatest. Note the last LUN number that was created in section 3.2.2.1 you will use this information to create the new "Shared Volume".

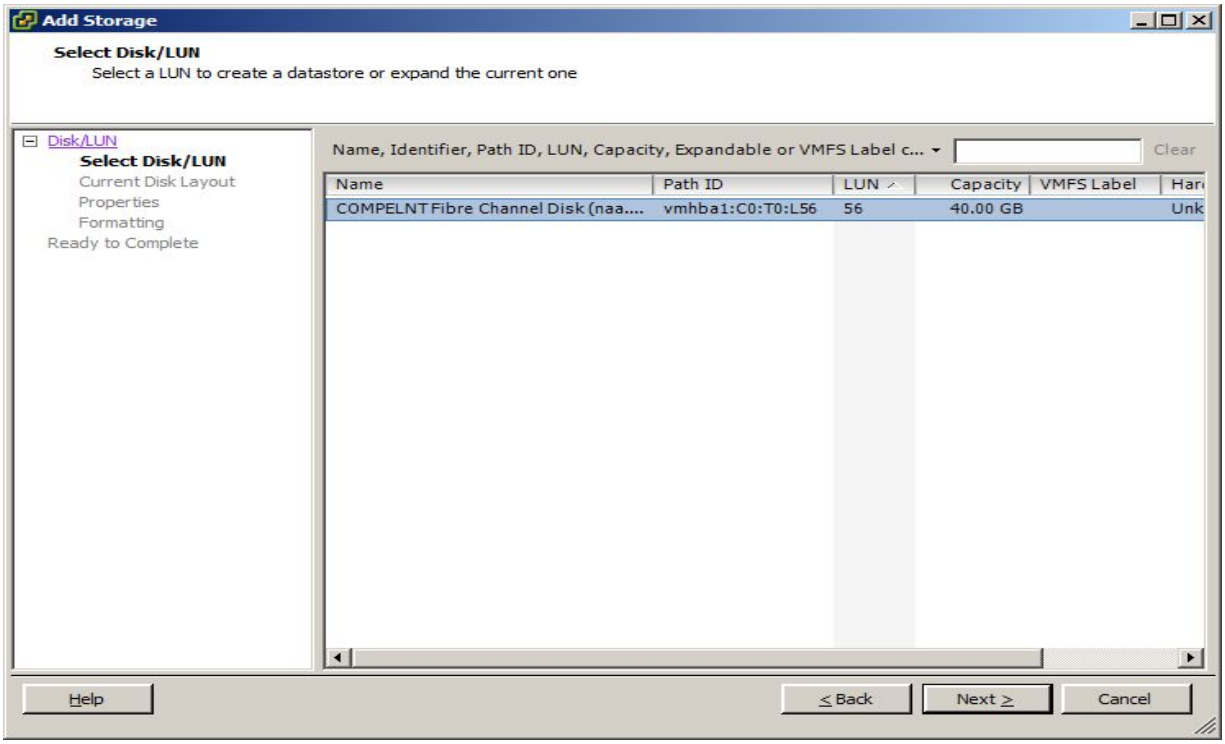
5.) In vSphere, Under the Configuration Tab of, vmware12.cgcc.cc.or.us, Click the link "Storage" this will bring up the Datastores configuration screen. Click "Add Storage" (pic)



6.) When adding a new storage, Select Disk/LUN and press NEXT. (pic)



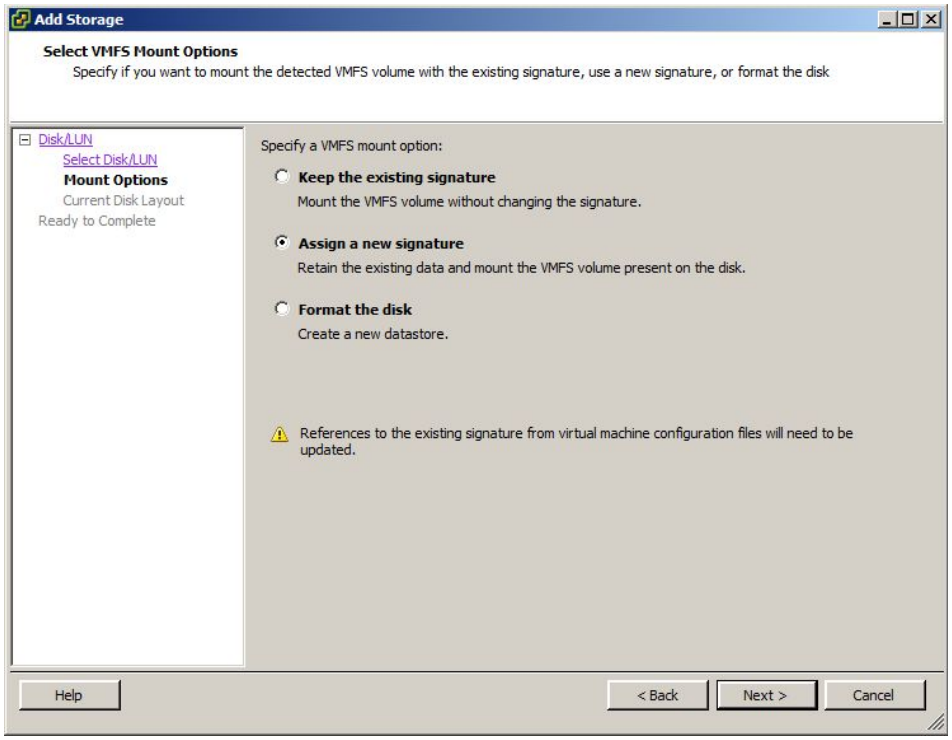
7.) Highlight the volume that was presented to VMWare from step 4, by clicking on it. Confirm the LUN ID is correct. Click NEXT (pic)



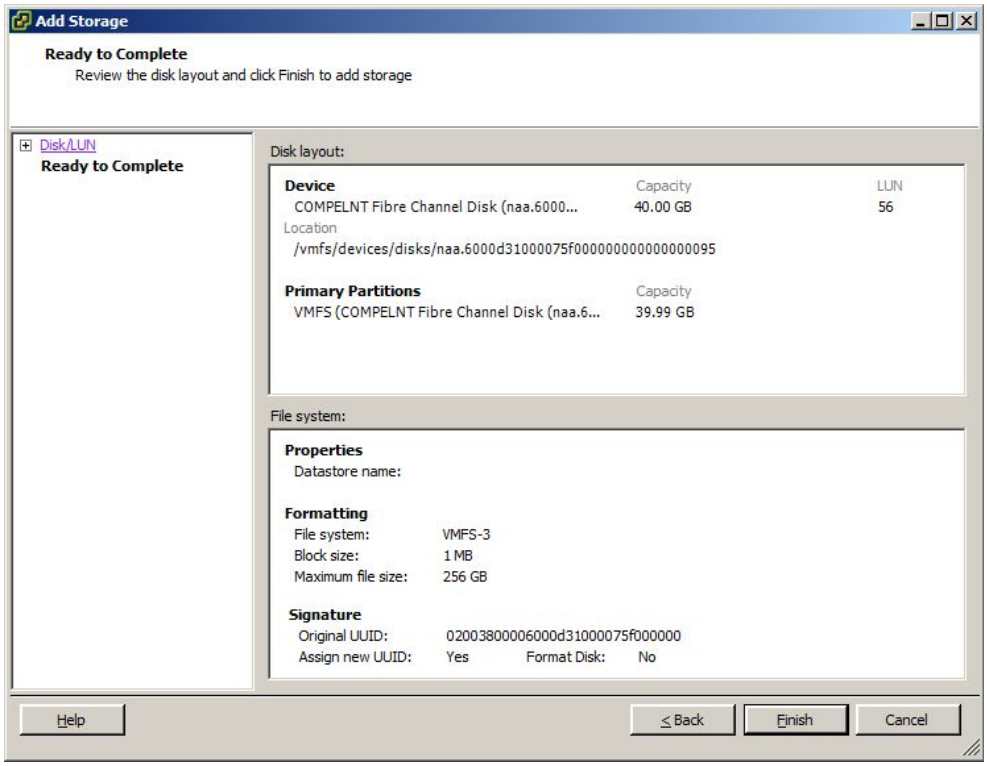
8.) ******Very Important*******

On the next screen, “Select VMFS Mount Options” We are essentially going to re-mount a similar volume that was previously being used for the “CMC” server. In the VMFS Mount options select

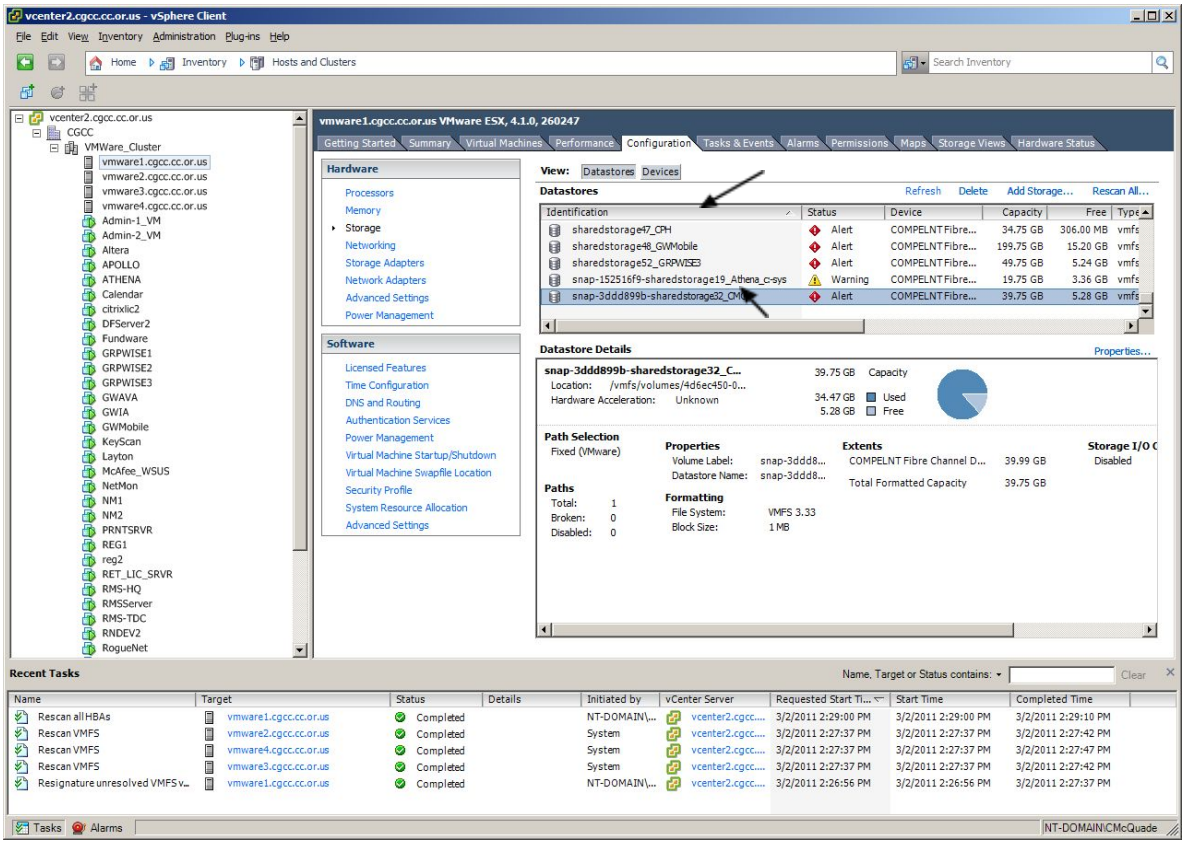
“Assign a new signature”



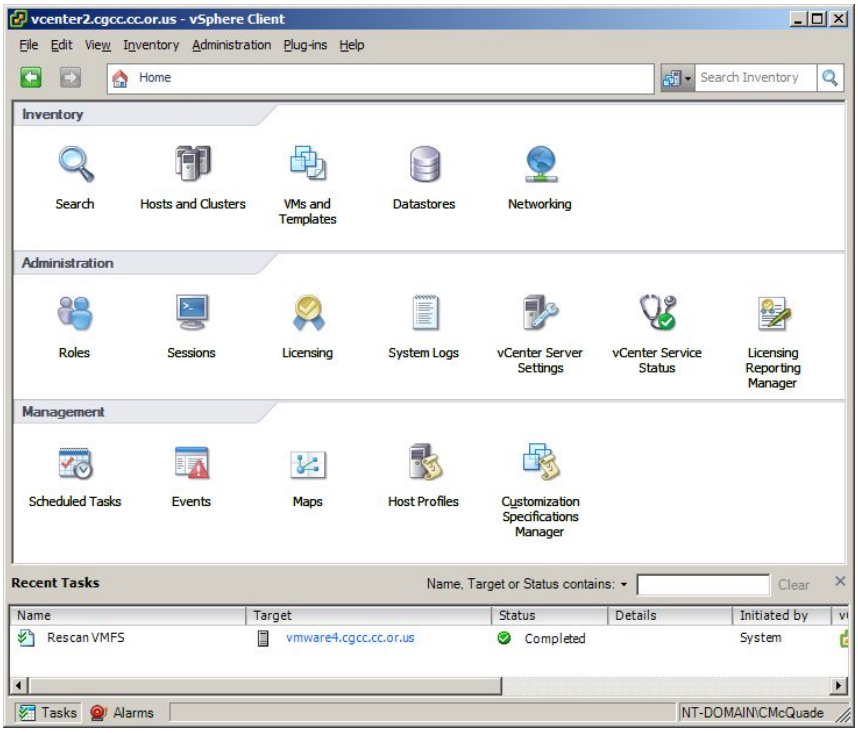
9.) Review the disk layout, Click Next. Ready to Complete. Click Finish. (pic)



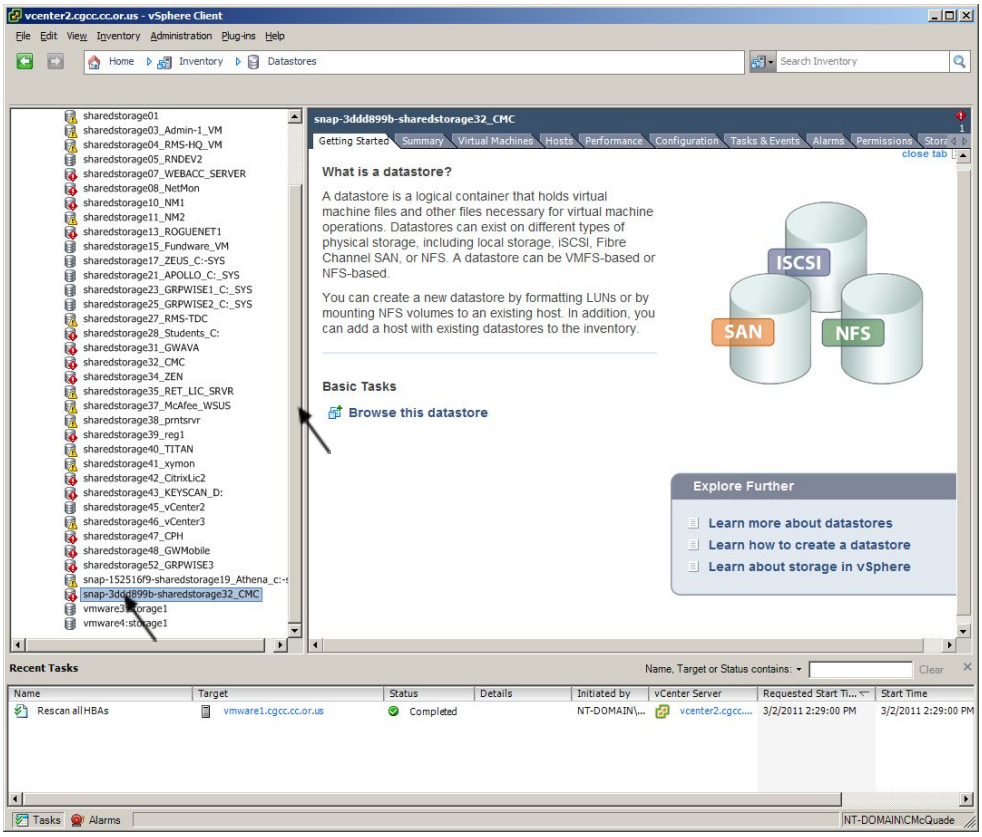
10.) Confirm that each VMWare host in the cluster has the newly created datastore. Click on Configuration Tab, Storage, Name should = "snap-(identifier)-sharedstorage(LUNID)_servername" To verify click the "Identification" button. (pic)



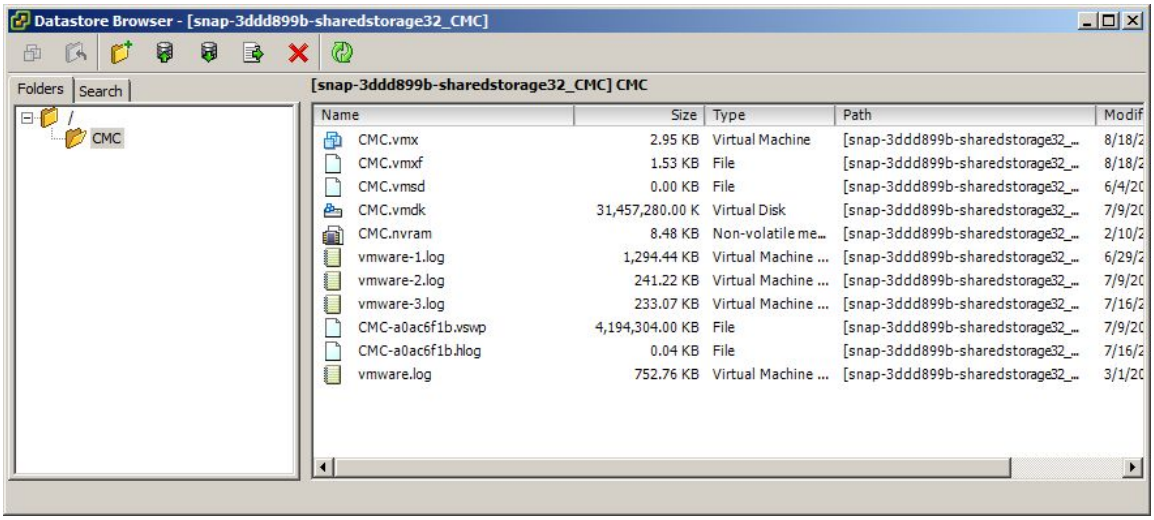
11.) Now that the “snap-(identifier)-sharedstorage(LUNID)_servername” has been successfully mapped to the VMWare cluster and the storage has been configured. The VM or server that exists inside this volume must be brought into the VMWare Inventory and booted. In vSphere click the “Home” link. Select “Datastores” (pic)



12.) Find the datastore “snap-(identifier)-sharedstorage(LUNID)_servername” datastore that was previously created, highlight it and then click **“Browse this datastore”** (pic)

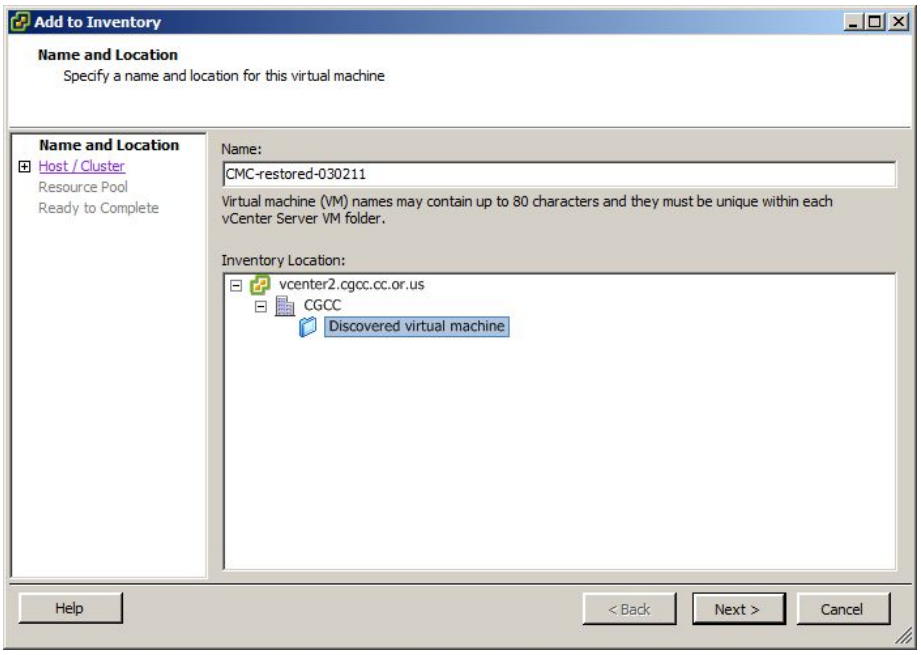


13.) In the “Datastore” browser, expand root, expand the VM folder (i.e. “CMC”) (pic)

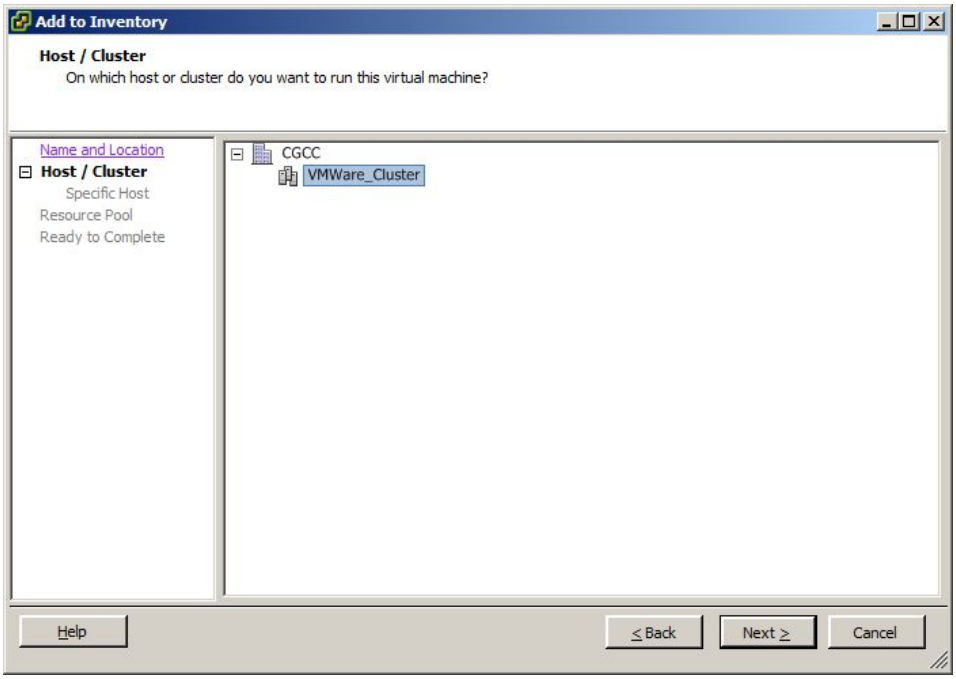


14.) Rt. Mouse Click the “CMC.vmx” and select “Add to Inventory” (pic)

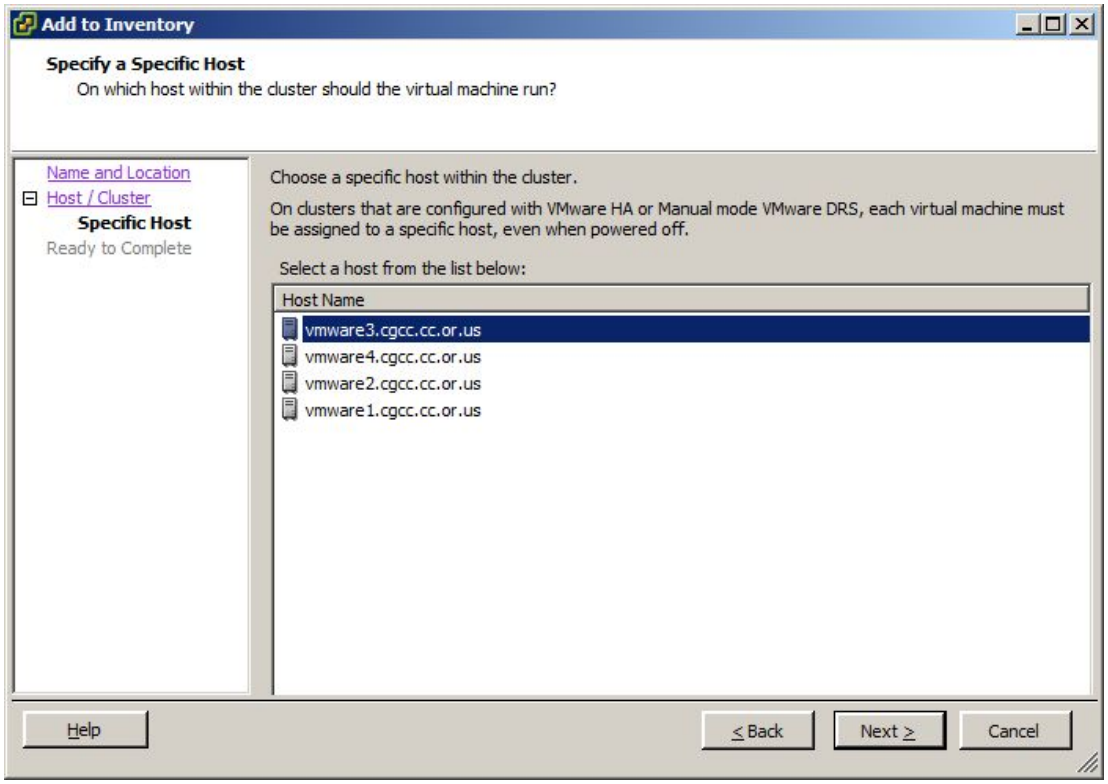
15.) In the “Add to Inventory” wizard, **“Name:”** use the following name for recovered VMs “servername-restored-mmddyy” i.e. “CMC-restored-030211” highlight the blue folder “Discovered virtual machine” Click Next (pic)



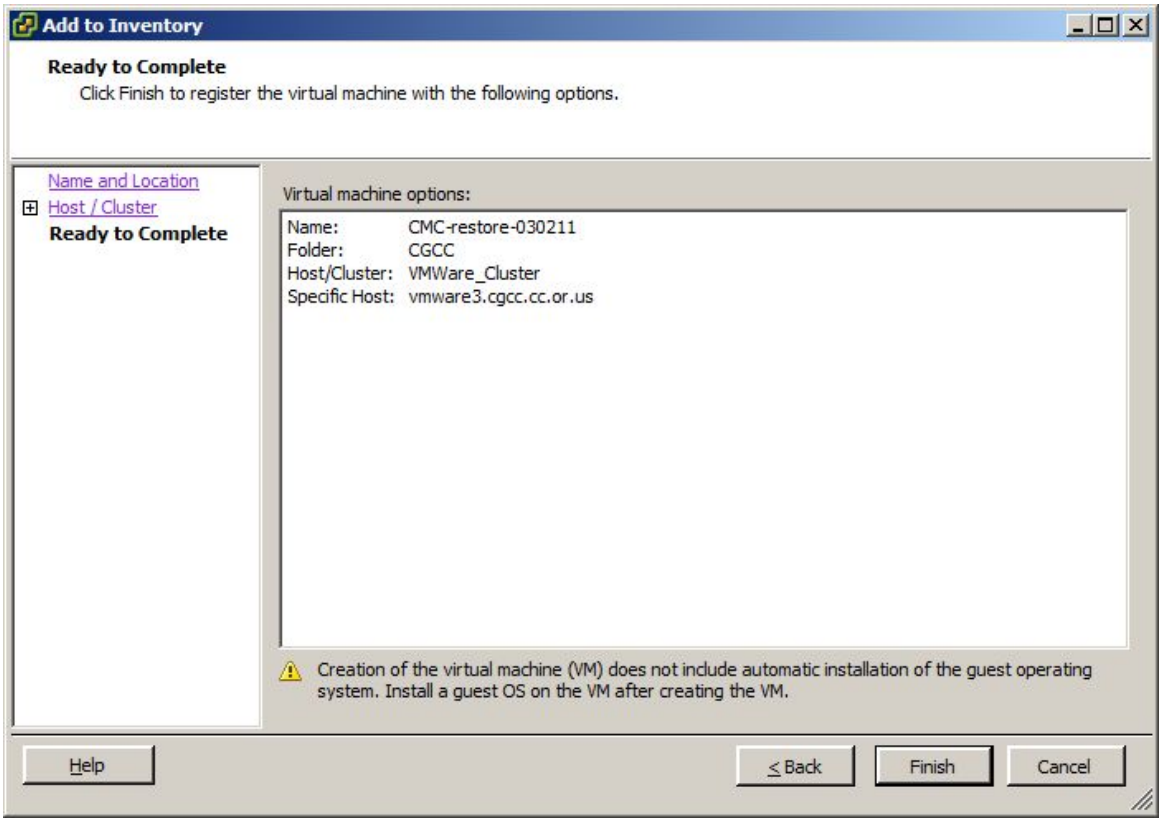
16.) In the Host/Cluster window specify “VMWare_Cluster” highlight it by clicking it. Click Next. (pic)



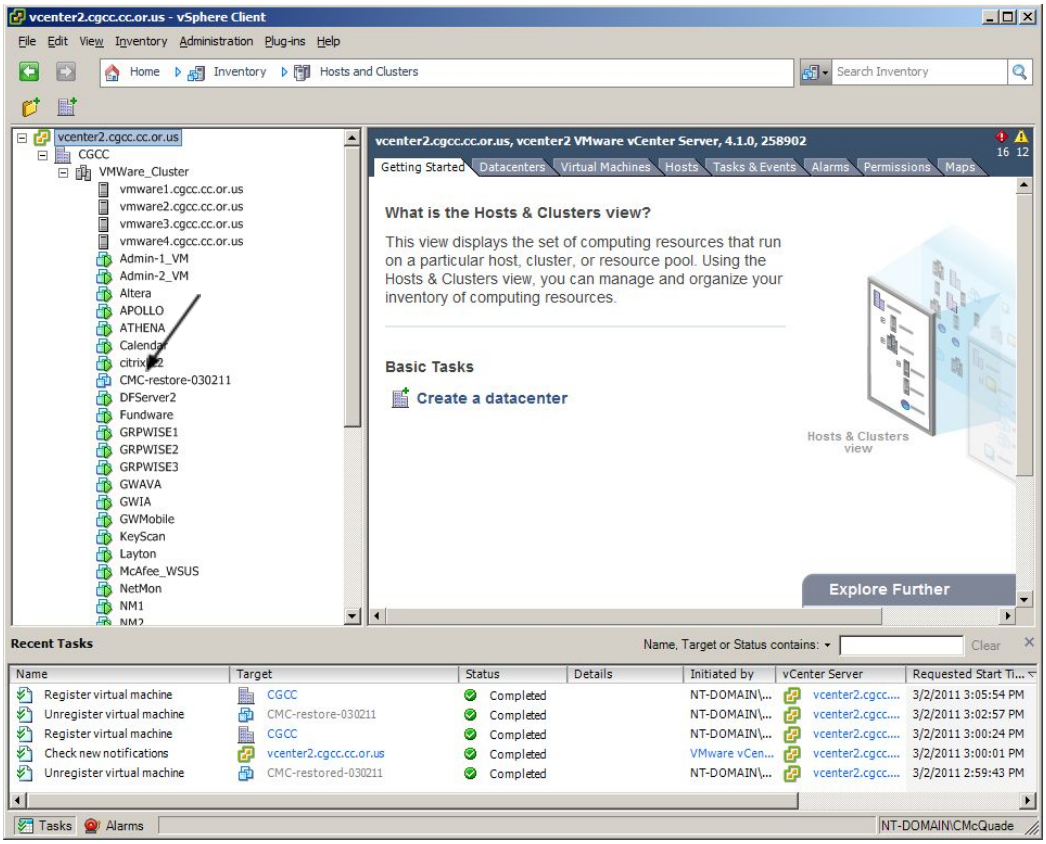
17.) In the “Specify a Specific Host” window any VMWare host will adequately support a restored server. Select any one of the “VMWare(x).cgcc.cc.or.us” hosts 1-4, Click Next. (pic)



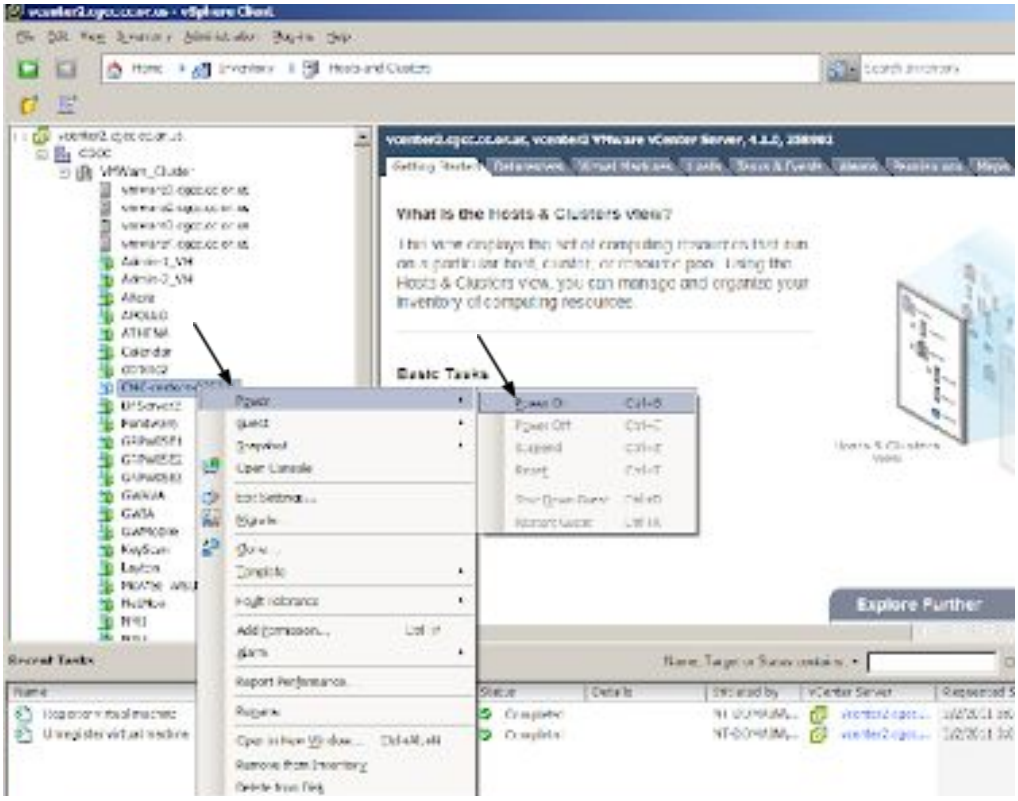
18.) Verify the newly restored VM, Click Finish (pic)



19.) In vSphere, Goto Home->Inventory->Hosts and Clusters, Expand VSphere.cgcc.cc.or.us, Expand The Dalles, Expand, TD_PE-R620. Verify that the newly restored VM is listed in Inventory. (pic)



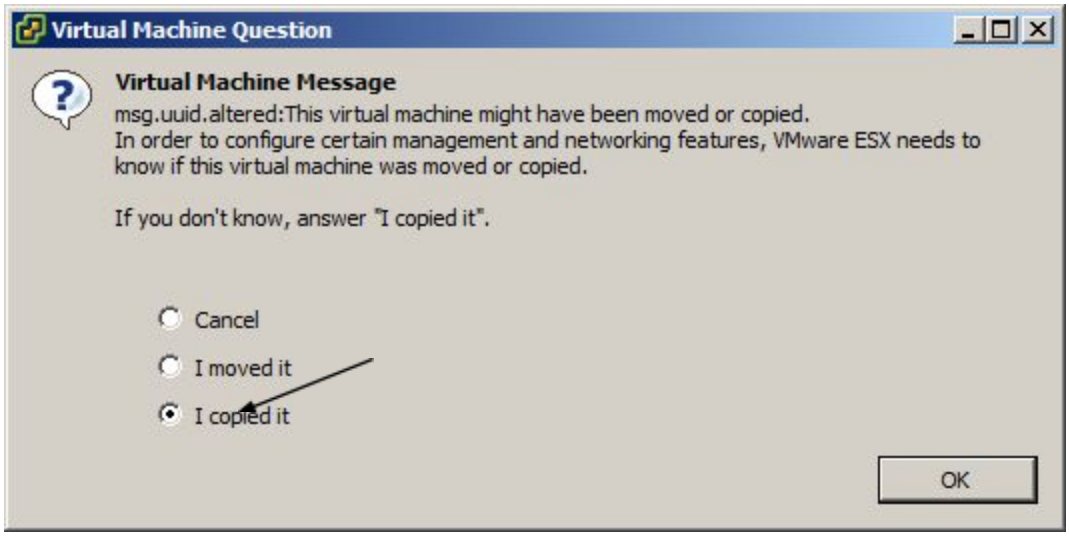
20.) Power On Server by rt. Mouse clicking the guest VM and select Power, Power On! (pic)



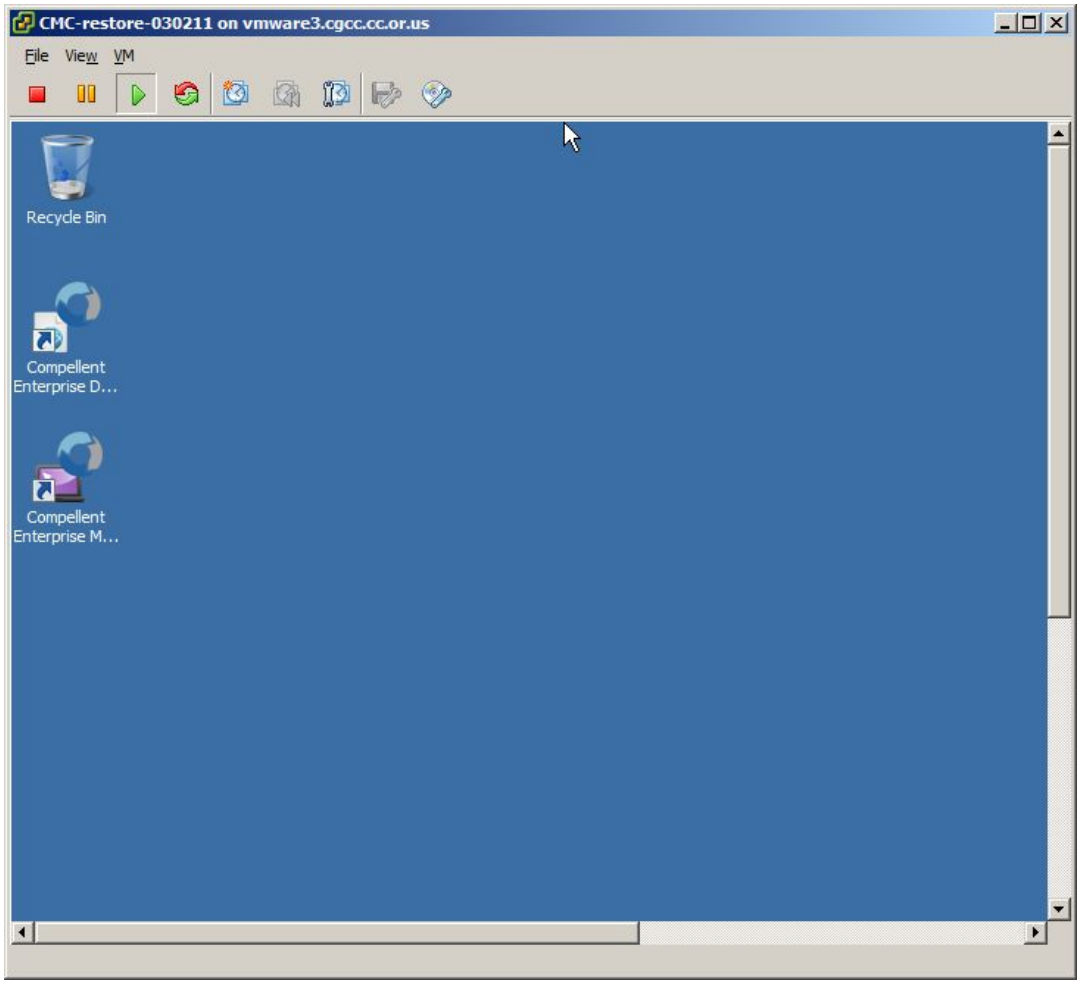
21.) ******Very Important******

After powering on the VM, open a console to the server. You will be prompted with the following question. Select "**I moved it"** Press OK, VMWare will then boot the server normally.

NOTE: In the console session select "Start Normally" for Windows Servers. (pic)



22.) Verify that the VM has booted properly by logging into the VM with [redacted]



3.3.4 VMWare Virtual Server Hosting

Areas of recovery / protection

Applications	Data	Hardware	Infrastructure	
			Data Center	Edge
✓	✓			

Primary Contacts:

	Name	Home Phone	Mobile Phone
Primary	Adam Gietl	[redacted]	[redacted]
Secondary	Bill Bohn	[redacted]	[redacted]
Past	Chris McQuade	[redacted]	[redacted]
Vendor Support	VMWare C2ITSystems		

Description:

The College utilizes local cloud computing technology from VMWare. VMWare provides the ability to virtualize multiple server OS's (Guests) on a single piece of server hardware (Host) that

is connected to a central Storage Area Network (SAN). Additional enhancements also provide the ability to migrate a Guest OS from one physical Host to another Host, without shutting down the OS. Yet another enhancement provides for the automatic OS migration should the infrastructure monitoring system discovers a problem on a Host.

Current VMWare products and version include:

- VMWare12.cgcc.cc.or.us ESXi 6.0
- VMWare13.cgcc.cc.or.us ESXi 6.0
- VMWare14.cgcc.cc.or.us ESXi 6.0
- VMWare15.cgcc.cc.or.us ESXi 6.0

Scope of protection:

What it protects: This technology protects the integrity and “up time” for the College servers.

1. This technology changes an OS to an object that can be backed up and restored on any available Host. This gives us the capability to implement major changes to a server or network software package, and have the ability to use a backup of the Guest to return the system as it was before the change.
2. Since the OS’s are no longer hardware dependant, should there be hardware problems, the Guest can be migrated to another Host. Then when the hardware is fixed, the Guest can be migrated back to the original (or new) Host.

Parameters of protection:

Automatic Guest migration is limited to Hosts that have the exact same motherboard specifications. Currently we have (4) Hosts capable of automatic OS migration.

3.3.5 User Security Redundancy (eDir & Windows domain)

The College operates two network security systems, eDirectory and Windows Domain Services. Each provide access to different areas of the College's network. Users are manually entered in both systems, and passwords duplicated in each system to allow for a single sign-on.

The college duplicates each security system on different servers to provide continuous security services if another security server goes offline. Security servers are as follows:

Netware eDirectory servers:

NM1	Master Replica
NM2	Read/Write Replica
GrpWise1	Read/Write Replica
Zeus	Read/Write Replica
HRC1	Read/Write Replica

Windows Domain Services

TD-DC1	Master R/W Domain Controller
TD-DC2	Secondary R/W Domain Controller
TD-DC3	Read-Only Domain Controller
HR-DC1	Secondary R/W Domain Controller

3.3.6 Moodle Backup

Moodle is hosted by eThink Education. If there has been a loss of data within Moodle you will need to submit a help ticket with eThink Education to request that the missing data be restored. The request must come from an approved vendor contact, which is listed below.

Primary Contacts

	Name	Email	Primary Phone	Secondary Phone
Primary	Rob Kovacich	[redacted]	[redacted]	
Secondary	Danny Dehaze	[redacted]	[redacted]	[redacted]
Third	Bill Bohn	[redacted]	[redacted]	[redacted]
Vendor Support	eThink Education	support@ethink.com	ethink.desk.com	

3.4 Hardware & Network Infrastructure Precautions

3.4.1 Server Hardware

Areas of recovery / protection

Applications	Data	Hardware	Infrastructure	
			Data Center	Edge
✓	✓			

Primary Contacts:

	Name	Home Phone	Mobile Phone
Primary	Adam Gietl	[redacted]	[redacted]
Secondary	Bill Bohn	[redacted]	[redacted]
Past	Chris McQuade	[redacted]	[redacted]
Vendor Support	Dell		

Description:
The College standardized on Dell servers to maintain consistent operating & support specifications and processes. RAID 5 and dual power supplies are standard configurations for all servers.

Scope of protection:
What it protects: RAID 5 protects data integrity and system “up time”. It requires a set of 3 or more hard drives. This technology allows for any one drive to fail without losing data or having the system fail.
The redundant power supplies allow for a one power supply to fail, and not affect the server's operation. Dual power supplies also provide a convenience of not needing to shut down a server when relocating its power source. (One power supply can be relocated at t time without shutting down the server.)

3.4.2 Brocade POE Wire Closet Switches (extra & stored configurations)

Describe the edge switches & configurations & UPS setup
Outline where the backup configurations exist

3.4.3 Core Switch Hardware & Route redundancy

Describe the core setup
Outline location for backup configurations

3.4.4 Physical Security

Every technology infrastructure distribution point is secured by either the College’s security card system or by key. The security cards are managed by Facility Services, and only select employees have physical keys that will open the technology rooms.

3.4.5 Environmental Controls

The data center environment is controlled by two Liebert HVAC units. These units are managed and maintained by the Facility Services Department.

Areas of recovery / protection

Applications	Data	Hardware	Infrastructure	
			Data Center	Edge
		✓	✓	

Primary Contacts:

	Name	Home Phone	Mobile Phone
Primary	Jim Austin		[redacted]
Secondary	Ino Olivan		[redacted]
Vendor Support	Liebert Vendor ???		

Description:
The College standardized on Dell servers to maintain consistent operating & support specifications and processes. RAID 5 and dual power supplies are standard configurations for all servers.

Scope of protection:
What it protects: RAID 5 protects data integrity and system “up time”. It requires a set of 3 or more hard drives. This technology allows for any one drive to fail without losing data or having the system

Two Liebert environmental units
CGCC Expectations:
1. Server Room temperature maintained at 70 +/- 3 degrees
2. Humidity maintained at 50% +/- 10%
3. Either single Liebert unit can maintain expectations #1 & #2
4. Email/text event notification capability
5. Automated (scheduled) monthly fail-over test (with event notification)
6. Automatic fail-over (lead/standby) on High or Low temperature levels (76 high, 64 low), with event notification
7. Remote control capability (I.e. for monitoring and switching active unit

Monitoring/Notification:
Lieberts send alert to ZX-CriticalAlerts@cgcc.edu
APC InfrastruXure temperature & humidity
Sends alert to ZX-CriticalAlerts@cgcc.edu as outlined in section 3.1.
Different alerts for : “HVAC” & “Critical” or “HVAC” & “General”XXX” in the Subject line (check CriticalAlerts account for notification list)

Monitor levels:
Temperature ranges that trigger an alert:

Humidity triggers:
Extra APC independent Temperature on Data Center Rack

3.5 Future Plans

GWAVA RELOAD for GroupWise

4.0 MID-DISASTER PROCEDURES

This section covers the activities to perform during a disaster. Since we cannot predict every type & scope of a disaster, basic scenarios will be used.

4.1 Activity Checklists

Steps to take in case of fire, earthquake, water disaster, physical property damage, data corruption, power outage, computer virus attack, or hacking attack

4.1.1 Communication

- For fire, bomb threat, physical property damage (taking place), or earthquake with damage – CALL 911
- Communicate to ITS Staff

In the case of a disaster that affects the Data Center, notify the following:

	Name	Home Phone	Mobile Phone
1	Bill Bohn	[redacted]	[redacted]
2	Adam Gietl		
3	Richard Jepson		
4	Danny Dehaze		
5	Ron Watrus		

- Communicate to Facilities

	Name	Home Phone	Mobile Phone
1	Jim Austin		[redacted]
2	Ino Olivan		
3	Call Facilities Emergency ph#		

- Once one of the above is notified, they should notify all of ELT, in the following order:

ELT	Phone #1	Phone #2
Dr. Toda	[redacted]	[redacted]
Robb Van Cleave		
Saundra Buchanan		
Karen Carter		
Dan Spatz		
Susan Wolff		

4.1.2 Power outage

- Determine what is providing power to the Data Center, the generator or APC system.
  - ➢ You can tell by hearing the generator running, and looking at the displays on the front of the APC units in the Data Center
    - Determine an expected recovery time frame
      - Determine what shutdown is needed
        - ➢ Partial Shutdown (Section 6.1)
          - o *Follow these steps if you have <u>over</u> 1 hour AND the Data Center temperature is over 85 degrees and not cooling.*
        - ➢ Complete Graceful Shutdown (Section 6.2)
          - o *Follow these steps if you have <u>under</u> 1 hour and over 15 minutes left of power OR the Data Center temperature is over 90 degrees and not cooling.*
        - ➢ Emergency Quick Shutdown (Section 6.3)
          - o ***Follow these steps if you have 15 minutes or less power left OR the Data Center is over 95 degrees and not cooling.***

4.1.3 Environmental Unit Failure (Heat)

- Get current data center temperature and idea of how fast it is raising
  - Determine an expected recovery time frame
    - Determine what shutdown is needed
      - ➢ Partial Shutdown (Section 6.1)
        - o *If the Data Center temperature is over 85 degrees and not cooling.*
      - ➢ Complete Graceful Shutdown (Section 6.2)
        - o *If the Data Center temperature is over 90 degrees and not cooling*
      - ➢ Emergency Quick Shutdown (Section 6.3)
        - o ***If the Data Center is over 95 degrees and not cooling***

5.0 DATA CENTER SHUTDOWN PROCEDURES

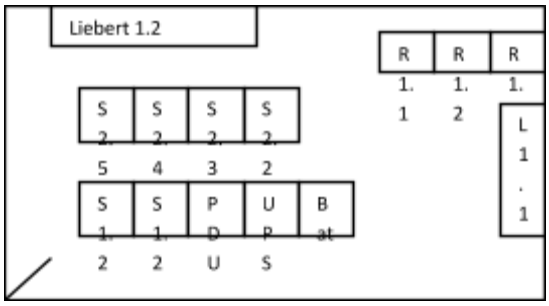
There are three different shutdown levels, Partial, Complete Graceful, and Complete Quick Emergency. Each is used for different circumstances.

Each shutdown procedure will reference similar terminology & server shutdown steps.

Terminology:
Cabinets are the black units in the center part of the Data Center room.
Racks are the open air units in the back right corner of the room.

The Dalles Data Center
Identifying equipment locations.
Cabinets are numbers by row & cabinet number.
For example: Cabinet S1.2 is the second cabinet in row 1.
The Racks are numbered 1.1 thru 1.3
The Lieberts are numbered 1.1 & 1.2

The floor plan with related numbering is shown below:



Steps for shutting downing servers
Servers are controlled by KVM units or through our VM virtual infrastructure. The servers are shutdown via one of these methods.

KVM usage:
KVM units utilize one keyboard & mouse to control multiple servers.
KVM's are located in Cabinets S1.2, S2.3 & S2.5
To use the KVM slide out the keyboard/monitor & tilt up the monitor
To select the server, press:
Scroll-Lock, Scroll-Lock, Space-Bar
Use the arrow keys to point to a server, and Enter to select the server
Press Esc to remove the server list from the screen

Virtual host access via vSphere
Go to the vSphere KVM, select the vSphere Server
Login using [redacted]
When prompted by VSphere
Select to use domain credentials
Enter the IP: [redacted]

Select the desired server by name

Right click on the server name, select Power, then select ***Issue guest shutdown***

Or

Select the Console Tab to get to the server's desktop, then

Follow the type of server shutdown procedures

Login to that server (check IP table for Login information)

Click on Start, Shutdown

Netware Servers:
Close any major applications by displaying the application list (Press Alt-Esc), selecting the highest numbered application, then follow any onscreen instructions to Exit or Quit
There will be applications listed that cannot be closed, do not worry about those apps.
When you cannot close anything else,
Get to the console screen by pressing Alt-Esc, and then selecting One
At the console screen type DOWN
Enter Y if prompted that there are open files.
If the server does not shut down, then issue a power off from vSphere

Windows Servers:
With Windows servers, you can issue a “Shutdown Guest” from vSphere Power options. OR,
Login to the desired server using [redacted]
Click on Start, then select Shut Down

Linux Servers:
With Linux servers, you can issue a “Shutdown Guest” from vSphere Power options. OR, Login to the desired server using local credentials then shutdown.

5.1 PARTIAL SHUTDOWN

Follow these steps if you have over 1 hour AND
the Data Center temperature is over 85 degrees and not cooling.

Perform a partial shutdown in the case of needing to lessen the heat generation in the Data Center.

SERVER	CABINET	Virtual / Physical	SOFTWARE TO CLOSE
NETWARE SERVERS			
Isis	S2.3	P	BackupExec

WINDOWS SERVERS			
MtHood (Tape)	S2.3	P	Turn off Tape drive unit too!
CASAS	S2.5	P	
EMeter	S2.4	P	
Citrix3	S2.4	P	
Citrix2	S2.4	P	
Terabyte01 & 02	S2.2	P	After server off – turn off external drives

5.2 COMPLETE GRACEFUL SHUTDOWN

Follow these steps if you have under 1 hour and over 15 minutes left of power OR the Data Center temperature is over 90 degrees and not cooling.

Graceful shutdown means that Data Center equipment is shutdown in an ordered process that helps assure best success for system startup and least possibility for data loss or corruption.

First notify users that the entire system will be shut down.

- Send a Novell message to all users attached to Apollo
  - Right click on the red N in the taskbar
  - Select Novell Utilities, Send Message, To Users
  - Select the server Apollo, and click Select
  - Click the checkbox to "Show only user objects in list"
  - Type in the message that the system is shutting down
  - Click on Send
- From any phone, follow these procedures:
  - …..

5.2.1 Process the shutdown steps as outlined section 5.0 in the following order:

SERVER SHUTDOWN ORDER

SERVER	CABINET	Virtual / Physical	SOFTWARE TO CLOSE
NETWARE SERVERS			
Isis	S2.3	P	BackupExec
WebAcc		V	
Athena		V	Grpwise Student PO
GWIA		V	Internet Agent & MTA
GWAVA- Linux		V	Special shutdown-> Go to gwava's vSphere console Click to enable the screen Login using : [redacted] Type: shutdown now (Exit will logout)
GrpWise2		V	Admin PO
GrpWise1		V	MTA
Zeus		V	
Apollo		V	

SERVER	CABINET	Virtual / Physical	SOFTWARE TO CLOSE
WINDOWS SERVERS			
MtHood (Tape)	S2.3	P	>Turn off Tape drive unit too! >For startup, turn Tape drive on 1st
CASAS	S2.5	P	
EMeter	S2.4	P	
Citrix3	S2.4	P	
Terabyte01 & 02	S2.2	P	>After server off – turn off external drive >For startup, turn drive ON before starting the server
LinuxBase		V	Linux
Altera		V	
RET_LIC_SRVR			
AMX-DS		V	
zentdc			
MTGMGR		V	
HelpBox		V	
Intranet		V	Linux
Citrixlic2		V	
Reg1		V	
Reg2		V	
Students		V	
RNDev2		V	
Layton		V	
MtgMgr (AMX remote mgmt)		V	
CMC		V	
DFServer2		V	
DocImg		V	
K2Verity		V	
Admin-1		V	
Admin-2		V	
McAfee		V	
PrntSrvr		V	
GWMobile		V	Linux
Groupwise3		V	Server 2008
Calendar		V	Linux
RogueNet		V	
NetMon		V	
RMS-TDC		V	
RMS-HQ		V	
Titan		V	
vSphere3		V	

Fundware		V	
HVAC	S2.2	P	
TG2000	S2.2	P	
VideoSecurity	S2.2	P	
Keyscan		V	
Citrixlic2		V	
Phone System Shutdown			***See NEXT page 6.1.2***
Nm2		V	
Nm1		V	
RnDev	S2.3	P	
Admin-2		V	
Domain2 (domain & dns)		V	
Domain1 (domain & dns)		V	
vSphere2		V	
Citrix2	S2.4	P	
Hosts & vSphere		***P***	***See NEXT page 6.1.3***
SAN		***P***	***See NEXT page 6.1.4***

5.2.2 PHONE SYSTEM SHUTDOWN

1.) From the **KVM in S2.5** select each of the following servers and follow the Windows shutdown steps

a.) Cistera Convergence Server (Yellow Server) Depress and hold pwr button

b.) Unity –

a. You must be at the kvm console

b. Login using (User: [redacted] [redacted]

c. Type: Util system shutdown

c.) Cisco CM01 – Publisher (Phones are not connected to this one)

a. You must be at the kvm console

b. Login using (User: [redacted] [redacted]

c. Type: Util system shutdown

d.) Cisco CM02 – Subscriber (Phones are connected here – you will lose phone service at this point)

a. You must be at the kvm console

b. Login using (User: [redacted] [redacted]

c. Type: Util system shutdown

5.2.3 VMWARE SERVERS

VSphere client right click on the VM and select shutdown

In vSphere, go to each host server, right-click and select to go Enter Maintenance Mode,

Then shut down: User on all is :root

			PW
VMWare1	S1.2	P	[redacted]
VMWare2	S1.2	P	
VMWare3	S1.2	P	
VMWare4	S1.1	P	
TDC-vSphere	S1.2	P	

5.2.4 SAN

Once all of the servers are shut down, you can shutdown the SAN

1.) POWER DOWN SAN (Storage Area Network) – Confirmed by Compellent Co-Pilot support

AT THE SAME TIME:

Depress and hold “Red” power button on Compellent SAN Controller #1, [redacted]

Depress and hold “Red” power button on Compellent SAN Controller#2, [redacted]

Row 1, Rack2 (S1.2)

2.) Go to Back of Row1, Rack2 and turn off dual-pwr supplies on SAN Disk array, (2) on/off switches located on the left and right hand side of Disk Array

5.2.5 APC SHUTDOWN

1.) Pull ON/Off lever in cabinet in order of: Q2, Q1, A

5.2.6 LIEBERT UNITS

1.) Blue ON/Off button on control panel on the front right side of each unit.

6.0 EMERGENCY (QUICK) SHUTDOWN

Follow these steps if you have 15 minutes or less power left OR the Data Center is over 95 degrees and not cooling.

Emergency Server Room Shutdown Procedure – QUICK manual turn-off 09-30-09 (DRAFT)

2.) Depress and hold pwr button on server " vSphere ", Row1, Rack1

Note: saves vm database and health in current state

3.) Depress and hold pwr button on server "VMWare12", Row1, Rack1

4.) Depress and hold pwr button on server "VMWare13", Row1, Rack1

5.) Depress and hold pwr button on server "VMWare14", Row1, Rack1

6.) Depress and hold pwr button on server "VMWare15", Row1, Rack2

7.) Turn off DELL 132t Power Vault Tape Back-Up shelf, on/off switch located upper right corner

Row 2, Rack3

8.) Depress and hold pwr button on server "ISIS"

Row2, Rack3

Note: This now completes shutting down all server/ fc and iscsi volumes to SAN, therefore no more I/O to SAN

9.) POWER DOWN SAN (Storage Area Network) – Confirmed by Compellent Co-Pilot support

AT THE SAME TIME:

Depress and hold "Red" power button on Compellent SAN Controller #1, [redacted]

Depress and hold "Red" power button on Compellent SAN Controller#2, [redacted]

Row 1, Rack2

10.) Go to Back of Row1, Rack2 and turn off dual-pwr supplies on SAN Disk array, (2) on/off switches located on the left and right hand side of Disk Array

11.) Power Down Remaining Servers Manually

Row 2, Rack2

a.) Reg1, Depress and hold pwr button

b.) Titan, Depress and hold pwr button

c.) RNDEV, Depress and hold pwr button

d.) Citrix, Depress and hold pwr button

e.) Citrix3, Depress and hold pwr button

12.) Power Down Remaining Servers Manually

Row 2, Rack4

a.) Artemis, Depress and hold pwr button

b.) Video Server, Depress and hold pwr button

c.) HVAC Server#1, Depress and hold pwr button

d.) HVAC Server#2, Depress and hold pwr button

13.) Power Down Remaining Servers Manually “PHONE SERVERS”

Row2, Rack1

e.) Cistera Convergence Server (Yellow Server) Depress and hold pwr button

f.) Unity

g.) Cisco CM01 – Publisher (Phones are not connected to this one)

h.) Cisco CM02 – Subscriber (Phones are connected here – you may lose some phones at this point)

NOW THAT ALL SERVERS HAVE BEEN TURNED OFF – OK to hit “RED” EPO (Emergency Power Off) switch on wall nearest the entry door. “THIS WILL SHUT DOWN EVERYTHING ELSE IN THE ROOM – Except the Liebert HVAC Units.

Systems: that will go offline

a.) APC – UPS, All Data Center Power

b.) All CGCC Networks and Internet

c.) All Phones

d.) Hood River Campus LAN, WAN and Internet

e.) All Analog Devices tied into our Analog Gateway

f.) Liebert Site-Link 4, note: (Except Liebert Units will continue to run)

CONFIRM THAT BOTH LIEBERT HVAC UNITS (1.1 AND 1.2) ARE IN THE “OFF” POSITION, UPPER RT. HAND CORNER

THE SERVER ROOM IS NOW “OFF” Estimated Time To Complete: About 5 Mins.

7.0 DATA CENTER STARTUP PROCEDURES

If the Data Center was completely shut down, follow these steps to bring it back up and running.

1. If the EPO switch was pressed, reset the EPO switch.
2. Verify the following:

a. The APC system is ON, not showing any errors, and shows that it will supply power for at least 30 minutes

i. If the toggle switches are OFF turn them ON in the following order:

1. A, Q1, Q2

b. The core switches are up and running

3. Turn on the SAN system

a. Switch on the Disk array – wait 1 minute for drives to come up to speed

b. Switch on Controller [redacted]

c. Switch on Controller [redacted] – no need to wait for [redacted]

d. Wait until the system appears to be up and stable

4. Startup systems in the ***reverse*** order of the shutdown order

7.1 Process the STARTUP steps as outlined section 6.0 in the following order:

SERVER STARTUP ORDER

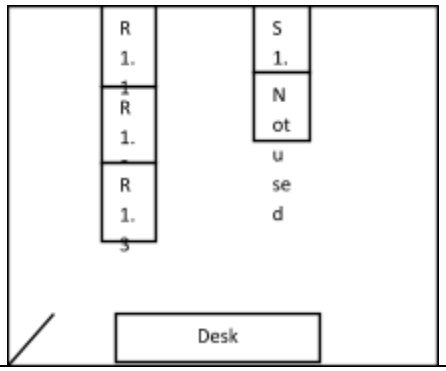
SERVER	CABINET	Virtual / Physical	SOFTWARE TO CLOSE
SAN		***P***	***See NEXT page XXX***
Hosts & vSphere		***P***	***See NEXT page XXX***
VMWare12	S1.2	P	
VMWare13	S1.2	P	
VMWare14	S1.2	P	
VMWare15	S1.2	P	
vSphere2	S1.2	P	
Domain1 (domain & dns)		V	
Domain2 (domain & dns)		V	
Admin-2		V	
Nm1		V	
Nm2		V	
CMC		V	
RnDev	S2.3	P	
Phone System Startup			***See NEXT page xxx***
NETWARE SERVERS			
Zeus		V	
Apollo		V	
GrpWise1		V	MTA
GrpWise2		V	Admin PO
Athena		V	Grpwise Student PO
GWIA		V	Internet Agent & MTA
GWAVA- Linux		V	Special shutdown ->
WebAcc		V	
Isis	S2.3	P	BackupExec *NOTE* Also Turn off the PowerVault Tape Unit, located in S2.3

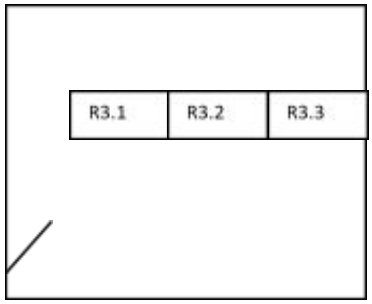
SERVER	CABINET	Virtual / Physical	SOFTWARE TO CLOSE
WINDOWS SERVERS			
GWMobile		V	
Titan		V	
RogueNet		V	
Reg1		V	
Reg2		V	
Citrixlic2		V	
Citrix3	S2.5	P	
Citrix2	S2.5	P	
McAfee		V	
VideoSecurity	S2.3	P	
HVAC	S2.3	P	
TG2000	S2.3	P	
CASAS	S2.5	P	
EMeter	S2.5	P	
Terabyte01 & 02		P	>After server off – turn off external drive >For startup, turn drive ON before starting the server
PrntSrvr		V	
RNDev2		V	
Layton		V	IT support
HelpBox		V	IT support
Xymon		V	
ZenTDC		V	
vSphere3		V	
MtgMgr			Meeting Manager ?
RMSServer (AMX remote mgmt)		V	
MtHood (Tape)	S2.3	P	>Turn off Tape drive unit too! >For startup, turn Tape drive on 1st
DocImg		V	
K2Verity		V	
NetMon		V	
Intranet		V	Linux
Students		V	
DFServer2		V	
Admin-1		V	
Admin-2		V	
FundWare		V	
KeyScan		V	
RMS-TDC		V	

RMS-HQ		V	
Altera		V	Must login WS only & leave logged in.
AMX_DS		V	
Calendar		V	
McAfee_WSUS		V	
RET_LIC_SRVR		V	

8.0 Hood River Indian Creek Campus –Startup & Shutdown

Identifying equipment locations.
The main HRICC data center is on the Ground Floor, with a floor plan as follows:





1st Floor Data Center	3rd Floor Data Closet
1.1 HREC Cisco Switch - VOIP Wifi 2 x UPS 1.2 Blank 1.3 Cisco Core Switch - VOIP, 1st floor labs, podiums Cisco Voice Gateway Patch (UPS from 1.1 services this rack) Row 2 (Left to Right) 1.4 KVM 3 x Servers VMWare5 VMWare6 VMWare7 3 x UPS	3.1 HP Lab Switch 3.2 Cisco Switch - VOIP (2nd/3rd Floor) HP 5303xl - Labs, Podiums 3.3 Patch

Overview of Shutdown / Startup Procedures

Shutdown	StartUp
Guest Servers	UPS's
vSphere Services	WAN Switches
Host Servers – physical	LAN Switches
Phone Gateway	Phone Gateway
LAN Switches	Host Servers – physical
WAN Switches	vSphere Services
UPS's	Guest Servers

SHUTDOWN DETAILS

Steps for Downing Servers

Servers are controlled by through our VM virtual infrastructure. The servers are shutdown via one of these methods.

Virtual host access:
Go to the VSphere KVM, select the VSphere Server
LocalAdmin – (See the IP table for login information)
Select the desired server by name
Select the Console Tab
Follow the type of server shutdown procedures

Login to that server (check IP table for Login information)
Click on Start, Shutdown
(If you select Turn Off from VSphere, does it do a windows shutdown (no)???)
Use VSphere client go to console of the VM (Guest Menu Ctrl+Alt+Delete)
Login, Click on Start, Shutdown
Server Shutdown Order: 5-3-10
Zenhrc
HRC-RMS
HRC-DC
HRC1 (Netware)
Use VSphere client to log into VMWare7 (10.2.1.15)
Shutdown HRC vSphere

VMWare Host shutdown order:
Can be shut down via vSphere (10.2.1.150)
VMWare5 (10.2.1.12)
VMWare6 (10.2.1.13)
VMWare7 (10.2.1.15) (recommended individually for shutting down vSphere server here and then the host since vSphere is virtualized)

Netware Servers:
Close any major applications by displaying the application list (Press Alt-Esc), selecting the highest numbered application, then follow any onscreen instructions to Exit or Quit
There will be applications listed that cannot be closed, do not worry about those apps.
When you cannot close anything else,
Get to the console screen by pressing Alt-Esc, and then selecting One
At the console screen type DOWN
Enter Y if prompted that there are open files.

Windows Servers:
Login to the desires server
Click on Start, then select ShutDown

Turn off Shoretel Phone Gateway to The Dalles [Location ….]
Turn off third floor UPS's
Turn off first floor UPS's – This will shutdown the LAN & WAN switches

STARTUP DETAILS

Physically turn ON UPS's
The WAN & LAN switches & phone Gateway will automatically startup
Turn ON Shoretel Gateway to The Dalles [Location ….]

Turn ON the Virtual Host server(s):
Vmware5
Vmware6
Vmware7

Virtual host access:
Go to the vSphere KVM, select the vSphere Server
[redacted]– (See the IP table for login information)
Select the desired server by name and select to turn it ON
Server startup order:
Using the vSphere Client, directly connect to VMWare7 (10.2.1.15) username: root p: (see ip table) (recommended since vSphere is virtualized)
Rt. Click on the HR-vSphere guest VM and select power "on"
Wait about 5 mins. to let vSphere server fully boot
Using the VSphere Client, connect to Hood River vSphere (10.2.1.150)
HRC1 – power on
HRC-DC – power on
HRC-RMS – power on
Zenhrc – power on

Login to that server (check IP table for Login information) to verify it is running correctly.
Netware Servers:
Once turned on via the vSphere, view the server console from the vSphere Console option to verify the server is up and running correctly, alternatively you can use ADREM.

9.0 DISASTER RECOVERY

This section differs from the mid-disaster, in that it describes procedures for after an event.

5.1 Tape Restore

5.2 Snapshot Restore

5.3 VM Guest recovery

5.4 Access to the SAN disaster recovery unit

5.5 Any disaster that renders the Data Center inoperable & inaccessible, but the rest of the College intact.

10.0 DOCUMENT MODIFICATION LOG

Modifications made to this document.

DATE	WHO	WHAT
7/19/13	WSB	Added information on the newly implemented off-site backup system CrashPlanPro
5/8/13	WSB	RMS SQL backup strategy and copies of batch files added Archive backup schedule added – full only
5/6/13	WSB	RMS password & vendor phone number
07/15/11	WSB	Added a table for server startup, to be used instead of reverse shutdown order. Done due to when shutting down, key servers may be shutdown first, whereas when starting they may be restarted first. Ie: priority in shutdown is different than priority in startup.
4/02/12	AG	Updated contact lists. Updated server list and priority. Updated index.
11/22/17	AG	Updating most of the document to reflect changes of systems and contacts