ECN Data Center
Configuration and Operations

June 22, 20

Introduction

This document describes ECN data center main IT systems together with system configuration, management interface access and regular maintenance tasks.

This document is intended to be a living document in which ECN IT staff collects configuration information necessary for system maintenance and to collect description of tasks to be performed.

Configuration, Administration and Operations

This document does not intend to describe every configuration setting, administration and operations parameter and task.

Each system and application has a wide range of configurations and functions ECN system administrators are therefore required to read and refer to the system documentation for the systems and applications that have been implemented. Reference to documentation is provided for each system.

Maintenance Schedule

Daily	
TaskID	Tasks / Description
Check system status	1. Ensure that Firewalls and switches are running. 2. Ensure SAN is running 3. Ensure XenServers are running 4. Ensure VMs are running
Review Logs	5. Check Email status reports (sent to all admins) 6. Check Xenserver system log 7. Check SAN system log 8. Check Bacula backup log 9. Check PHDVirtual log 10. Check ClearOS (Intranet) system logs
Review AntiVirus Logs	1. Check ClearOS (Intranet) anti-virus logs. 2. Check Cisco ASA logs
Document Errors/Incidents	1. Document all errors and incidents in problem log.
Review Intrusion Logs	1. Review Fortinet firewall logs for intrusion attempts. 2. Review Cisco ASA logs for intrusion attempts 3. Review ClearOS (intranet) for intrusion attempts.
Weekly	
Clean Virus Infections	1. Clean any workstation infected 2. Remove any infected files
Log storage usage	1. Log total SAN usage (Data/Clones/Snapshots) 2. Log Bacula server disk usage 3. Log Management server disk usage 4. Log email disk space usage (ClearOS) 5. Log Opendedup disk usage
Review & Log Tape usage	1. Log tape usage by pool (Used/Free)
Clean disk space	When necessary clear old log files (XenServer), old backups (Opendedup/Bacula), Disk clones (Equallogic) and snapshots (CVLA DB).
Monthly	
Update systems	1. Review updates on VLDB server (EnterpriseDB) 2. Update management server 3. Update bacula server 4. Update citrix xenserver 5. Update PHDBackup system 6. Update tools on Mgmt Station
Review Firewall Rules	1. Review Fortinet firewall rules 2. Review Cisco ASA firewall rules

Quarterly	
Swap CVLA backup tapes	1. Run CVLA backup 2. Remove CVLA tapes 3. Replace with old off-site tapes or add tapes 4. Erase tapes 5. Add tapes to CVLA backup pool 6. Run CVLA backup
Review tape usage	1. Review tape usage by pool 2. Prune and purge tapes as necessary
Yearly	
Plan storage	Plan data cleanup and plan for storage expansion
Plan upgrades/replacements	Plan major upgrades and replacements of hardware and software.

System Configuration, Administration and Maintenance

ECN Core Network	30-Jun-2012

Description

The Core Network provides connectivity throughout the datacenter and to Internet and user LAN segments.

The core network is divided into a number of VLANs separating traffic between security zones using both VLANs and IP address ranged:

Internet->Core network	VLAN600	10.0.6.0/24
User LAN	VLAN500	10.0.5.0/24
CVLA LAN	VLAN400 (Not used currently)	
Server LAN	VLAN300	10.0.3.0/24
Management LAN	VLAN200	10.0.2.0/24
Storage LAN	VLAN100	10.0.1.0/24

Notes/Comments

The current setup provides only minimal redundancy in network connections. To provide full redundancy additional switches are needed.

Documentation

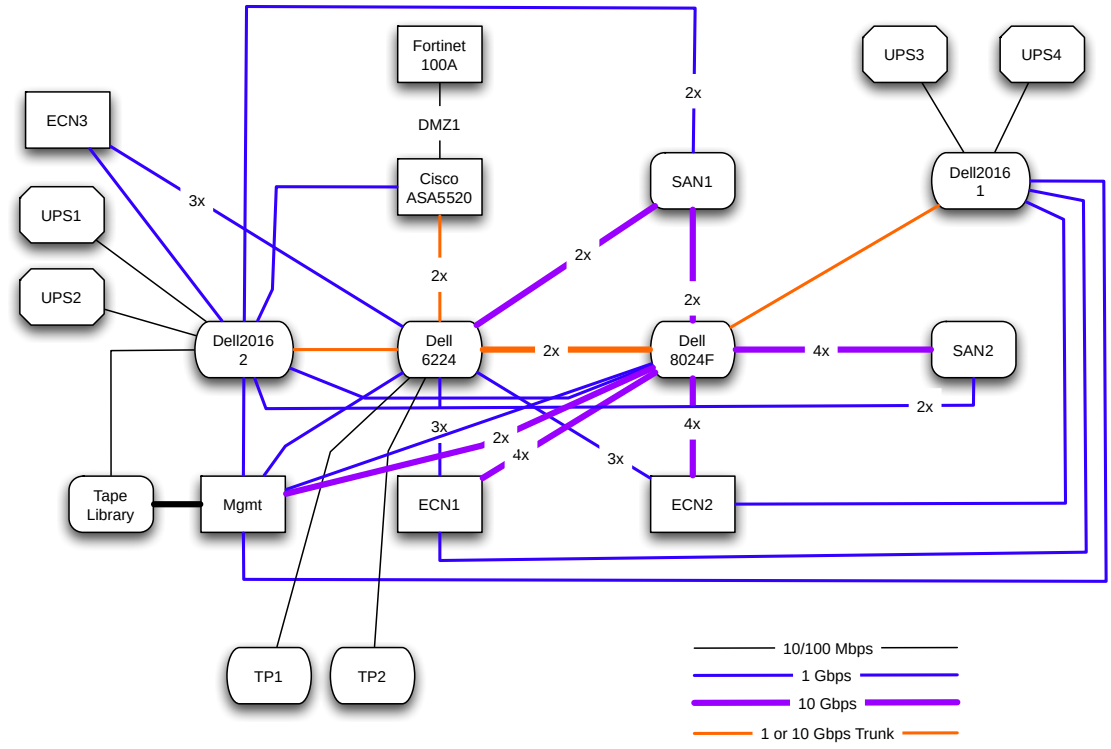
Fortinet: http://docs.fortinet.com/fgt30.html
Cisco ASA 5520:
http://www.cisco.com/en/US/products/ps6120/tsd_products_support_series_home.html
Dell PowerConnect 6224:
http://support.dell.com/support/edocs/network/pc62xx/en/index.htm
Dell PowerConnect 8024F:
http://support.dell.com/support/edocs/network/pc80xx/en/index.htm
Dell PowerConnect 2816:
http://support.dell.com/support/edocs/network/pc28xx/en/index.htm
Citrix DVSC:
http://docs.vmd.citrix.com/XenServer/6.0.0/1.0/en_gb/dvs_controller.html

Host / System / Hardware

Description / Name	Model	IP Addresses	
Border Firewall	Fortinet-100A	External DMZ1	116.90.236.203 10.0.6.2
Internal Firewall Router	Cisco ASA5520	GE 0/0,0/1 GE 0/3 Mgmt 0/0 Trunk: Vlan0.100 Vlan0.300	LAG 1 trunk 10.0.6.1 10.0.2.1 10.0.1.1 10.0.3.1

		Vlan0.400 Vlan0.500	10.0.4.1 10.0.5.254
Core switch 1Gb	Dell PowerConnect 6224 w/ 4x10Gb	Vlan100 Vlan200 Vlan300 Vlan400 Vlan500	10.0.1.2 10.0.2.2 10.0.3.2 10.0.4.2 10.0.5.2
Core switch 10Gb	Dell PowerConnect 8024F	Vlan100 Vlan200 Vlan300 Vlan400 Vlan500	10.0.1.3 10.0.2.3 10.0.3.3 10.0.4.3 10.0.5.3
Management Switch 1	Dell PowerConnect 2816	Vlan200	10.0.2.4
Management Switch 2	Dell PowerConnect 2816	Vlan200	10.0.2.5
Distributed vSwitch	Citrix DVSC	-	10.0.2.32

Network diagram



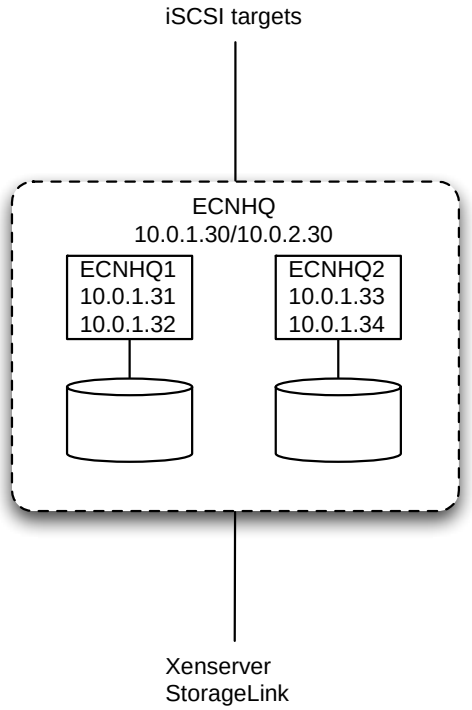
Management Interfaces		
Fortinet	http://10.0.6.2	admin/P@ssw0rd
Cisco	http://10.0.2.1 use ADSM on Management station	--/electi0n
Dell Switches	http://10.0.2.2 http://10.0.2.3 http://10.0.2.4 http://10.0.2.5	admin/electi0n
Citrix DVSC	https://10.0.2.32	admin/electi0n
Management / Maintenance Tasks		
Check firewall logs	Use ADSM to review firewall logs noting intrusion attempts, outages and errors.	
Backup/Update configuration	Ensure that updated configuration files are archived on Bacula server (nfs:10.0.2.51/opt/share/local_backup_data/config/[host])	
Update firmware	Update firmware as directed by vendor.	

ECN SAN	30-Jun-2012
Description	
The SAN provides iSCSI storage for all servers. Storage services are provided via straight iSCSI or via Equallogic storage integration and Equallogic Host Integration Tools.).	
Notes/Comments	
Current storage capacity is 20TB using two Equallogic PS6010 configured as a group.	
Documentation	
See Dell supplied documentation and CD Electronic documentation demands an Equallogic/Dell customer login which ECN IT need to apply for.	

Host / System / Hardware

Description / Name	Model	IP Addresses	
ECNHQ/ECNHQ1	Dell Equallogic PS6010	SAN Group IP eth2 (Mgmt) eth0 eth1	10.0.1.30 10.0.2.30 10.0.1.31 10.0.1.32
ECNHQ/ECNHQ2	Dell Equallogic PS6010	SAN Group IP eth0 eth1	10.0.1.30 10.0.1.33 10.0.1.34

System diagram



Management Interfaces		
Equallogic	http://10.0.2.30 use Equallogic Group Manager on Management station	grpadmin/electi0n
Management / Maintenance Tasks		
Check system logs	Use Equallogic Group Manager to review system log..	
Backup/Update configuration	Ensure that updated configuration files are archived on management server (nfs:10.0.2.50/opt/bacula/local_backup_data/)	
Update firmware	Update firmware as directed by vendor.	
Monitor space usage	Monitor and document data growth and usage in Excel sheet.	

ECN Virtualization Platform	30-Jun-2012

Description

The virtualization platform provides computing, storage and networking resources to all virtual machines.

Notes/Comments

Two hosts are currently in use. ECN3 is intended to be used in secondary location.

ECN1 & ECN2 are configured as members of ECNHQ pool. ECN1 is pool master.

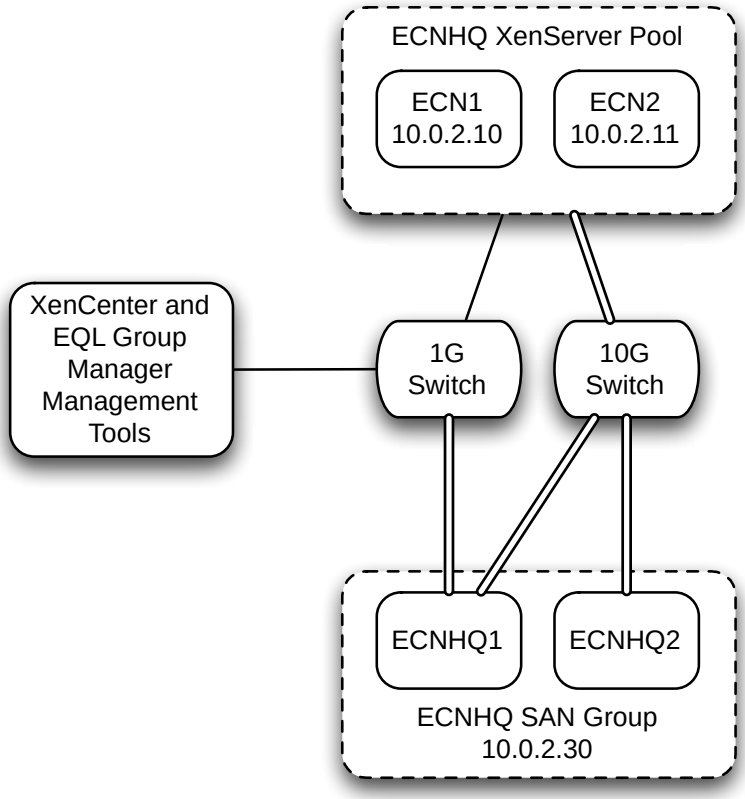
Documentation

Citrix Xenserver 6: http://docs.vmd.citrix.com/XenServer/6.0.0/1.0/en_gb/

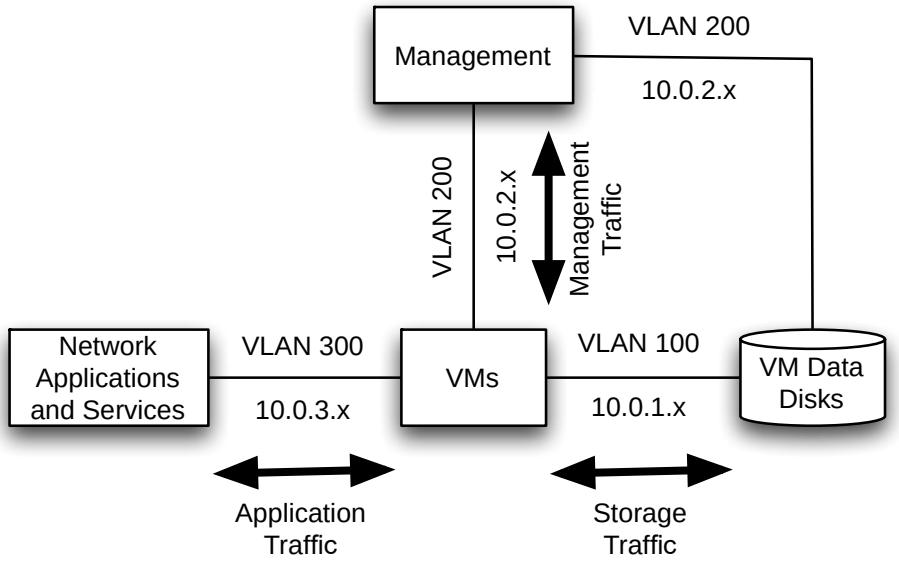
Host / System / Hardware

Description / Name	Model	IP Addresses	
ECN1, ECN2	Dell	Eth4 (Mgmt) Eth6 (SAN) Eth7 (Servers) Eth8 (LAN)	10.0.2.10,10.0.2.11 10.0.1.10,10.0.1.11
ECN3 – not configured	Dell		
License.election.gov.np	Citrix	Eth0	10.0.2.33

System diagram



VLAN diagram



Management Interfaces		
XenCenter	10.0.2.10 use XenCenter on Management station	root/electi0n
Console	Use KVM console to manage hosts directly	--
Citrix License Server	http://10.0.2.33:8082	admin/electi0n

Management / Maintenance Tasks	
Check system logs	Use Xencenter to check system logs
Clear system logs	1. Use “df –h” to check free disk space on “/” 2. If free space is lower than 80% delete old log files in /var/log/
Upgrade software	Update as directed by vendor and on Citrix web site.
Apply patches / updates	Update as directed by vendor and on Citrix web site.
System Startup	1. Power on all switches (6224,8024F, 2x2816, 2xTP) 2. Power on Fortinet and Cisco ASA 3. Power on SAN (ECNHQ1 & ECNHQ2) 4. Power on Tape drive 5. Power on Management Server 6. Power on ECN1 and then ECN2 7. Start DVSC and Citrix License servers 8. Start MMServer and MM Face and Finger servers 9. Start all other servers 10. Check all servers for complete startup without errors. 11. Check that Bacula server is running on Management Server and check that all bacula services are running (DIR, SD, FD) 12. Check Intranet and Internet services.

System Shutdown	1. Shutdown all servers on ECN1 and ECN2. 2. Shutdown ECN1 & ECN2 3. Shut down SAN (ECNHQ1 and then ECNHQ2) 4. Shutdown Management server 5. Shutdown Cisco and Fortinet 6. Shutdown switches, tape drive and UPSs

ECN Backup	30-Jun-2012

Description

The Backup system consists of multi-layered backups of virtual machines (VMs) and data providing both disk-based backup and tape-based backup.

VM Protection – Clones VM disks as Xenserver Virtual Appliance (XVA) and archives to SDFS NFS share 10.0.1.19:/media/sdfs-pool-01/
PHD Virtual – Backs up VMs as Virtual Hard Disk (VHD) images CIFS share on 10.0.2.40:/LatestofEach/
Bacula – Backs up all VHDs and XVAs as well as CVLA Data, Management Server and Bacula server to tape.
Bacula SD - Simply controls the tape library and runs two backup jobs in parallel.
PoolDB Backup – Cron job which backs up weekly image of Xenserver Pool metadata to Management server.
SAN – Keeps clones and snapshots created by VM Protection and HIT.
Tape Library – 69TB capacity tape backup system.
HIT – Tools to automate snapshots on Windows 2008, used to keep daily and weekly snapshots of CVLA DB and to make Oracle CVLA DB backups.

Notes/Comments

Off-site storage of tapes is not yet implemented – 05-Jul-12

Backup run schedule:

17:00	Protection Policy
18:00	PHDVirtual backup
20:00	AutoSnapshot CVLA
21:00	Management, Bacula, CVLA, VHD and XVA backups

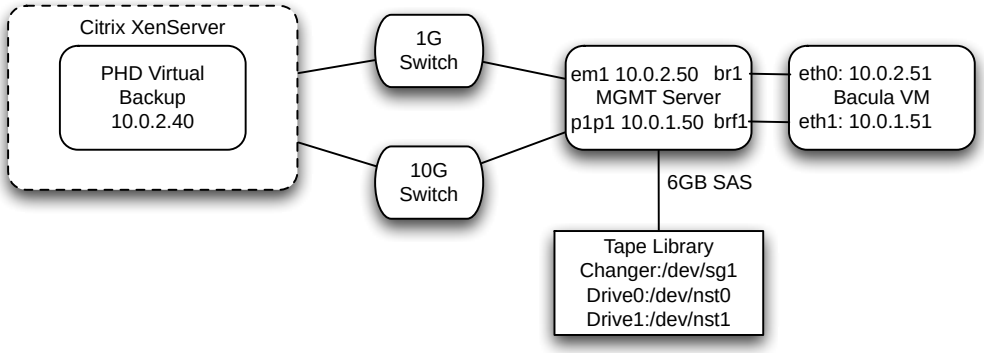
Full backup ~10hrs
Differential backup ~2hrs
Incremental backup ~1hr

Documentation

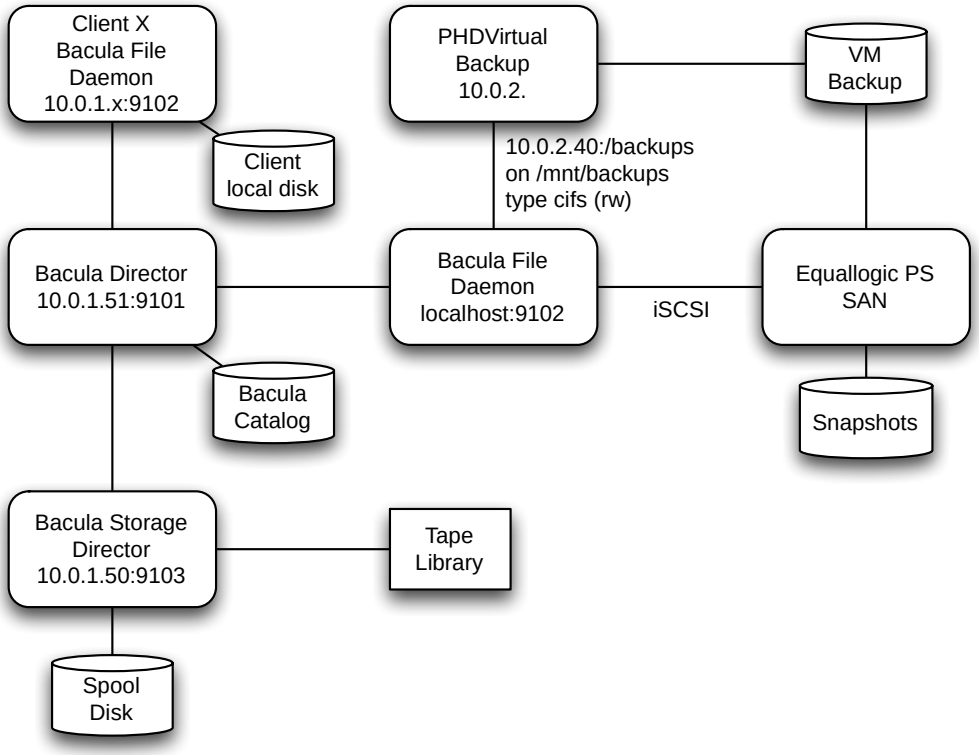
VM Protection: http://docs.vmd.citrix.com/XenServer/6.0.0/1.0/en_gb/
PHDVirtual: http://www.phdvirtual.com/product-documentation-citrix
Bacula: http://www.bacula.org/en/?page=documentation
SAN: *Equallogic/Dell support website – need support login registration*
Tape Library: http://support.dell.com/support/edocs/stor-sys/tl2k4k/en/
HIT: *Equallogic/Dell support website – need support login registration*

Host / System / Hardware			
Description / Name	Model	IP Addresses	
VM Protection	Citrix Xenserver	--	--
PHD Virtual Backup (PHDVBA)	PHDVBA 5.2.4	Eth0 (Mgmt) Eth1 (SAN)	10.0.2.40 10.0.1.40
Bacula	Bacula 5.2.10	Eth0 Eth1	10.0.2.51 10.0.1.51
Bacula SD	Bacula SD 5.2.10	Eth1	10.0.1.50
PoolDB Backup	Crontab	--	10.0.2.51
SAN	Equallogic PS6010	Eth2	10.0.2.30
Tape Library	DELL TL2000	Eth0	10.0.2.60
Dell Host Integration Tools (HIT)	V1.1		10.0.3.13

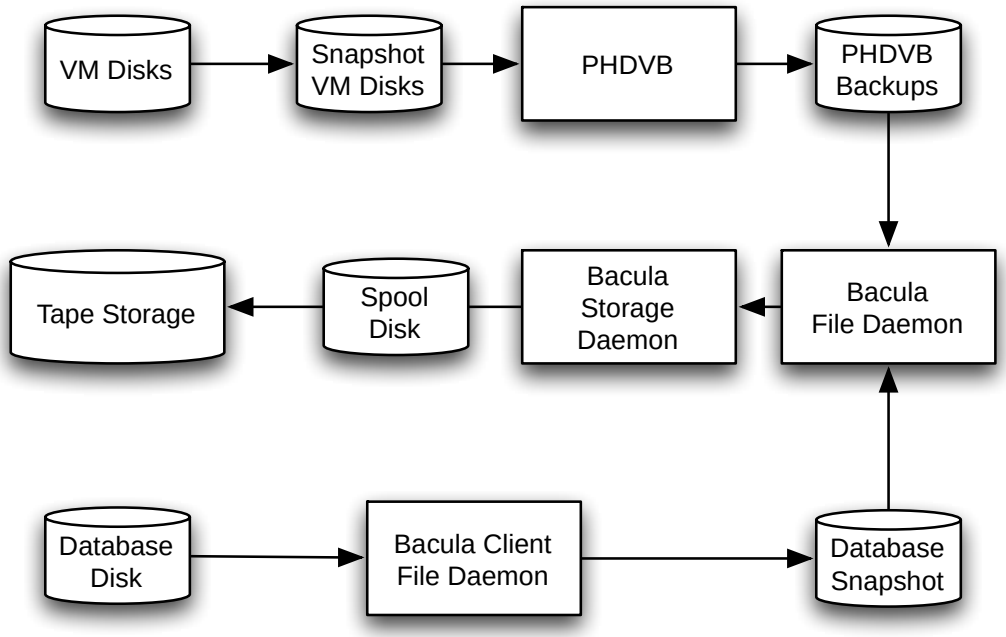
System diagram



Backup application diagram

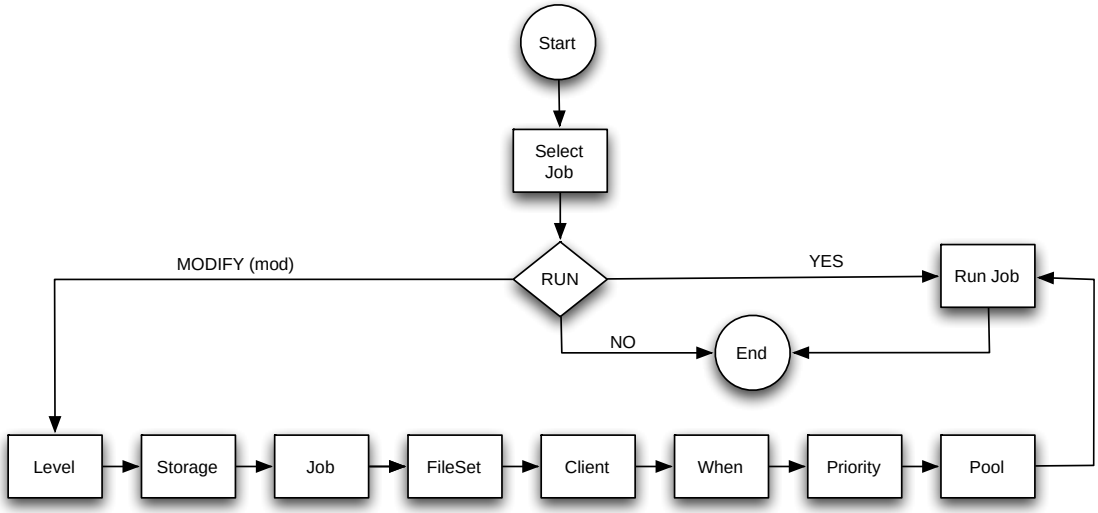


Backup flow diagram



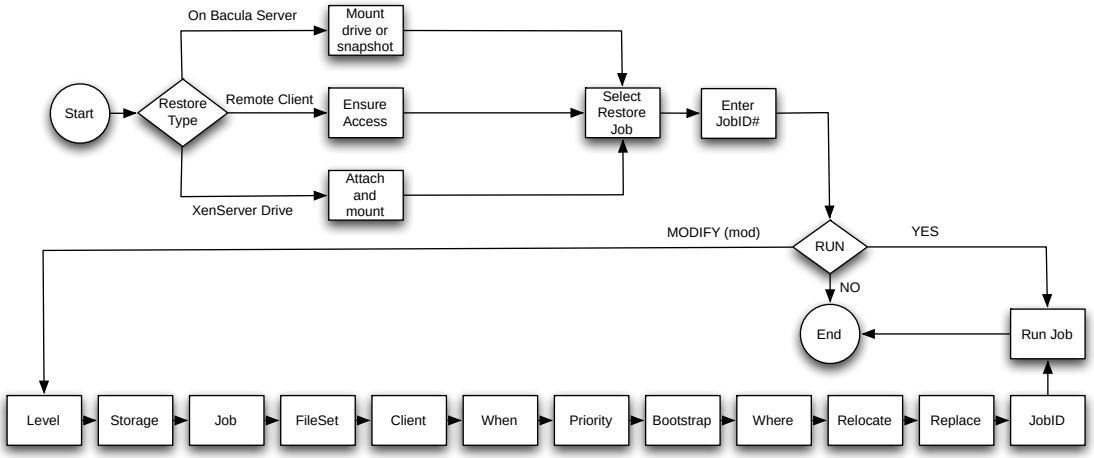
Management Interfaces		
VM Protection Policy	Pool | VM Protection menu in XenCenter	--
PHD Virtual Backup	10.0.2.10 use PHD Virtual Backup Console or XenCenter on Management station	root/electi0n
Bacula & Bacula SD	On Bacula server console use BAT from Application Menu or bconsole on command line.	--
SAN	See ECN SAN	
Tape Library	Web management via http://10.0.2.60	admin/secure
HIT – Auto-Snapshot Manger	Use Auto-Snapshot Manager on CVLA DB server (10.0.2.13)	--
Management / Maintenance Tasks		
Check Job results	Ensure successful backups checking emails to admins and BAT. Re-run jobs if necessary.	
Monitor tape use	Use BAT to check tape use in each backup pool	
Rotate tapes	Rotate CVLA DB backup off-site tapes every 3 months	
Update Bacula	Regularly run “yum –y update” on Bacula server and Management server to update/upgrade. Note that Bacula Director, Bacula File Daemon, Bacula Storage Daemon on Bacula server and Bacula File Deamon and Bacula Storage Daemon needs to be restrted after upgrade. Use “service bacula-fd restart; service bacula-sd restart; service bacula-dir restart” and “service bacula-fd restart;bacula-sd restart” on respective server after update.	
Check Snapshot status	Use AutoSnapshot Manager (on 10.0.2.13 – CVLA DB)and/or SAN management interface to check for errors and status of snapshots.	

Backup job run process



Level - Select Full, Differential, Incremental level - usually Full for custom jobs
Storage - File, TL2000, select TL2000 for tape
Job - Change job/reselect job
FileSet - Select fileset to be backed up
Client - Select client to perform backup - normally not changed
When - Elect time to perform backup
Priority - select priority for the job, normally 10
Pool - Select tape pool to be used for backup - normally Monthly (Full)

Restore job process



Level - Can't be changed
Storage - Select TL2000 to restore from tape
Job - Change job
FileSet - Select file set to restore
Client - Select client to perform restore
When - Select when to restore
Priority - Select priority, normal 10
Bootstrap - Select bootstrap file if available
Where - Select prefix for restore if any
Relocate - Modify file path/prefix for restore
Replace - Replace files if exist?
JobID - Modify JobID #

ECN Management Server	30-Jun-2012

Description

The Management server provide a wide range of services supporting the other systems and services in ECN's network.

KVM Virtualization – used to run Bacula backup server and other separate management servers.
Xenserver ISO repository – provides NFS share for ISO images (nfs://10.0.2.50/opt/share/iso)
Xenserver HA volume – provides heartbeat volume storage (NFS) for xenserver high-availability (nfs://10.0.2.50/opt/share/ha)
Bacula Storage Daemon – provides connectivity to Tape Library for backups Xenserver (bacula-sd port 9102)
TFTP server – supporting backup of configuration files (/opt/bacula/local_backup_data)
UPS Load Check – Monitor remaining run-time and shutsdown system in case of power failure.
XenServer Pool Database backup – Back up Xenserver Pool Database weekly.

Notes/Comments

MegaMatcher VLM will be installed on this server when available.

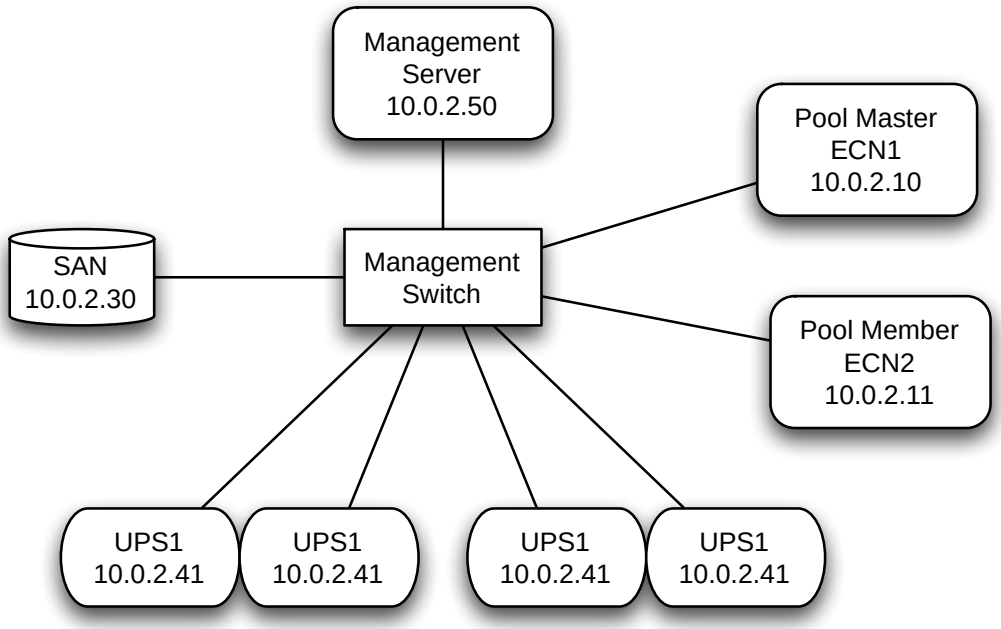
Documentation

CentOS/Red Hat Linux: http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/6/index.html
KVM: http://www.linux-kvm.org/page/Documents
XenServer: *See ECN Virtualization*
Bacula: *See ENC Backup*

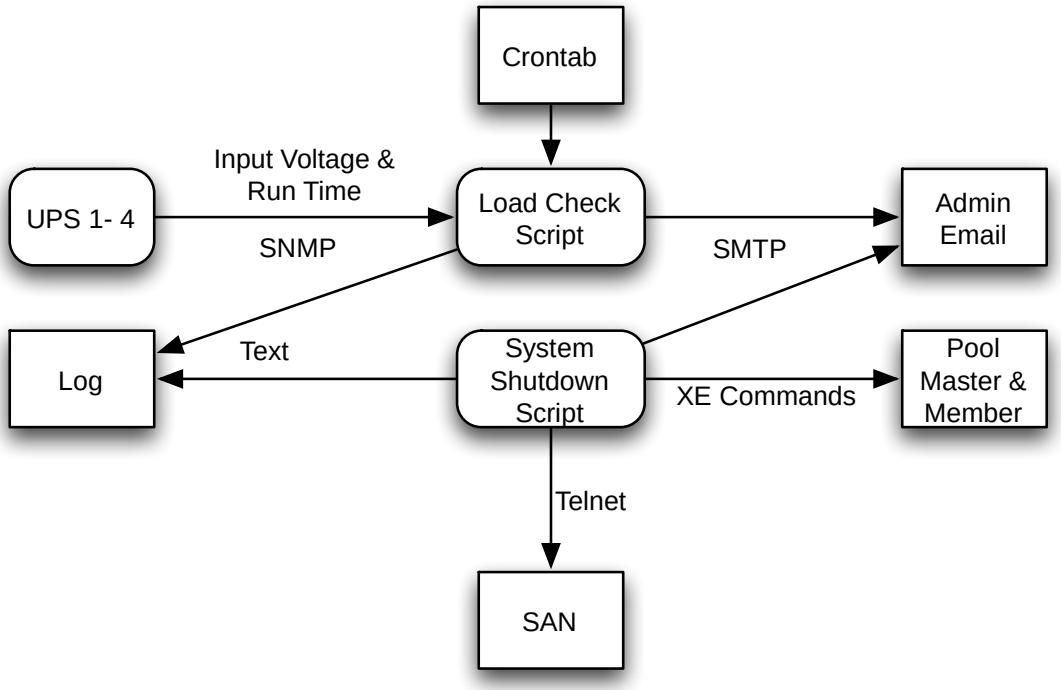
Host / System / Hardware

Description / Name	Model	IP Addresses	
Mgmt.election.gov.np	Dell	Em1 P1p1 Br1 Brf1	To br1 To brf1 10.0.2.50 10.0.1.50
Bacula.election.gov.np	KVM VM	Eth0 Eth1	10.0.2.51 10.0.1.51

System diagram



UPS Load check data flow



Management Interfaces		
Rack Console	Gnome Desktop	ecnadmin/electi0n root/electi0n
SSH	Ssh to 10.0.2.50	root/election
VNC	1. Start vnc server “vncserver :1” on command line. 2. Connect to 10.0.2.50:5901 (or screen 1) with UltraVNC from management station	Password: electi0n
Virtual Manager	From Application menu start Virtual Manager to manage Bacula VM (Gnome Desktop)	
UPS Load Check	Modify ~/scripts/ups_load_check.sh and ~/scripts/ups_system_shutdown.sh scripts	
PoolDB	Modify ~/scripts/xe_pool_dump.sh script	
Services	See service list /etc/ contains configuration files for services, see respective service documentation.	

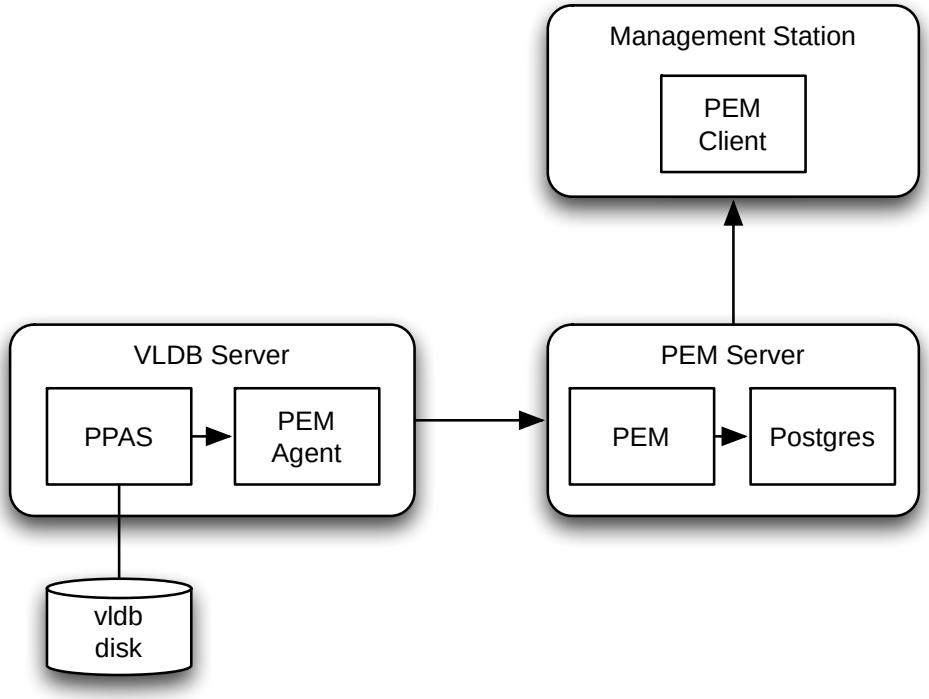
Management / Maintenance Tasks	
Check system logs	Review /var/log/ups_shutdown.log in case of power failures. Review /var/spool/bacula/mtx.log in case of tape errors
Backup/Update configuration	Ensure that updated configuration files are archived in /opt/bacula/local_backup_data/
Update system	Run ‘yum update’ regularly and restart services after update.
Monitor space usage	Monitor and document data growth and usage in Excel sheet.

ECN Database	30-Jun-2012
Description	
ECN Database system consists of EnterpriseDB's PostgresPlus Advanced Server (PPAS) and Postgres Enterprise Manager (PEM).	
Notes/Comments	
PEMServer is only used to collect performance and usage data from PPAS instances.	
Documentation	
EnterpriseDB PostgreSQL Plus Advanced Server & Postgres Enterprise Manager: http://www.enterprisedb.com/products-services-training/products/documentation	

Host / System / Hardware

Description / Name	Model	IP Addresses	
Vldb.election.gov.np	PPAS 9.1	Eth0 Eth1 Eth2	10.0.3.20 10.0.1.20 10.0.2.20
Pem.election.gov.np	PEM 2.1	Eth0	10.0.2.52

System diagram



Service / Management Interfaces		
PostgreSQL DB	CLI psql Port 5444	enterprisedb/electi0n
pgBouncer	Port 6432	
xDB	Application Menu	
Migration Tool Kit (MTK)	CLI	
PEM	Management Station Application	

Management / Maintenance Tasks	
Check system logs	Review /var/log/ups_shutdown.log in case of power failures. Review /var/spool/bacula/mtx.log in case of tape errors
Backup/Update configuration	Ensure that updated configuration files are archived in /opt/bacula/local_backup_data/
Update system	Run ‘yum update’ regularly and restart services after update.
Monitor space usage	Monitor and document data growth and usage in Excel sheet.
Monitor PPAS	Use PEM to review usage and performance

ECN AFIS	30-Jun-2012

Description

The AFIS consist of MegaMatcher Cluster Server with two Node Servers for Face and Fingerprint processing.

Notes/Comments

The AFIS is currently not configured due to delay in obtaining appropriate license management facility (dongle) from vendor.

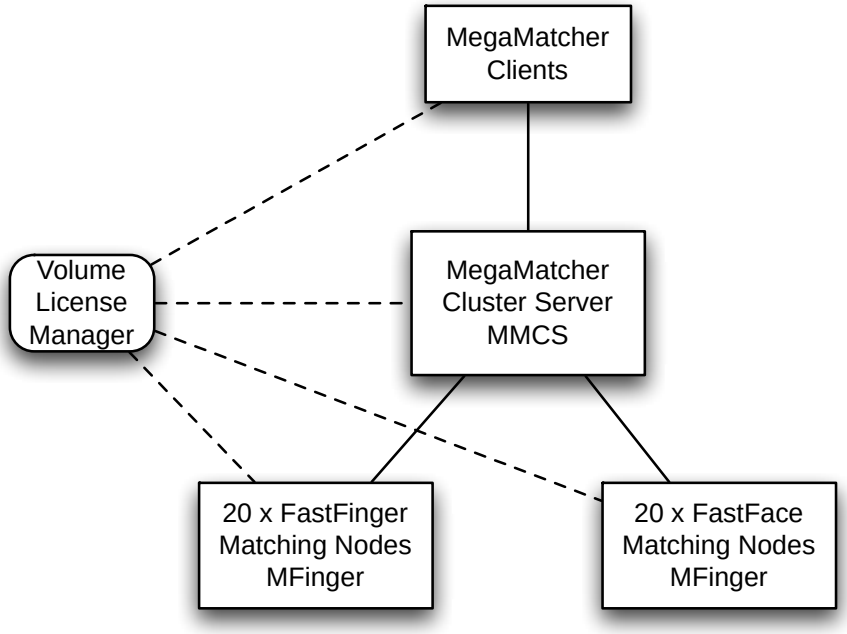
Documentation

MegaMatcher 4 SDK: *Available in SDK download from http://www.neurotechnology.com website.*

Host / System / Hardware

Description / Name	Model	IP Addresses	
Mmcs.election.gov.np	MegaMatcher v4.2	Eth0 Eth1 Eth2	10.0.3.100 10.0.1.100 10.0.2.100
Mmfinger.election.gov.np	FastFinger x 20	Eth0 Eth1	10.0.3.101 10.0.2.101
Mmface.election.gov.np	FastFace x 20	Eth0 Eth1	10.0.3.102 10.0.2.102

System diagram



Management Interfaces		
MegaMatcher	/opt/share/megamatcher	
SSH	Ssh to 10.0.2.100-103	root/electi0n
Management / Maintenance Tasks		

ECN Intranet	30-Jun-2012

Description

The Intranet server provides LAN users with a multitude of services. Primarily the following is provided:
User Database: User DB provides users (and groups) supporting all other functions such as email, and proxy services.
Email: Each user is provided an email account, webmail (SOGo) is available to all.
Internet Proxy: All users traffic passes through the proxy which provides content, anti-virus, anti-malware filtering.

Additionally ClearOS provies the following services:
Firewall
DNS server
Intrusion Prevention

Further services can be provided but are currently unconfigured:
Web Server: External and Internal web servers can be provisioned.
MySQL Database server: Users and external service can be providioned
OpenVPN and PPTP server: Can be enabled (Cisco ASA is preferred as VPN server)
Windows PDC: Can be enabled to provide network logon and shared drives.
Print Server: Printers can be connected to the network and shared among users.

Notes/Comments

15-May-2012: ECN IT have currently connected user LANs through Fortinet Firewall thus effectively disabling all proxy services along with content and anti-virus filtering.

19-July-2012: The system will shortly be upgraded to CentOS 6.3 which will mean changes to webmail and other services. Users will need to be retrained in webmail usage.

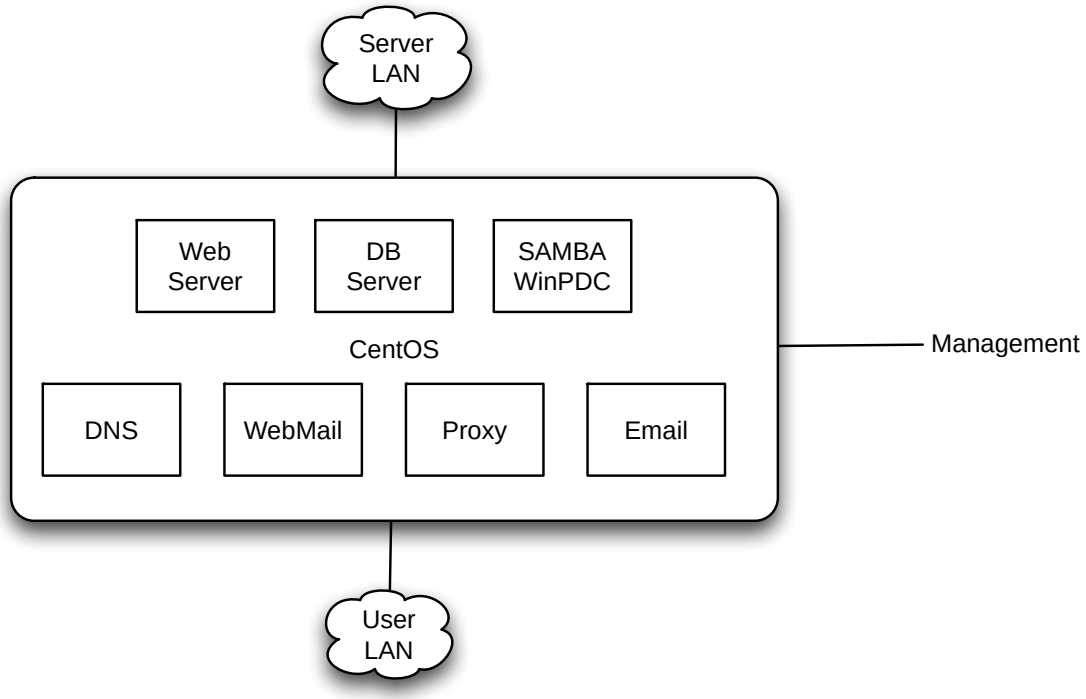
Documentation

ClearOS 5.2: http://www.clearfoundation.com/docs/

Host / System / Hardware

Description / Name	Model	IP Addresses	
Intranet (ClearOS)	CentOS 5.2	Eth0 (External) Eth1 (Internal) Eth2 (Mgmt)	10.0.3.14 10.0.5.10 10.0.2.14

System diagram



Management Interfaces		
ClearOS	https://10.0.3.14:81 https://10.0.2.14:81 https://10.0.5.10:81	root/electi0n

Management / Maintenance Tasks	
Check system logs	Use ClearOS reporting
Update Intrusion Prevention signatures	Use ClearOS reporting, updates are automatically done.
Update Anti-Virus signatures.	Use ClearOS reporting, updates are automatically done
Purge inactive users	Regularly remove deleted users
Update system	Run “yum –y update” regularly to update system components.

Server Specifications and Services

Name	Description	CPU	Cores	RAM (GB)	HDD (GB)
ECN1	XenServer Host	4 x AMD Opteron 6176 2.3GHz	48	256	300
ECN2	XenServer Host	4 x AMD Opteron 6176 2.3GHz	48	256	300
ECN3	XenServer Host	4 x AMD Opteron 6176 2.3GHz	48	256	300
Mgmt	Management Server	Intel Xeon E5620 2.40GHz	4	48	160
Bacula	Backup Server (Bacula)		2	1	8
dvsc	Distributed vSwitch Controller		2	2	16
phdvba	PHD Virtual Backup Server			1	8+1024

intranet	ClearOS Intranet Server		2	2	200
cvla	CVLA application & DB		8	32	30
cvla1	Backup CVLA application & DB		8	32	60
www2	Web Voter List		1	1	8
license	Citrix License Server		1	0.125	
sdfsnas	Opendedup SDFS NAS		4	4	2.5+256
ecnhq	SAN Group				
enchq1	SAN1				
ecnhq2	SAN2				
vldb	EnterpriseDB for new CVLA		8	128	60
pems	Postgres Enterprise Manager		2	2	20
mmcs	MegaMatcher Cluster Server		2	4	20
mmfinger	FastFinger Matcher Nodes		20	80	20
mmface	FastFace Matcher Nodes		20	80	20
webvl	Web Voter List DB		8	32	24+1500
ecnintra	CentOS 6.3 test		2	4	60

Name	Description	IP Management	OS	Patches	Applications	App version	Service Ports
ECN1	XenServer Host	10.0.2.10	XenServer 6.0.2	XS001-005			
ECN2	XenServer Host	10.0.2.11	XenServer 6.0.2	XS001-005			
ECN3	XenServer Host	10.0.2.12					
Mgmt	Management Server	10.0.2.50	CentOS 6.2				22/ssh 69/tftp 123/ntp 9102/bacula-fd 9103/bacula-sd
Bacula	Backup Server (Bacula)	10.0.2.51	CentOS 6.2		Bacula	5.2.6	22/ssh 9101/bacula-dir 9102/bacula-fd 9103/bacula-sd
dvsc	Distributed vSwitch Controller	10.0.2.32	Debian 5.0.6		Citrix DVSC		
phdvba	PHD Virtual Backup Server	10.0.2.40	Ubuntu 10.04 LTS		PHDVB	5.4	

intranet	ClearOS Intranet Server	10.0.2.14	CentOS 5.4		ClearOS	5	21/ftp 22/ssh 25/smtp 80/http 81/mgmt 110/pop 143/imap 993/imaps 995/pops 1194/openvpn 3306/mysql 8080/proxy 10000/webmin
cvla	CVLA application & DB	10.0.2.13	Win2k8R2		Oracle	10g R2	
cvla1	Backup CVLA application & DB	10.0.2.17	Win2k8R2		Oracle	10g R2	
www2	Web Voter List	10.0.2.35	CentOS 6.2		Apache	2	80/http
license	Citrix License Server	10.0.2.33	CentOS 5.4		Citrix LicSvr		27000/license
sdfsnas	Opendedup SDFS NAS	10.0.2.19	CentOS 6.2		SDFS	1.1.15	
ecnhq	SAN Group	10.0.2.30					
enchq1	SAN1						
ecnhq2	SAN2						
vldb	EnterpriseDB for new CVLA	10.0.2.20	CentOS 6.2		EnterpriseDB	9.1	5444/ppas
pems	Postgres Enterprise Manager	10.0.2.52	CentOS 6.2		PEM	2.1	
mmcs	MegaMatcher Cluster Server	10.0.2.100	CentOS 6.2		MegaMatcher	4.3	
mmfinger	FastFinger Matcher Nodes	10.0.2.101	CentOS 6.2		MegaMatcher	4.3	
mmface	FastFace Matcher Nodes	10.0.2.102	CentOS 6.2		MegaMatcher	4.3	
webvl	Web Voter List DB	10.0.2.18	Win2k8R2		Oracle	10g R2	
ecnintra	CentOS 6.3 test	DHCP	CentOS 6.2		CentOS	6.3	see intranet

Switch Port Assignment

Dell 8024F	Type	BOND	IP/VLAN	Dell 6224	Type	BOND	IP/VLAN
1	Storage 1 F0			1	Trunk Cisco G0		
2	Storage 1 F2			2	Trunk Cisco G1		
3	Storage 2 F0			3	TPSwitch 1		VLAN300
4	Storage 2 F1			4	TP Switch 2		VLAN300
5	Storage 2 F2			5	Server 1 G0	SAN Bond	VLAN100
6	Storage 2 F3			6	Server 1 G1	LAN	VLAN300
7	Server 1 F2	SAN Bond	VLAN100	7	Server 1 G2	CVLA	VLAN400
8	Server 1 F3	LAN	VLAN300	8	Server 2 G0	SAN Bond	VLAN100
9	Server 1 F0	CVLA	VLAN400	9	Server 2 G1	LAN	VLAN300
10	Server 2 F2	SAN Bond	VLAN100	10	Server 2 G2	CVLA	VLAN400
11	Server 2 F3	LAN	VLAN300	11	Server 3 G0		
12	Server 2 F0	CVLA	VLAN400	12	Server 3 G1		
13	Server 3 F2			13	Server 3 G2		
14	Server 3 F3			14	Mgmt Server G0		VLAN200
15	Server 3 F0			15			
16	Server 3 F1			16			
17	Mgmt Server F0		VLAN100	17			
18	Mgmt Server F1			18			
19	Trunk to 6224 switch		Trunk	19			
20	Trunk to 6224 switch		Trunk	20	Trunk 2816-2		VLAN200
21	Mgmt Server G1		VLAN200	21			
22	Trunk 2816-1		VLAN200	22			
23	Server 1 F1			23			
24	Server 2 F1			24			VLAN200
				Uplink 1	Storage 1 F1		
				Uplink 2	Storage 1 F3		
				Uplink 3	Trunk to 8024 switch		
				Uplink 4	Trunk to 8024 switch		

Dell 2816-1	Type	IP/VLAN	Dell 2816-2	Type	IP/VLAN
1	Server 1 G3	VLAN200	1	Mgmt Server G3	VLAN200
2	Server 2 G3	VLAN200	2	Tape Mgmt port	10.0.2.60/VLAN200
3			3	Storage 1 Mgmt G0	moved
4	Mgmt Server G2	VLAN200	4	Storage 1 Mgmt G1	moved
5			5	Cisco FE port	VLAN200
6			6	Storage 2 G0	
7			7	Storage 2 G1	
8			8	Server 3 G3	
9			9	Dell 8024 OOB	
10	UPS 3	VLAN200	10	UPS 1	VLAN200
11	UPS 4	VLAN200	11	UPS 2	VLAN200
12			12		
13			13		
14	Trunk 2816-1	Not connected	14	Trunk 2816-2	not connected
15	Trunk 2816-1	Not connected	15	Trunk 2816-2	not connected
16	Trunk 8024	VLAN200	16	Trunk 6224	VLAN200
Cisco ASA5520					
0	Trunk 6224				
1	Trunk 6224				
2	ISP	DMZ1			
3	GIDC	Not connected			
Management	Dell 2816-2				

Server 1	SAN Bond	Server 1 F0		**Server 2**	SAN Bond	Server 2 F0	
		Server 1 G0				Server 2 G0	
	LAN	Server 1 F1			LAN	Server 2 F1	
		Server 1 G1				Server 2 G1	
	CVLA	Server 1 F2			CVLA	Server 2 F2	
		Server 1 G2				Server 2 G2	
	Management	Server 1 G3	10.0.2.10		Management	Server 2 G3	10.0.2.11
Storage 1	Group	ECNHQ	10.0.1.30				
	Link 1		10.0.1.31				
	Link 2		10.0.1.32				
	Management		10.0.2.30				
Storage 2	Group		--				
	Link 1		10.0.1.33				
	Link 2		10.0.1.34				
	Management		--				

IP Assignments

SAN			Management			LAN		
10.0.1.0			10.0.2.0			10.0.3.0		
10.0.1.1	Router		10.0.2.1	Router		10.0.3.1	Router	
10.0.1.2			10.0.2.2	6224		10.0.3.2		
10.0.1.3			10.0.2.3	8024F		10.0.3.3		
10.0.1.4			10.0.2.4	Rack1		10.0.3.4		
10.0.1.5			10.0.2.5	Rack2		10.0.3.5		
10.0.1.6			10.0.2.6			10.0.3.6		
10.0.1.7			10.0.2.7			10.0.3.7		
10.0.1.8			10.0.2.8			10.0.3.8		
10.0.1.9			10.0.2.9			10.0.3.9		
10.0.1.10	ECN1	F0	10.0.2.10	ECN1	G3	10.0.3.10		
10.0.1.11	ECN2	F0	10.0.2.11	ECN2	G3	10.0.3.11		
10.0.1.12	ECN3	F0	10.0.2.12	ECN3	G3	10.0.3.12	DDK-Old	
10.0.1.13	CVLA1		10.0.2.13	CVLA1 DB	Win2k8	10.0.3.13	CVLA1 DB	Win2k8
10.0.1.14			10.0.2.14	Intranet	ClearOS	10.0.3.14	Intranet	ClearOS
10.0.1.15			10.0.2.15			10.0.3.15		
10.0.1.16			10.0.2.16			10.0.3.16		
10.0.1.17	CVLA Backup		10.0.2.17	CVLA Backup		10.0.3.17	CVLA Backup	
10.0.1.18	WebDB		10.0.2.18	WebDB		10.0.3.18	WebDB	
10.0.1.19	SDFS		10.0.2.19	SDFS Backup	CentOS 6.1	10.0.3.19		
10.0.1.20	VLDB		10.0.2.20	VLDB		10.0.3.20	VLDB	
10.0.1.21			10.0.2.21			10.0.3.21		
10.0.1.22			10.0.2.22			10.0.3.22		
10.0.1.23			10.0.2.23			10.0.3.23		
10.0.1.24			10.0.2.24			10.0.3.24		
10.0.1.25	ECNINTRA		10.0.2.25	ECNINTRA		10.0.3.25	ECNINTRA	
10.0.1.26			10.0.2.26			10.0.3.26		
10.0.1.27			10.0.2.27			10.0.3.27		
10.0.1.28			10.0.2.28			10.0.3.28		
10.0.1.29			10.0.2.29			10.0.3.29		
10.0.1.30	SAN - Group		10.0.2.30	SAN Mgmt		10.0.3.30		

10.0.1.31	SAN1 - p0		10.0.2.31			10.0.3.31		
10.0.1.32	SAN1 - p1		10.0.2.32	vSwitch Ctrl		10.0.3.32		
10.0.1.33	SAN2 - p0		10.0.2.33	License Svr		10.0.3.33		
10.0.1.34	SAN2 - p1		10.0.2.34			10.0.3.34		
10.0.1.35			10.0.2.35	WebVL		10.0.3.35	WebVL	
10.0.1.36			10.0.2.36			10.0.3.36		
10.0.1.37			10.0.2.37			10.0.3.37		
10.0.1.38			10.0.2.38			10.0.3.38		
10.0.1.39			10.0.2.39			10.0.3.39		
10.0.1.40			10.0.2.40	PHDBackup		10.0.3.40		
10.0.1.41			10.0.2.41	APC1		10.0.3.41		
10.0.1.42			10.0.2.42	APC2		10.0.3.42		
10.0.1.43			10.0.2.43	APC3		10.0.3.43		
10.0.1.44			10.0.2.44	APC4		10.0.3.44		
10.0.1.45			10.0.2.45			10.0.3.45		
10.0.1.46			10.0.2.46			10.0.3.46		
10.0.1.47			10.0.2.47			10.0.3.47		
10.0.1.48			10.0.2.48			10.0.3.48		
10.0.1.49			10.0.2.49			10.0.3.49		
10.0.1.50	Mgmt		10.0.2.50	Mgmt		10.0.3.50		
10.0.1.51			10.0.2.51	Bacula Backup		10.0.3.51		
10.0.1.52			10.0.2.52	PEMS		10.0.3.52		
10.0.1.53			10.0.2.53			10.0.3.53		
10.0.1.54			10.0.2.54			10.0.3.54		
10.0.1.55			10.0.2.55			10.0.3.55		
10.0.1.56			10.0.2.56			10.0.3.56		
10.0.1.57			10.0.2.57			10.0.3.57		
10.0.1.58			10.0.2.58			10.0.3.58		
10.0.1.59			10.0.2.59			10.0.3.59		
10.0.1.60			10.0.2.60	TL2000		10.0.3.60		
10.0.1.100	MMCS		10.0.2.100	MMCS		10.0.3.100	MMCS	
10.0.1.101	MFINGER		10.0.2.101	MFINGER		10.0.3.101		
10.0.1.102	MFACE		10.0.2.102	MFACE		10.0.3.102		

UserLAN			GW LAN	
10.0.5.1			10.0.6.1	Router
10.0.5.2	6224		10.0.6.2	Fortigate DMZ1
10.0.5.3	8024F			
10.0.5.4				
10.0.5.5				
10.0.5.6				
10.0.5.7				
10.0.5.8				
10.0.5.9				
10.0.5.10	ClearOS	Users GW		
10.0.5.11				
10.0.5.12				
10.0.5.13				
10.0.5.14				
10.0.5.15				
10.0.5.16				
10.0.5.17				
10.0.5.18				
10.0.5.19				
10.0.5.20				
10.0.5.21				
10.0.5.22				
10.0.5.23				
10.0.5.24				
10.0.5.25	ECNINTRA			
10.0.5.26				
10.0.5.27				
10.0.5.28				
10.0.5.29				
10.0.5.30				
10.0.5.31				
10.0.5.32				

10.0.5.33				
10.0.5.34				
10.0.5.35				
10.0.5.36				
10.0.5.37				
10.0.5.38				
10.0.5.39				
10.0.5.40				
10.0.5.41				
10.0.5.42				
10.0.5.43				
10.0.5.44				
10.0.5.45				
10.0.5.46				
10.0.5.47				
10.0.5.48				
10.0.5.49				
10.0.5.50				
10.0.5.51				
10.0.5.52				
10.0.5.53				
10.0.5.54				
10.0.5.55				
10.0.5.56				
10.0.5.57				
10.0.5.58				
10.0.5.59				
10.0.5.60				
10.0.5.61				
10.0.5.61-240	Users			
10.0.2.254	Router			

iSCSI and NFS file systems

Name	Description	External Mounts	Exports
ECN1	XenServer Host		
ECN2	XenServer Host		
ECN3	XenServer Host		
Mgmt	Management Server		NFS:/opt/share/iso NFS:/opt/share/ha
Bacula	Backup Server (Bacula)	10.0.1.40->/mnt/backups 10.0.1.19->/mnt/backupsXVA	
dvsc	Distributed vSwitch Controller		
phdvba	PHD Virtual Backup Server		CIFS:10.0.2.40/backups NFS:10.0.2.19/mnt/sdfs
intranet	ClearOS Intranet Server		
cvla	CVLA application & DB	iscsi->10.0.1.30/cvladata	

cvla1	Backup CVLA application & DB	iscsi->10.0.1.30/CVLA-Backup iscsi->10.0.1.30/cvladata32	
www2	Web Voter List		
license	Citrix License Server		
sdfsnas	Opendedup SDFS NAS		/media/sdfs-pool-01
ecnhq	SAN Group		
enchq1	SAN1		
ecnhq2	SAN2		
vldb	EnterpriseDB for new CVLA	iscsi->10.0.1.30/vldb	
pems	Postgres Enterprise Manager		
mmcs	MegaMatcher Cluster Server		
mmfinger	FastFinger Matcher Nodes		
mmface	FastFace Matcher Nodes		
webvl	Web Voter List DB		
ecnintra	CentOS 6.3 test		

Miscellaneous Administration Tasks

Connecting to an iSCSI disk on Equallogic SAN

Linux – open-iscsi

Command Line Tool: iscsiadm
Daemon service: /etc/init.d/iscsid
Configuration file: /etc/iscsi/iscsid.conf

Open-iscsi is used to connect iscsi exposed disks and snapshots on the Equallogic PS6010 SAN.

The tasks consist of:

1. Ensure that iscsi configuration is correct (mainly providing passwords for session and discovery).
2. Discover the available targets on the SAN.
3. Connect to a target.
4. Mount the iSCSI taget on the local file system.
5. Optionally ensure that the drive is connected automatically on boot.
6. Optionally create a file system on the connected iSCSI disk.

Detailed steps:

1. Ensure connectivity to the SAN by pinging the SAN IP:

   ```
   Host#>ping 10.0.1.30
   ```

   If this works continue

2. Ensure that you have configured necessary passwords and enabled CHAP authentication as needed in the /etc/iscsi/iscsid.conf file.
3. Discover the available targets:

   ```
   Host#>iscsiadm -m discovery -t st -p 10.0.1.30
   10.0.1.30:3260,1 iqn.2001-05.com.equallogic:0-
   8a0906-2ce31b209-5862108708f4f1df-management
   10.0.1.30:3260,1 iqn.2001-05.com.equallogic:0-
   8a0906-25a61b209-149999db23d4f1f9-cvladata
   10.0.1.30:3260,1 iqn.2001-05.com.equallogic:0-
   8a0906-7f061b209-465999db2434f221-backup
   ```

   We receive a listing of all available targets. If none of these targets are desired use the Equallogic Group Manager to create and configure the desired target.

4. Connect to the desired target and store it in the target table:

```
Host#>iscsiadm -m node -T iqn.1992-
08.com.netapp:sn.84211978 -p 10.0.1.30 -l
```

The iSCSI drive is now connected and will have been assigned a device id. (Disconnect the drive using the same command replacing *-l* with *-u*)

```
Host#>tail /var/log/messages
Jun  4 00:15:39 mgmt kernel: scsi 5:0:0:0: Direct-
Access     EQLOGIC  100E-00          5.2  PQ: 0
ANSI: 5
Jun  4 00:15:39 mgmt kernel: sd 5:0:0:0: Attached
scsi generic sg6 type 0
Jun  4 00:15:39 mgmt kernel: sd 5:0:0:0: [sdb]
2147512320 512-byte logical blocks: (1.09 TB/1.00
TiB)
Jun  4 00:15:39 mgmt kernel: sd 5:0:0:0: [sdb] Write
Protect is off
Jun  4 00:15:39 mgmt kernel: sd 5:0:0:0: [sdb] Write
cache: disabled, read cache: enabled, doesn't
support DPO or FUA
Jun  4 00:15:39 mgmt kernel: sdb: sdb1
Jun  4 00:15:39 mgmt kernel: sd 5:0:0:0: [sdb]
Attached SCSI disk
Jun  4 00:15:40 mgmt iscsid: Connection1:0 to
[target: iqn.2001-05.com.equallogic:0-8a0906-
2ce31b209-5862108708f4f1df-m$
```

The device id is marked in bold red above. We can also check which iSCSI drives are attached by:

```
Host#>iscsiadm -m session
tcp: [1] 10.0.1.30:3260,1 iqn.2001-
05.com.equallogic:0-8a0906-2ce31b209-
5862108708f4f1df-management
```

5. Mount the iSCSI drive on the local file system:

```
Host#>mount -t ext4 /dev/sdb1 /mnt/
```

The disk is now available on /mnt/

6. If you want the disk attached on each boot you need to ensure that iSCSI daemon is running and is started on boot.

```
Host#>chkconfig iscsid on
Host#>service iscsid start
```

Open-ISCSI daemon will now be started on boot and automatically attach to the target(s) earlier connected.

7. If you want to create a file system on the attached iSCSI disk use:

```
Host#>fdisk /dev/sdb
```

or if disk is larger than 2TB (change label to GPT as DOS only supports max 2TB):

```
Host#>parted /dev/sdb
```

Windows – iSCSI Client

To connect Windows Server 2008 to an iSCSI target, you need to first go to Control Panel and double click on the iSCSI Initiator.

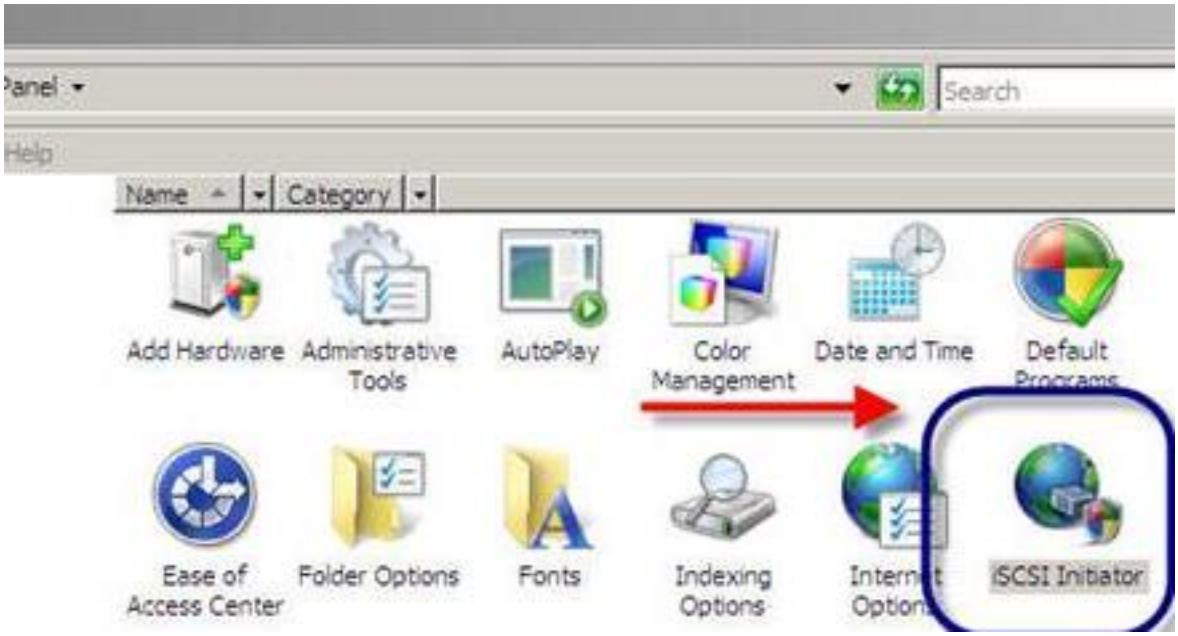


Figure 11: Windows Server 2008 – Launch iSCSI Initiator in Control Panel

Next, you will be prompted to indicate if you want the iSCSI Service to start automatically.

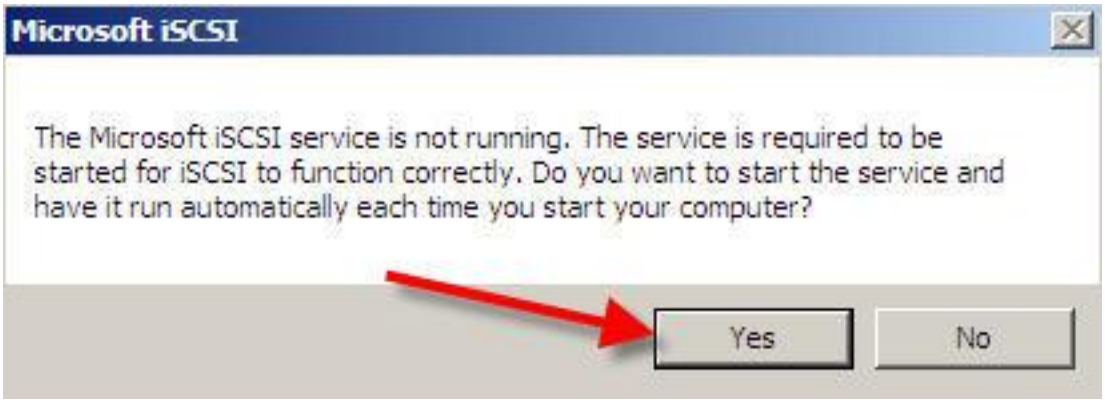


Figure 12: Windows Server 2008 – Launch iSCSI Initiator whenever Win 2008 starts

Then, click **Yes,** that you want iSCSI to be allowed through the Windows Server 2008 Firewall.

Figure 13: Windows Server 2008 – Allow iSCSI through Firewall

When the iSCSI Initiator Properties come up, click on the **Discovery** tab. Click on **Add Portal**.

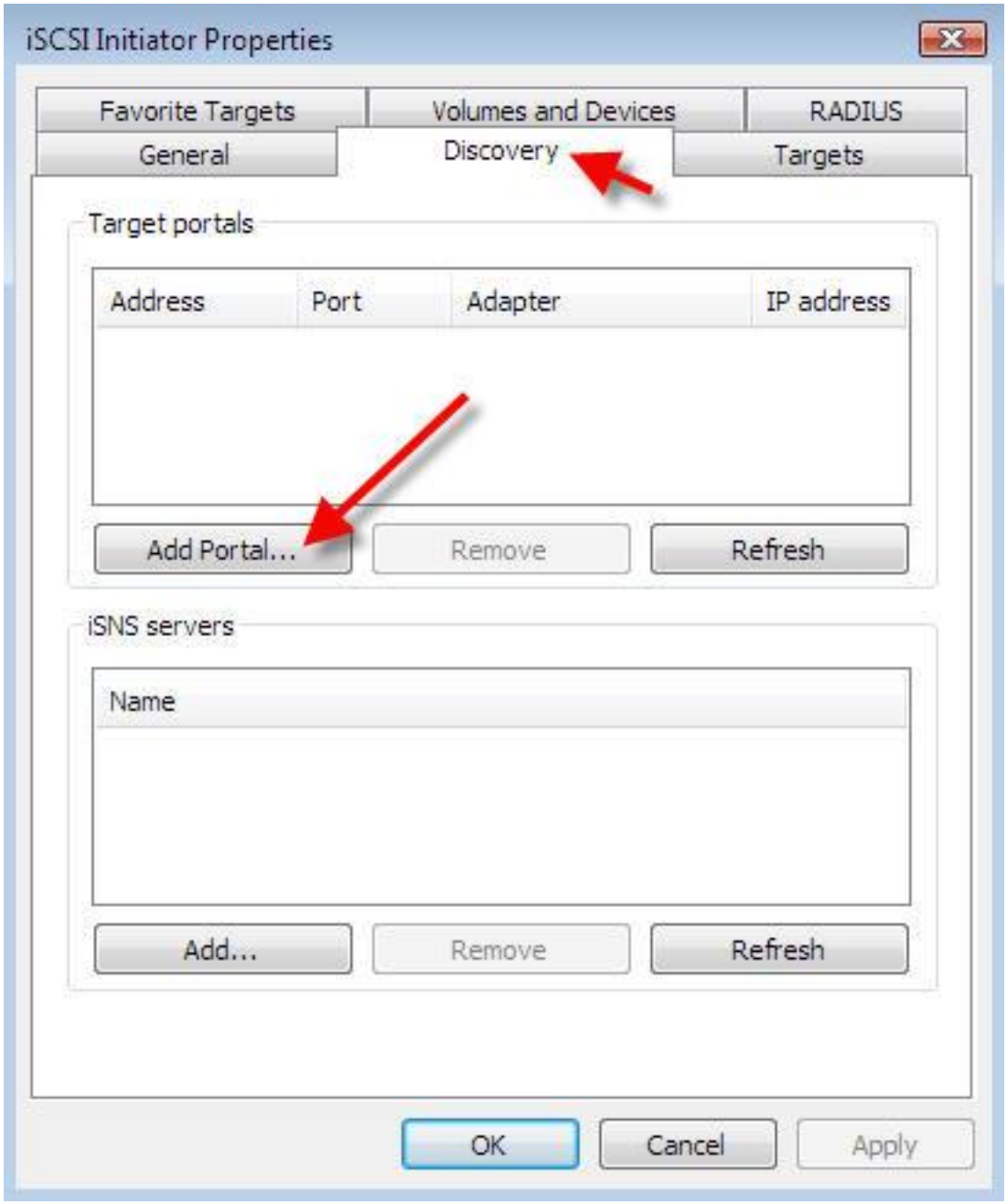


Figure 5: Vista – Add an iSCSI Portal

Enter the IP address (10.0.1.30) or DNS name of the iSCSI server when the **Add Target Portal** window appears, like this:

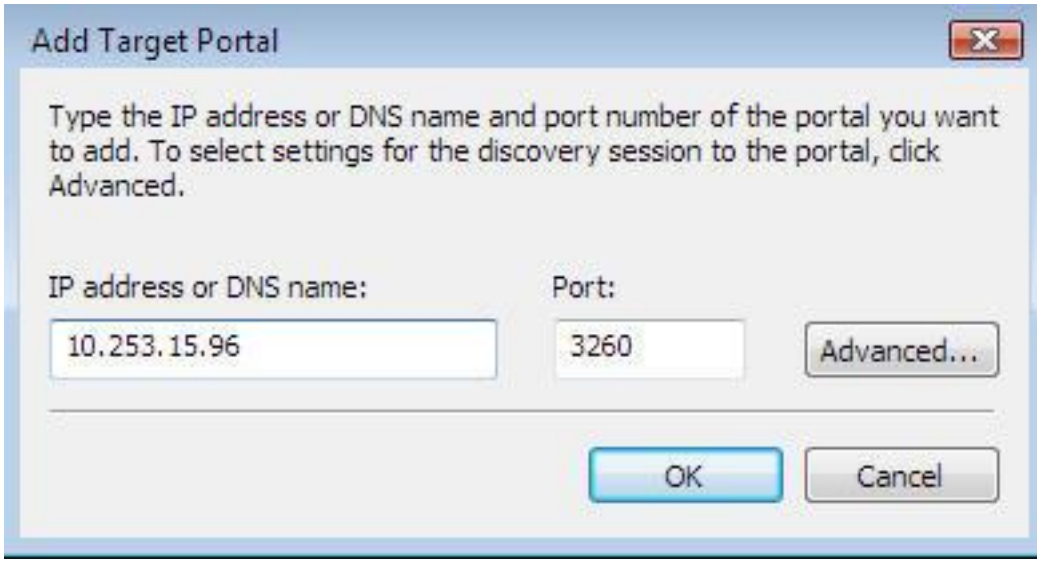


Figure 6: Vista – iSCSI Adding a Target Portal

(the port number of 3260 will already be there as this is the default iSCSI port number).
Click **OK**.
Go to the **Targets** tab and click **Refresh**. You should see the name of your iSCSI Target in the list.
Select your target server and click **Log on**.
Check to **automatically restore this connection when the computer starts** and click **OK.**

Figure 7: Vista – Log on to iSCSI Target

You should now see that you are **Connected.**
Click **OK** and close out the iSCSI Initiator Properties.
Because, in our case, this iSCSI volume was already initialized on our Windows Vista machine, we don't need to go into the Disk Manager. If, however, this is a new iSCSI volume that has never been connected to from another Windows machine, you will

have to use your Windows 2008 Server's Disk Manager to initialize the volume, format it, and assign a drive letter.
As this is already done in our case, just go into my computer and you can see the new disk volume.

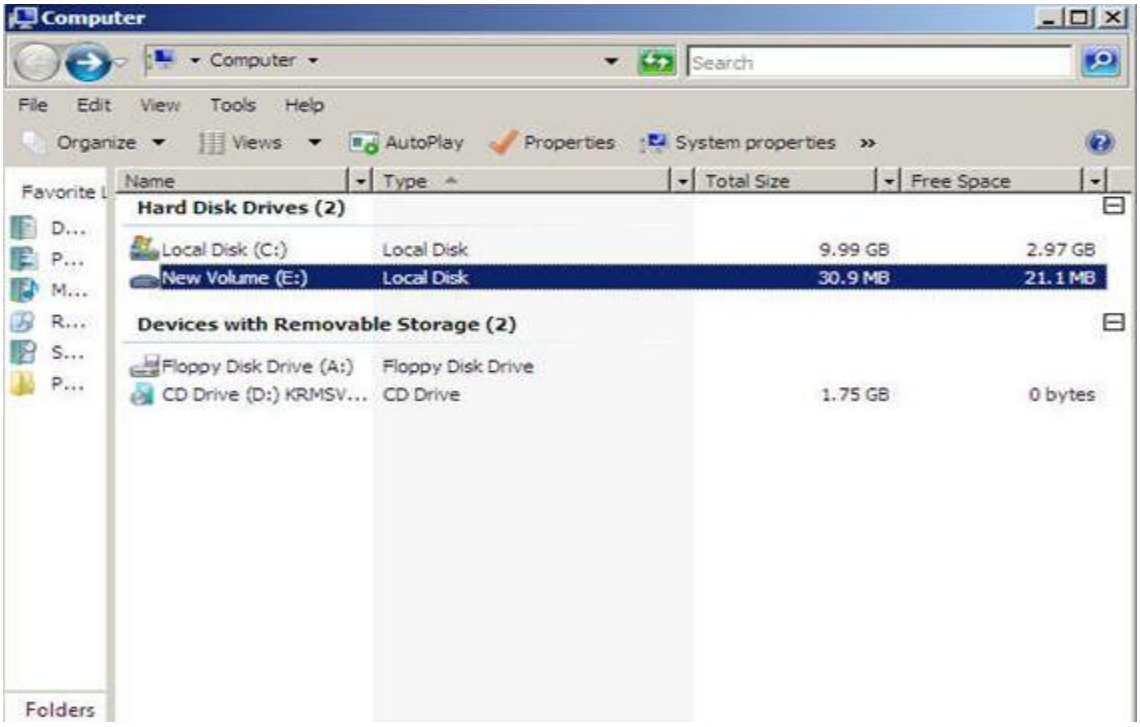
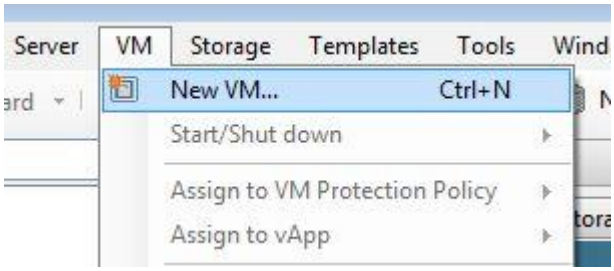


Figure 14: Windows Server 2008 – view of shared iSCSI volume

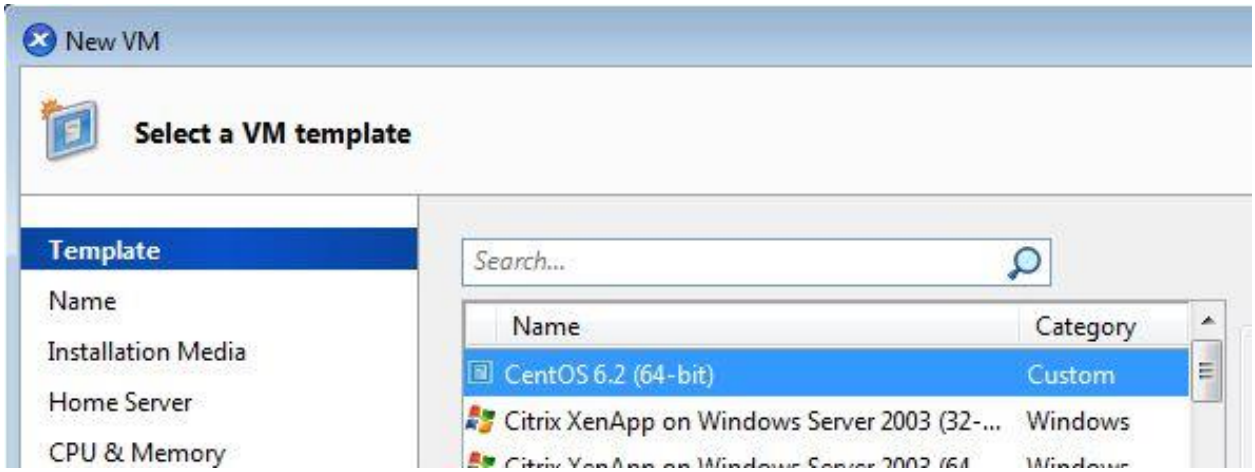
Create new CentOS 6.2 Virtual Server

To create a new Linux CentOS 6.2 64-bit server use Citrix XenCenter with CentOS 6.2 (64-bit) template.

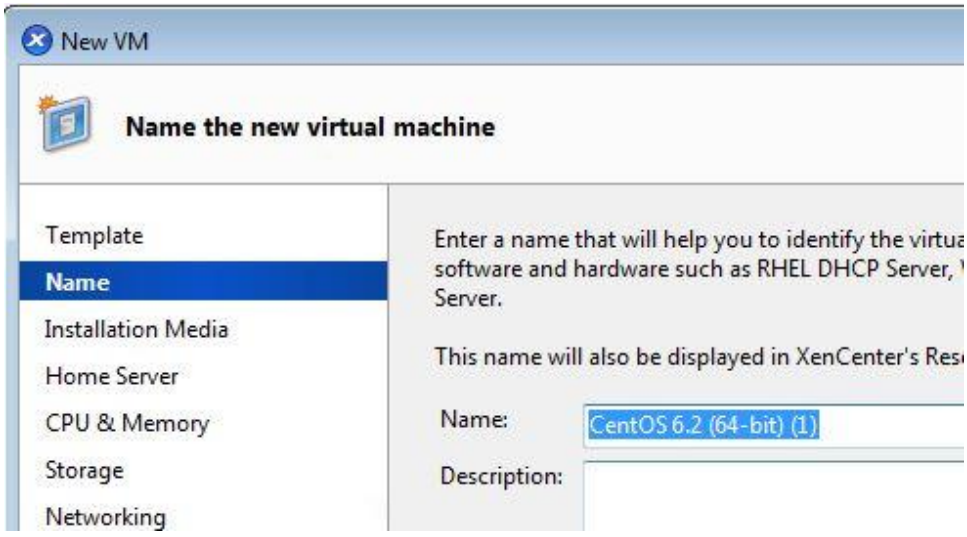
1. Start the VM Wizard by selecting “New VM…” in the VM menu



2. Select CentOS 6.2 Template

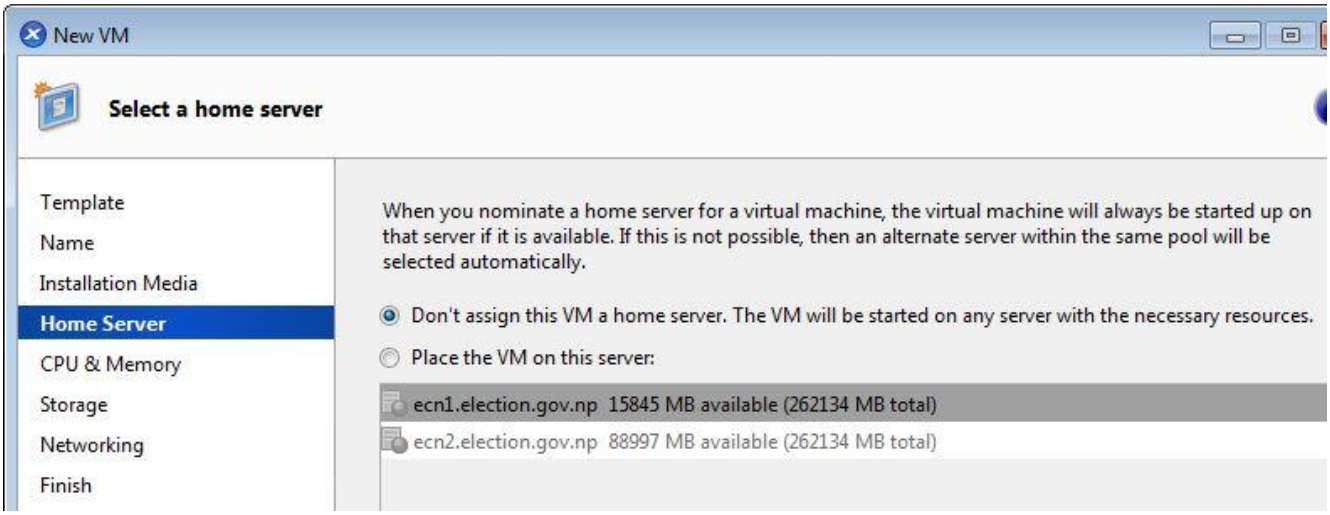


3. Enter name and description

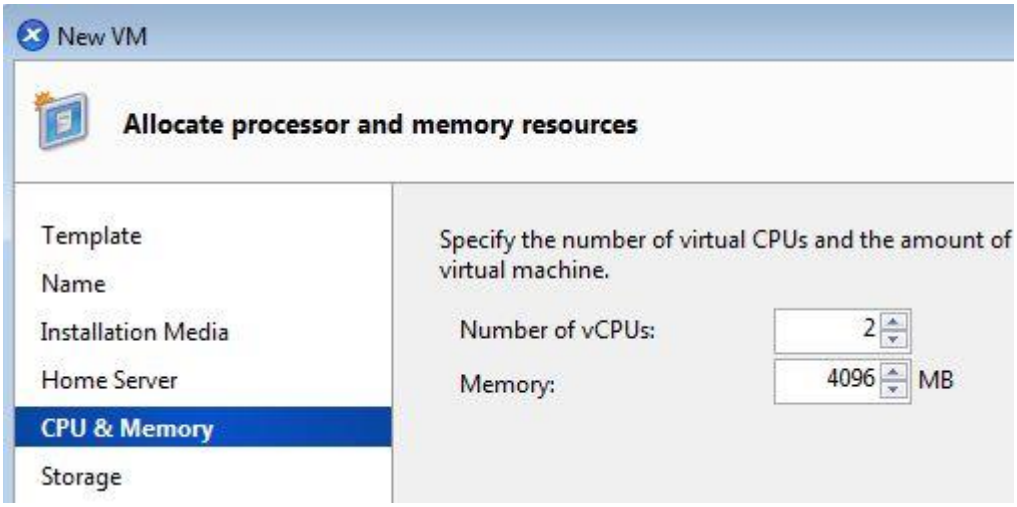


4. Make sure the installation media drive is “<Empty>”.

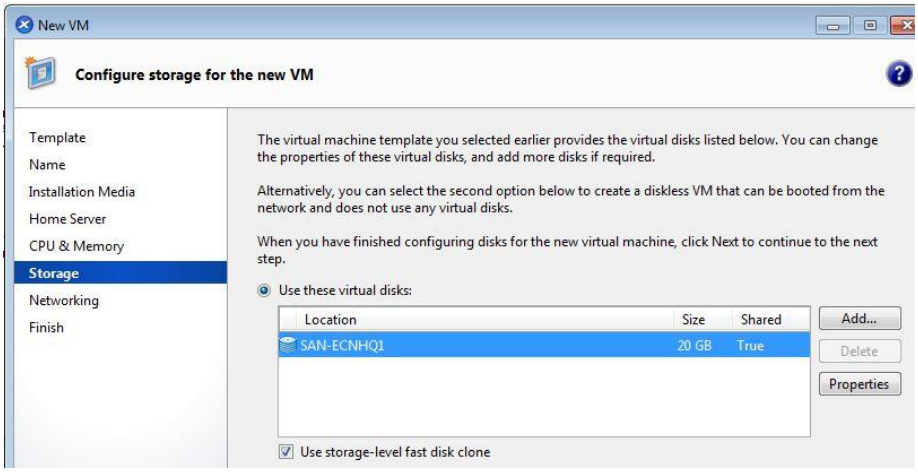
5. Select pool managed home server – i.e. no home server.



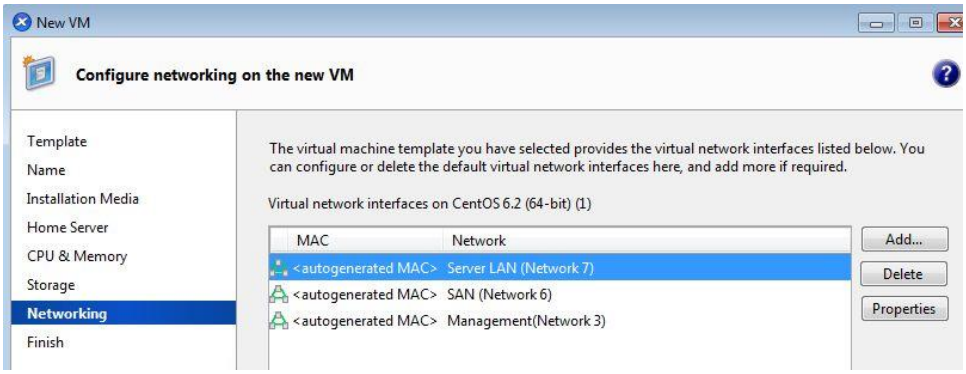
6. Adjust CPU and Memory as required.



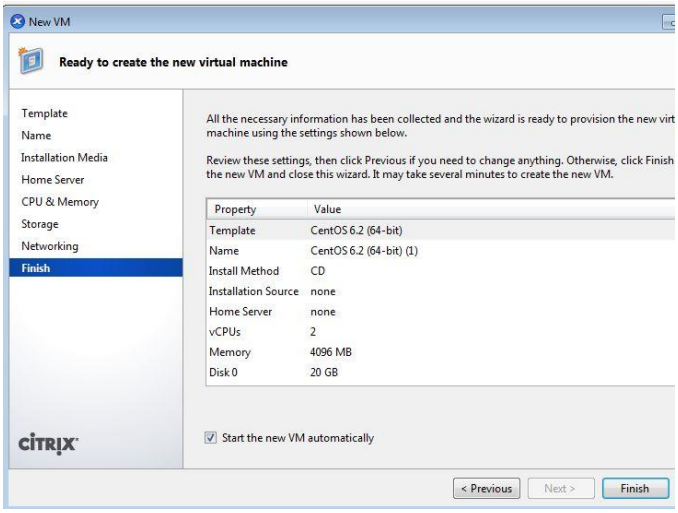
7. Adjust storage as required.



8. Adjust network as required.



9. Check settings and create the new VM.



10. After startup you must edit network settings by setting:

    ONBOOT=yes
    IPADDR=[IP Address]
    PREFIX=255.255.255.0
    DNS1=116.90.227.65
    DNS2=116.90.227.15
    In /etc/sysconfig/ifcfg-[Interface]

11. You must also set hostname by editing /etc/sysconfig/network
12. Restart the network and update the system:

    ```
    service network restart
    ```

    Make sure the network restarts with your new settings (e.g. ping www.google.com).

    Then update the system by running

    ```
    yum –y update
    ```

13. Finally reboot the system.

    ```
    reboot
    ```

Repair LDAP Database

When the Intranet server is uncleanly shut down the LDAP database (which manages all users and email) may become corrupt. You may see errors like this either when you try to manually start LDAP or in the startup messages:

```
[root@intranet ldap]# service ldap start
Checking configuration files for slapd: bdb_db_open:
unclean shutdown detected; attempting recovery.
bdb_db_open: Recovery skipped in read-only mode. Run
manual recovery if errors are encountered.
bdb_db_open: Database cannot be opened, err 13. Restore
from backup!
bdb(dc=mydomain,dc=com): DB_ENV->lock_id_free interface
requires an environment configured for the locking
subsystem
backend_startup_one: bi_db_open failed! (13)
slap_startup failed (test would succeed using the -u
switch)
[FAILED]
stale lock files may be present in /var/lib/ldap
[WARNING]
```

To repair the database follow these steps:

1. First stop the LDAP service using the console:

   ```
   [root@intranet ldap]# service ldap stop
   Stopping slapd: [  OK  ]
   ```

2. Repair the database:

   ```
   [root@intranet ldap]# /usr/sbin/slapd_db_recover -v
   -h /var/lib/ldap
   Finding last valid log LSN: file: 2 offset 5391986
   Recovery starting from [2][5391841]
   Recovery complete at Thu Jun 21 12:44:13 2012
   Maximum transaction ID 80000013 Recovery checkpoint
   [2][5391986]
   ```

3. Restart the LDAP service

   ```
   [root@intranet ldap]# service ldap start
   Starting slapd: [  OK  ]
   ```

Configuration files

Fortinet

```
#config-version=FG100A-3.00-FW-build678-090504:opmode=0:vdom=0:user=admin
#conf_file_ver=12131535706409079390
#buildno=0678
config system global
    set access-banner disable
    set admin-https-pki-required disable
    set admin-lockout-duration 60
    set admin-lockout-threshold 3
    set admin-maintainer enable
    set admin-port 80
    set admin-scp disable
    set admin-server-cert "Fortinet_Factory"
    set admin-sport 443
    set admin-ssh-port 22
    set admin-ssh-v1 disable
    set admin-telnet-port 23
    set admintimeout 15
    set allow-interface-subnet-overlap disable
    set auth-cert "self-sign"
    set auth-http-port 1000
    set auth-https-port 1003
    set auth-keepalive disable
    set batch-cmdb enable
    set cfg-save automatic
    set check-reset-range disable
    set clt-cert-req disable
    set conn-tracking enable
    set daily-restart disable
    set detection-summary enable
    set dst disable
    set failtime 5
    set fds-statistics enable
    set fsae-burst-size 300
    set fsae-rate-limit 100
    set gui-ipv6 disable
    set gui-lines-per-page 50
    set hostname "Election-Comm-FG"
    set http-obfuscate modified
    set ie6workaround disable
    set internal-switch-mode switch
    set interval 5
    set ip-src-port-range 1024-25000
    set language english
    set ldapconntimeout 500
    set loglocaldeny disable
    set management-vdom "root"
    set ntpserver "pool.ntp.org"
    set ntpsync disable
    set phase1-rekey enable
    set radius-port 1812
    set refresh 0
    set remoteauthtimeout 5
    set reset-sessionless-tcp disable
    set sslvpn-sport 10443
    set strong-crypto disable
    set syncinterval 60
    set tcp-halfclose-timer 120
    set tcp-halfopen-timer 60
    set tcp-option enable
    set tcp-timewait-timer 120
    set timezone 48
    set tos-based-priority high
    set udp-idle-timer 180
    set user-server-cert "Fortinet_Factory"
    set vdom-admin disable
```

```
    set vip-arp-range restricted
    set fds-statistics-period 60
  end
  config system accprofile
    edit "prof_admin"
      set admingrp read-write
      set authgrp read-write
      set avgrp read-write
      set fwgrp read-write
      set imp2pgrp read-write
      set ipsgrp read-write
      set loggrp read-write
      set mntgrp read-write
      set netgrp read-write
      set routegrp read-write
      set spamgrp read-write
      set sysgrp read-write
      set updategrp read-write
      set vpngrp read-write
      set webgrp read-write
    next
  end
  config system interface
    edit "wan1"
      set vdom "root"
      set ip 116.90.232.38 255.255.255.252
      set allowaccess ping https ssh
      set type physical
      set alias "Primary-Fiber"
    next
    edit "wan2"
      set vdom "root"
      set ip 116.90.232.146 255.255.255.252
      set allowaccess ping https ssh
      set type physical
      set alias "Backup-Wireless"
    next
    edit "dmz1"
      set vdom "root"
      set ip 10.0.6.2 255.255.255.0
      set allowaccess ping https ssh
      set type physical
      set alias "ISP Gateway"
    next
    edit "dmz2"
      set vdom "root"
      set allowaccess ping telnet
      set status down
      set type physical
    next
    edit "internal"
      set vdom "root"
      set ip 192.168.10.1 255.255.255.0
      set allowaccess ping https telnet
      set type physical
      set alias "Election-Commission-LAN"
    next
    edit "ssl.root"
      set vdom "root"
      set type tunnel
    next
    edit "loopback"
      set vdom "root"
      set ip 116.90.236.201 255.255.255.248
      set allowaccess ping
      set type loopback
      set description "Loopback BGP"
    next
  end
  config system admin
    edit "admin"
```

```
      set accprofile "super_admin"
      set vdom "root"
        config dashboard
          edit "tr-history"
            set column 1
            set refresh disable
          next
          edit "licinfo"
            set column 1
          next
          edit "sysinfo"
            set column 1
          next
          edit "jsconsole"
            set column 1
            set status close
          next
          edit "statistics"
            set column 2
          next
          edit "alert"
            set column 2
            set show-conserve-mode enable
            set show-firmware-change enable
            set show-system-restart enable
          next
          edit "sysop"
            set column 2
          next
          edit "sysres"
            set column 2
            set show-fds-chart enable
            set show-fortianalyzer-chart enable
          next
        end
      set password ENC AK1Y2AL+sLK5iUpUjzDTbNuTBa5yWF85Y53YUVI61/raKM=
    next
end
config system ha
    set group-id 0
    set group-name "FGT-HA"
    set mode standalone
    set password ENC
AXAud6b24eR4vNND3O/P5FZvJEMuXlRtgaGJjDYgkjloAnfxXdK3tyJbByjRW91ceny9ANQbD6QRUOB1oLwZLdECnRWGSQdtuknAc
w4KrKbalL/F
    set hbdev "dmz2" 50 "wan2" 50
    set route-ttl 10
    set route-wait 0
    set route-hold 10
    set sync-config enable
    set encryption disable
    set authentication disable
    set hb-interval 2
    set hb-lost-threshold 6
    set helo-holddown 20
    set arps 5
    set arps-interval 8
    set session-pickup disable
    set link-failed-signal disable
    set uninterruptable-upgrade enable
    set vcluster2 disable
    set override disable
    set priority 128
    set pingserver-failover-threshold 0
    set pingserver-flip-timeout 60
end
config system dns
    set primary 116.90.227.65
    set secondary 116.90.227.15
    set domain ''
    set autosvr disable
```

```
    set fwdintf "internal"
    set dns-cache-limit 5000
    set cache-notfound-responses disable
end
config system replacemsg mail "email-block"
    set buffer "Potentially Dangerous Attachment Removed. The file \"%%FILE%%\" has been blocked.  File quarantined as:
\"%%QUARFILENAME%%\"."
    set format text
    set header 8bit
end
config system replacemsg mail "email-virus"
    set buffer "Dangerous Attachment has been Removed.  The file \"%%FILE%%\" has been removed because of a virus.  It was
infected with the \"%%VIRUS%%\" virus.  File quarantined as: \"%%QUARFILENAME%%\"."
    set format text
    set header 8bit
end
config system replacemsg mail "email-filesize"
    set buffer "This email has been blocked.  The email message is larger than the configured file size limit."
    set format text
    set header 8bit
end
config system replacemsg mail "partial"
    set buffer "Fragmented emails are blocked."
    set format text
    set header 8bit
end
config system replacemsg mail "smtp-block"
    set buffer "The file %%FILE%% has been blocked. File quarantined as: %%QUARFILENAME%%"
    set format text
    set header none
end
config system replacemsg mail "smtp-virus"
    set buffer "The file %%FILE%% has been infected with the virus %%VIRUS%% File quarantined as %%QUARFILENAME%%"
    set format text
    set header none
end
config system replacemsg mail "smtp-filesize"
    set buffer "This message is larger than the configured limit and has been blocked."
    set format text
    set header none
end
config system replacemsg http "bannedword"
    set buffer "<HTML><BODY>The page you requested has been blocked because it contains a banned word. URL =
http://%%URL%%</BODY></HTML>"
    set format html
    set header http
end
config system replacemsg http "url-block"
    set buffer "<HTML><BODY>The URL you requested has been blocked. URL = %%URL%%</BODY></HTML>"
    set format html
    set header http
end
config system replacemsg http "infcache-block"
    set buffer "<HTML><BODY><H2>High security alert!!!</h2><p>The URL you requested was previously found to be
infected.</p><p>URL = http://%%URL%%</p></BODY></HTML>"
    set format html
    set header http
end
config system replacemsg http "http-block"
    set buffer "<HTML> <BODY> <h2>High security alert!!!</h2> <p>You are not permitted to download the file
\"%%FILE%%\".</p> <p>URL = http://%%URL%%</p> </BODY> </HTML>"
    set format html
    set header http
end
config system replacemsg http "http-virus"
    set buffer "<HTML><BODY><h2>High security alert!!!</h2><p>You are not permitted to download the file \"%%FILE%%\"
because it is infected with the virus \"%%VIRUS%%\". </p><p>URL = http://%%URL%%</p><p>File quarantined
as: %%QUARFILENAME%%.</p></BODY></HTML>"
    set format html
    set header http
end
```

```
config system replacemsg http "http-filesize"
   set buffer "<HTML><BODY>  <h2>Attention!!!</h2><p>The file \"%%FILE%%\" has been blocked.  The file is larger than the
configured file size limit.</p> <p>URL = http://%%URL%%</p> </BODY></HTML>"
   set format html
   set header http
end
config system replacemsg http "http-client-block"
   set buffer "<HTML> <BODY> <h2>High security alert!!!</h2> <p>You are not permitted to upload the file \"%%FILE%%\".</p>
<p>URL = http://%%URL%%</p> </BODY> </HTML>"
   set format html
   set header http
end
config system replacemsg http "http-client-virus"
   set buffer "<HTML><BODY><h2>High security alert!!!</h2><p>You are not permitted to upload the file \"%%FILE%%\"
because it is infected with the virus \"%%VIRUS%%\". </p><p>URL = http://%%URL%%</p><p>File quarantined
as: %%QUARFILENAME%%.</p></BODY></HTML>"
   set format html
   set header http
end
config system replacemsg http "http-client-filesize"
   set buffer "<HTML><BODY>  <h2>Attention!!!</h2><p>Your request has been blocked.  The request is larger than the
configured file size limit.</p> <p>URL = http://%%URL%%</p> </BODY></HTML>"
   set format html
   set header http
end
config system replacemsg http "http-client-bannedword"
   set buffer "<HTML><BODY>The page you uploaded has been blocked because it contains a banned word. URL =
http://%%URL%%</BODY></HTML>"
   set format html
   set header http
end
config system replacemsg ftp "ftp-dl-infected"
   set buffer "Transfer failed.  The file %%FILE%% is infected with the virus %%VIRUS%%. File quarantined
as %%QUARFILENAME%%."
   set format text
   set header none
end
config system replacemsg ftp "ftp-dl-blocked"
   set buffer "Transfer failed.  You are not permitted to transfer the file \"%%FILE%%\"."
   set format text
   set header none
end
config system replacemsg ftp "ftp-dl-filesize"
   set buffer "File size limit exceeded."
   set format text
   set header none
end
config system replacemsg nntp "nntp-dl-infected"
   set buffer "Dangerous Attachment has been Removed.  The file \"%%FILE%%\" has been removed because of a virus.  It was
infected with the \"%%VIRUS%%\" virus.  File quarantined as: \"%%QUARFILENAME%%\"."
   set format text
   set header none
end
config system replacemsg nntp "nntp-dl-blocked"
   set buffer "The file %%FILE%% has been blocked. File quarantined as: %%QUARFILENAME%%"
   set format text
   set header none
end
config system replacemsg nntp "nntp-dl-filesize"
   set buffer "This article has been blocked.  The article is larger than the configured file size limit."
   set format text
   set header none
end
config system replacemsg alertmail "alertmail-virus"
   set buffer "Virus/Worm detected: %%VIRUS%% Protocol: %%PROTOCOL%% Source IP: %%SOURCE_IP%% Destination
IP: %%DEST_IP%% Email Address From: %%EMAIL_FROM%% Email Address To: %%EMAIL_TO%% "
   set format text
   set header none
end
config system replacemsg alertmail "alertmail-block"
```

```
    set buffer "File Block Detected: %%FILE%% Protocol: %%PROTOCOL%% Source IP: %%SOURCE_IP%% Destination
IP: %%DEST_IP%% Email Address From: %%EMAIL_FROM%% Email Address To: %%EMAIL_TO%% "
    set format text
    set header none
end
config system replacemsg alertmail "alertmail-nids-event"
    set buffer "The following intrusion was observed: %%NIDS_EVENT%%."
    set format text
    set header none
end
config system replacemsg alertmail "alertmail-crit-event"
    set buffer "The following critical firewall event was detected: %%CRITICAL_EVENT%%."
    set format text
    set header none
end
config system replacemsg alertmail "alertmail-disk-full"
    set buffer "The log disk is Full."
    set format text
    set header none
end
config system replacemsg fortiguard-wf "ftgd-block"
    set buffer "<html><head><title>Web Filter Violation</title></head><body><font size=2><table
width=\"100%\"><tr><td>%%FORTIGUARD_WF%%</td><td align=\"right\">%%FORTINET%%</td></tr><tr><td
bgcolor=#ff6600 align=\"center\" colspan=2><font color=#ffffff><b>Web Page
Blocked</b></font></td></tr></table><br><br>You have tried to access a web page which is in violation of your internet usage
policy.<br><br>URL: %%URL%%<br>Category: %%CATEGORY%%<br><br>To have the rating of this web page re-
evaluated <u><a href=\"%%FTGD_RE_EVAL%%\">please click here</a></u>.<br>%%OVERRIDE%%<br><hr><br>Powered
by %%SERVICE%%.</font></body></html>"
    set format html
    set header http
end
config system replacemsg fortiguard-wf "http-err"
    set buffer "<html><head><title>%%HTTP_ERR_CODE%% %%HTTP_ERR_DESC%%</title></head><body><font size=2><table
width=\"100%\"><tr><td>%%FORTIGUARD_WF%%</td><td align=\"right\">%%FORTINET%%</td></tr><tr><td
bgcolor=#3300cc align=\"center\" colspan=2><font
color=#ffffff><b>%%HTTP_ERR_CODE%% %%HTTP_ERR_DESC%%</b></font></td></tr></table><br><br>The webserver
for %%URL%% reported that an error occurred while trying to access the website.  Please click <u><a
onclick=\"history.back()\">here</a></u> to return to the previous page.<br><br><hr><br>Powered
by %%SERVICE%%.</font></body></html>"
    set format html
    set header http
end
config system replacemsg fortiguard-wf "ftgd-ovrd"
    set buffer "<html><head><title>Web Filter Block Override</title></head><body><font size=2><table
width=\"100%\"><tr><td>%%FORTIGUARD_WF%%</td><td align=\"right\">%%FORTINET%%</td></tr><tr><td
bgcolor=#3300cc align=\"center\" colspan=2><font color=#ffffff><b>Web Filter Block Override</b></font></td></tr><tr><td
colspan=2><br><br>If you have been granted override creation privileges by your administrator, you can enter your username
and password here to gain immediate access to the blocked web-page.  If you do not have these privileges, please contact your
administrator to gain access to the web-page.<br><br></td></tr><tr><td align=\"center\"
colspan=2>%%OVRD_FORM%%</td></tr></table><br><br><hr><br>Powered by %%SERVICE%%.</font></body></html>"
    set format html
    set header http
end
config system replacemsg spam "ipblocklist"
    set buffer "Mail from this IP address is not allowed and has been blocked."
    set format text
    set header none
end
config system replacemsg spam "smtp-spam-dnsbl"
    set buffer "This message has been blocked because it is from a DNSBL/ORDBL IP address."
    set format text
    set header none
end
config system replacemsg spam "smtp-spam-feip"
    set buffer "This message has been blocked because it is from a FortiGuard - AntiSpam black IP address."
    set format text
    set header none
end
config system replacemsg spam "smtp-spam-helo"
    set buffer "This message has been blocked because the HELO/EHLO domain is invalid."
    set format text
```

```
    set header none
end
config system replacemsg spam "smtp-spam-emailblack"
    set buffer "Mail from this email address is not allowed and  has been blocked."
    set format text
    set header none
end
config system replacemsg spam "smtp-spam-mimeheader"
    set buffer "This message has been blocked because it contains an invalid header."
    set format text
    set header none
end
config system replacemsg spam "reversedns"
    set buffer "This message has been blocked because the return email domain is invalid."
    set format text
    set header none
end
config system replacemsg spam "smtp-spam-bannedword"
    set buffer "This message has been blocked because it contains a banned word."
    set format text
    set header none
end
config system replacemsg spam "smtp-spam-fsurl"
    set buffer "This message has been blocked because it contains FortiGuard - AntiSpam blocking URL(s)."
    set format text
    set header none
end
config system replacemsg spam "smtp-spam-fschksum"
    set buffer "This message has been blocked because its checksum is in FortiGuard - AntiSpam checksum blacklist."
    set format text
    set header none
end
config system replacemsg spam "submit"
    set buffer "If this email is not spam, click here to submit the signatures to FortiGuard - AntiSpam Service."
    set format text
    set header none
end
config system replacemsg admin "admin-disclaimer-text"
    set buffer "W A R N I N G W A R N I N G W A R N I N G W A R N I N G
This is a private computer system. Unauthorized access or use
is prohibited and subject to prosecution and/or disciplinary
action. All use of this system constitutes consent to
monitoring at all times and users are not entitled to any
expectation of privacy. If monitoring reveals possible evidence
of violation of criminal statutes, this evidence and any other
related information, including identification information about
the user, may be provided to law enforcement officials.
If monitoring reveals violations of security regulations or
unauthorized use, employees who violate security regulations or
make unauthorized use of this system are subject to appropriate
disciplinary action.
W A R N I N G W A R N I N G W A R N I N G W A R N I N G
"
    set format text
    set header none
end
config system replacemsg auth "auth-disclaimer-page-1"
    set buffer "<HTML><HEAD><TITLE>Firewall Disclaimer</TITLE></HEAD><BODY><FORM ACTION=\"/\"
method=\"POST\"><INPUT TYPE=\"hidden\" NAME=\"%%MAGICID%%\" VALUE=\"%%MAGICVAL%%\"><INPUT
TYPE=\"hidden\" NAME=\"%%ANSWERID%%\" VALUE=\"%%DECLINEVAL%%\"><INPUT TYPE=\"hidden\"
NAME=\"%%REDIRID%%\" VALUE=\"%%PROTURI%%\"><TABLE ALIGN=\"CENTER\" width=400 height=250 cellpadding=2
cellspacing=0 border=0 bgcolor=\"#008080\"><TR><TD><TABLE border=0 width=\"100%\" height=\"100%\" cellpadding=0
cellspacing=0 bgcolor=\"#9dc8c6\"><TR height=30 bgcolor=\"#008080\"><TD><b><font size=2 face=\"Verdana\"
color=\"#ffffff\">Disclaimer Agreement</font></b></TD><TR><TR height=\"100%\"><TD><TABLE border=0 cellpadding=5
cellspacing=0 width=\"320\" align=center><TR><TD colspan=2><font size=2 face=\"Times New Roman\">You are about to
access Internet content that is not under the control of the network access provider.  The network access provider is therefore
not responsible for any of these sites, their content or their privacy policies. The network access provider and its staff do not
endorse nor make any representations about these sites, or any information, software or other products or materials found
there, or any results that may be obtained from using them. If you decide to access any Internet content, you do this entirely at
your own risk and you are responsible for ensuring that any accessed material does not infringe the laws governing, but not
exhaustively covering, copyright, trademarks, pornography, or any other material which is slanderous, defamatory or might
```

```
cause offence in any other way.</font></TD></TR><TR><TD>Do you agree to the above terms?</TD></TR><TR><TD><INPUT
CLASS=\"button\" TYPE=\"button\" VALUE=\"Yes, I agree\" ONCLICK=\"agree()\"><INPUT CLASS=\"button\" TYPE=\"button\"
VALUE=\"No, I decline\"
ONCLICK=\"decline()\"></TD></TR></TABLE></TD></TR></TABLE></TD></TR></TABLE></FORM><SCRIPT
LANGUAGE=\"JavaScript\">function
agree(){document.forms[0].%%ANSWERID%%.value=\"%%AGREEVAL%%\";document.forms[0].submit();}function
decline(){document.forms[0].submit();}</SCRIPT></BODY></HTML>"
    set format html
    set header http
end
config system replacemsg auth "auth-disclaimer-page-2"
    set buffer ''
    set format html
    set header http
end
config system replacemsg auth "auth-disclaimer-page-3"
    set buffer ''
    set format html
    set header http
end
config system replacemsg auth "auth-reject-page"
    set buffer "<HTML><HEAD><TITLE>Firewall Disclaimer Declined</TITLE></HEAD><BODY><FORM ACTION=\"/\"
method=\"POST\"><INPUT TYPE=\"hidden\" NAME=\"%%MAGICID%%\" VALUE=\"%%MAGICVAL%%\"><INPUT
TYPE=\"hidden\" NAME=\"%%REDIRID%%\" VALUE=\"%%PROTURI%%\"><TABLE ALIGN=\"CENTER\" width=400 height=250
cellpadding=2 cellspacing=0 border=0 bgcolor=\"#008080\"><TR><TD><TABLE border=0 width=\"100%\" height=\"100%\"
cellpadding=0 cellspacing=0 bgcolor=\"#9dc8c6\"><TR height=30 bgcolor=\"#008080\"><TD><b><font size=2 face=\"Verdana\"
color=\"#ffffff\">Disclaimer Declined</font></b></TD><TR><TR height=\"100%\"><TD><TABLE border=0 cellpadding=5
cellspacing=0 width=\"320\" align=center><TR><TD colspan=2><font size=2 face=\"Times New Roman\">Sorry, network access
cannot be granted unless you agree to the disclaimer.</font></TD><TR><TR><TD></TD><TD><INPUT TYPE=\"submit\"
VALUE=\"Return to Disclaimer\"></TD></TR></TABLE></TD></TR></TABLE></TD></TR></TABLE></FORM></BODY></HTML>"
    set format html
    set header http
end
config system replacemsg auth "auth-login-page"
    set buffer "<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD><BODY><FORM ACTION=\"/\"
method=\"POST\"><INPUT TYPE=\"hidden\" NAME=\"%%MAGICID%%\" VALUE=\"%%MAGICVAL%%\"><TABLE
ALIGN=\"CENTER\" width=400 height=250 cellpadding=2 cellspacing=0 border=0 bgcolor=\"#008080\"><TR><TD><TABLE
border=0 cellpadding=0 cellspacing=0 bgcolor=\"#9dc8c6\"><TR height=30 bgcolor=\"#008080\"><TD><b><font size=2
face=\"Verdana\" color=\"#ffffff\">Authentication Required</font></b></TD></TR><TR><TD><TABLE border=0 cellpadding=5
cellspacing=0 width=\"320\" align=center><TR><TD colspan=2><font size=2 face=\"Times New
Roman\">%%QUESTION%%</font></TD></TR><TR><TD><font size=2 face=\"Times New
Roman\">Username:</font></TD><TD><INPUT TYPE=\"text\" NAME=\"%%USERNAMEID%%\"
size=25></TD></TR><TR><TD><font size=2 face=\"Times New Roman\">Password:</font></TD><TD><INPUT
TYPE=\"password\" NAME=\"%%PASSWORDID%%\" size=25></TD></TR><TR><TD><INPUT TYPE=\"hidden\"
NAME=\"%%REDIRID%%\" VALUE=\"%%PROTURI%%\"><INPUT TYPE=\"submit\"
VALUE=\"Continue\"></TD></TR></TABLE></TD></TR></TABLE></TD></TR></TABLE></FORM></BODY></HTML>"
    set format html
    set header http
end
config system replacemsg auth "auth-login-failed-page"
    set buffer "<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD><BODY><FORM ACTION=\"/\"
method=\"POST\"><INPUT TYPE=\"hidden\" NAME=\"%%MAGICID%%\" VALUE=\"%%MAGICVAL%%\"><TABLE
ALIGN=\"CENTER\" width=400 height=250 cellpadding=2 cellspacing=0 border=0 bgcolor=\"#008080\"><TR><TD><TABLE
border=0 cellpadding=0 cellspacing=0 bgcolor=\"#9dc8c6\"><TR height=30 bgcolor=\"#008080\"><TD><b><font size=2
face=\"Verdana\" color=\"#ffffff\">Authentication Failed</font></b></TD></TR><TR><TD><TABLE border=0 cellpadding=5
cellspacing=0 width=\"320\" align=center><TR><TD colspan=2><font size=2 face=\"Times New
Roman\">%%FAILED_MESSAGE%%</font></TD></TR><TR><TD><font size=2 face=\"Times New
Roman\">Username:</font></TD><TD><INPUT TYPE=\"text\" NAME=\"%%USERNAMEID%%\"
size=25></TD></TR><TR><TD><font size=2 face=\"Times New Roman\">Password:</font></TD><TD><INPUT
TYPE=\"password\" NAME=\"%%PASSWORDID%%\" size=25></TD></TR><TR><TD><INPUT TYPE=\"hidden\"
NAME=\"%%REDIRID%%\" VALUE=\"%%PROTURI%%\"><INPUT TYPE=\"submit\"
VALUE=\"Continue\"></TD></TR></TABLE></TD></TR></TABLE></TD></TR></TABLE></FORM></BODY></HTML>"
    set format html
    set header http
end
config system replacemsg auth "auth-challenge-page"
    set buffer "<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD><BODY><FORM ACTION=\"/\"
method=\"POST\"><INPUT TYPE=\"hidden\" NAME=\"%%MAGICID%%\" VALUE=\"%%MAGICVAL%%\"><TABLE
ALIGN=\"CENTER\" width=400 height=250 cellpadding=2 cellspacing=0 border=0 bgcolor=\"#008080\"><TR><TD><TABLE
border=0 cellpadding=0 cellspacing=0 bgcolor=\"#9dc8c6\"><TR height=30 bgcolor=\"#008080\"><TD><b><font size=2
face=\"Verdana\" color=\"#ffffff\">Authentication Required</font></b></TD></TR><TR><TD><TABLE border=0 cellpadding=5
```

```
cellspacing=0 width=\"320\" align=center><TR><TD colspan=2><font size=2 face=\"Times New
Roman\">%%QUESTION%%</font></TD></TR><TR><TD><font size=2 face=\"Times New
Roman\">Answer:</font></TD><TD><INPUT TYPE=\"password\" NAME=\"%%PASSWORDID%%\"
size=25></TD></TR><TR><TD><INPUT TYPE=\"hidden\" NAME=\"%%USERNAMEID%%\"
VALUE=\"%%USERNAMEVAL%%\"><INPUT TYPE=\"hidden\" NAME=\"%%REQUESTID%%\"
VALUE=\"%%REQUESTVAL%%\"><INPUT TYPE=\"hidden\" NAME=\"%%REDIRID%%\" VALUE=\"%%PROTURI%%\"><INPUT
TYPE=\"hidden\" NAME=\"%%USERGROUPID%%\" VALUE=\"%%USERGROUPVAL%%\"><INPUT TYPE=\"submit\"
VALUE=\"Continue\"></TD></TR></TABLE></TD></TR></TABLE></TD></TR></TABLE></FORM></BODY></HTML>"
    set format html
    set header http
end
config system replacemsg auth "auth-keepalive-page"
    set buffer "<HTML>
<HEAD>
<TITLE>Firewall Authentication Keepalive Window</TITLE>
</HEAD>
<BODY>
<SCRIPT LANGUAGE=\"JavaScript\">
var countDownTime=%%TIMEOUT%% + 1;
function countDown(){
countDownTime--;
if (countDownTime <= 0){
    location.href=\"%%KEEPALIVEURL%%\";
    return;
}
document.getElementById(\'countdown\').innerHTML = countDownTime;
counter=setTimeout(\"countDown()\", 1000);
}
function startit(){
    countDown();
}
window.onload=startit
</SCRIPT>
<table width=\"100%\" height=\"100%\"><tr><td align=\"center\">
<H3>This browser window is used to keep your authentication session active.</H3>
<H3>Please leave it open in the background and open a <a href=\"%%AUTH_REDIR_URL%%\" target=\"_blank\">new
window</a> to continue.</H3>
<p>Authentication Refresh in <b id=countdown>%%TIMEOUT%%</b> seconds</p>
<p><a href=\"%%AUTH_LOGOUT%%\">logout</a></p>
</td></tr></table>
</BODY>
</HTML>
"
    set format html
    set header http
end
config system replacemsg im "im-file-xfer-block"
    set buffer "Transfer failed.  You are not permitted to transfer the file \"%%FILE%%\"."
    set format text
    set header none
end
config system replacemsg im "im-file-xfer-name"
    set buffer "Transfer %%ACTION%%.  The file name \"%%FILE%%\" matches the configured file name block list."
    set format text
    set header none
end
config system replacemsg im "im-file-xfer-infected"
    set buffer "Transfer %%ACTION%%.  The file \"%%FILE%%\" is infected with the virus %%VIRUS%%.  File quarantined
as %%QUARFILENAME%%."
    set format text
    set header none
end
config system replacemsg im "im-file-xfer-size"
    set buffer "Transfer %%ACTION%%.  The file \"%%FILE%%\" is larger than the configured limit."
    set format text
    set header none
end
config system replacemsg im "im-voice-chat-block"
    set buffer "Connection failed.  You are not permitted to use voice chat."
    set format text
    set header none
```

```
end
config system replacemsg im "im-photo-share-block"
    set buffer "Photo sharing failed.  You are not permitted to share photo."
    set format text
    set header none
end
config system replacemsg im "im-long-chat-block"
    set buffer "Message blocked.  The message is longer than the configured limit."
    set format text
    set header none
end
config system replacemsg sslvpn "sslvpn-login"
    set buffer "<html><head><title>login</title><meta http-equiv=\"Pragma\" content=\"no-cache\"><meta http-
equiv=\"cache-control\" content=\"no-cache\"><meta http-equiv=\"cache-control\" content=\"must-revalidate\"><link
href=\"/ssl_style.css\" rel=\"stylesheet\" type=\"text/css\"><script language=\"JavaScript\"><!--if (top && top.location !=
window.location) top.location = top.location;if (window.opener && window.opener.top) { window.opener.top.location =
window.opener.top.location; self.close(); }//--></script></head><body class=\"main\"><center><table width=\"100%\"
height=\"100%\" align=\"center\" class=\"container\" valign=\"middle\" cellpadding=\"0\" cellspacing=\"0\"><tr
valign=middle><td><form action=\"%%SSL_ACT%%\" method=\"%%SSL_METHOD%%\" name=\"f\"><table class=\"list\"
cellpadding=10 cellspacing=0 align=center width=400
height=180>%%SSL_LOGIN%%</table>%%SSL_HIDDEN%%</td></tr></table></form></center></body><script>document.for
ms[0].username.focus();</script></html>"
    set format html
    set header http
end
config vpn certificate ca
end
config vpn certificate local
end
config system fortiguard
    set hostname "service.fortiguard.net"
    set srv-ovrd disable
    set port 53
    set client-override-status disable
    set service-account-id ''
    set central-mgmt-status disable
    set antispam-status disable
    set antispam-cache enable
    set antispam-cache-ttl 1800
    set antispam-cache-mpercent 2
    set antispam-timeout 7
    set avquery-status disable
    set avquery-cache enable
    set avquery-cache-ttl 1800
    set avquery-cache-mpercent 2
    set avquery-timeout 7
    set webfilter-status disable
    set webfilter-cache enable
    set webfilter-cache-ttl 3600
    set webfilter-timeout 15
end
config gui console
    unset preferences
end
config system session-helper
    edit 1
        set name pptp
        set port 1723
        set protocol 6
    next
    edit 2
        set name h323
        set port 1720
        set protocol 6
    next
    edit 3
        set name ras
        set port 1719
        set protocol 17
    next
    edit 4
```

```
    set name tns
    set port 1521
    set protocol 6
next
edit 5
    set name tftp
    set port 69
    set protocol 17
next
edit 6
    set name rtsp
    set port 554
    set protocol 6
next
edit 7
    set name rtsp
    set port 7070
    set protocol 6
next
edit 8
    set name ftp
    set port 21
    set protocol 6
next
edit 9
    set name mms
    set port 1863
    set protocol 6
next
edit 10
    set name pmap
    set port 111
    set protocol 6
next
edit 11
    set name pmap
    set port 111
    set protocol 17
next
edit 12
    set name sip
    set port 5060
    set protocol 17
next
edit 13
    set name dns-udp
    set port 53
    set protocol 17
next
edit 14
    set name rsh
    set port 514
    set protocol 6
next
edit 15
    set name rsh
    set port 512
    set protocol 6
next
edit 16
    set name dcerpc
    set port 135
    set protocol 6
next
edit 17
    set name dcerpc
    set port 135
    set protocol 17
next
edit 18
    set name mgcp
```

```
      set port 2427
      set protocol 17
    next
    edit 19
      set name mgcp
      set port 2727
      set protocol 17
    next
end
config system auto-install
    set auto-install-config enable
    set auto-install-image enable
    set default-config-file "fgt_system.conf"
    set default-image-file "image.out"
end
config system console
    set mode line
    set output more
end
config antivirus service "http"
    set port 80
    set scan-bzip2 disable
    set uncompnestlimit 12
    set uncompsizelimit 10
end
config antivirus service "https"
    set port 443
    set scan-bzip2 disable
    set uncompnestlimit 0
    set uncompsizelimit 0
end
config antivirus service "ftp"
    set port 21
    set scan-bzip2 disable
    set uncompnestlimit 12
    set uncompsizelimit 10
end
config antivirus service "pop3"
    set port 110
    set scan-bzip2 disable
    set uncompnestlimit 12
    set uncompsizelimit 10
end
config antivirus service "imap"
    set port 143
    set scan-bzip2 disable
    set uncompnestlimit 12
    set uncompsizelimit 10
end
config antivirus service "smtp"
    set port 25
    set scan-bzip2 disable
    set uncompnestlimit 12
    set uncompsizelimit 10
end
config antivirus service "nntp"
    set port 119
    set scan-bzip2 disable
    set uncompnestlimit 12
    set uncompsizelimit 10
end
config antivirus service "im"
    set scan-bzip2 disable
    set uncompnestlimit 12
    set uncompsizelimit 10
end
config antivirus grayware "Adware"
end
config antivirus grayware "Dial"
end
config antivirus grayware "Game"
```

```
end
config antivirus grayware "Joke"
end
config antivirus grayware "P2P"
end
config antivirus grayware "Spy"
end
config antivirus grayware "Keylog"
end
config antivirus grayware "Hijacker"
end
config antivirus grayware "Plugin"
end
config antivirus grayware "NMT"
end
config antivirus grayware "RAT"
end
config antivirus grayware "Misc"
end
config antivirus grayware "BHO"
end
config antivirus grayware "Toolbar"
end
config antivirus grayware "Download"
end
config antivirus grayware "HackerTool"
end
config system dhcp server
  edit "Election-DhcpServer"
    set default-gateway 192.168.10.1
    set dns-server1 192.168.10.1
    set dns-server2 116.90.227.65
    set dns-server3 116.90.227.15
    set end-ip 192.168.10.199
    set interface "internal"
    set netmask 255.255.255.0
    set start-ip 192.168.10.10
  next
end
config firewall address
  edit "all"
  next
  edit "EC_Network"
    set associated-interface "internal"
    set subnet 192.168.10.0 255.255.255.0
  next
  edit "black-list-23"
    set associated-interface "internal"
    set subnet 192.168.10.23 255.255.255.255
  next
  edit "wsn-bgp"
    set associated-interface "wan1"
    set subnet 116.90.232.37 255.255.255.255
  next
  edit "Loop-Back"
    set subnet 116.90.236.201 255.255.255.255
  next
  edit "ECN Data Center 1"
    set associated-interface "dmz1"
    set subnet 10.0.0.0 255.255.0.0
  next
  edit "Internet"
    set associated-interface "wan1"
  next
  edit "Internet_Wireless"
    set associated-interface "wan2"
  next
  edit "ECN DC Server LAN"
    set associated-interface "dmz1"
    set subnet 10.0.3.0 255.255.255.0
  next
```

```
    edit "ECN DC Management LAN"
      set associated-interface "dmz1"
      set subnet 10.0.2.0 255.255.255.0
    next
    edit "ECN DC External"
      set associated-interface "dmz1"
      set subnet 10.0.6.0 255.255.255.0
    next
    edit "PPTPVPN_EXt"
      set associated-interface "wan1"
      set type iprange
      set end-ip 10.0.2.90
      set start-ip 10.0.2.80
    next
    edit "PPTPVPN_Int_Mgmt"
      set associated-interface "dmz1"
      set type iprange
      set end-ip 10.0.2.60
      set start-ip 10.0.2.1
    next
    edit "PPTPVPN_Int_Svr"
      set associated-interface "dmz1"
      set type iprange
      set end-ip 10.0.3.254
      set start-ip 10.0.3.1
    next
    edit "WebVL-Host"
      set subnet 10.0.3.0 255.255.255.0
    next
end
config firewall addrgrp
    edit "ECN Data Center"
        set member "ECN DC Server LAN" "ECN DC External" "ECN DC Management LAN"
    next
end
config ips sensor
    edit "all_default"
      set comment "all predefined signatures with default setting"
        config filter
          edit "1"
          next
        end
    next
    edit "all_default_pass"
      set comment "all predefined signatures with PASS action"
        config filter
          edit "1"
            set action pass
          next
        end
    next
    edit "protect_http_server"
      set comment "protect against HTTP server-side vulnerabilities"
        config filter
          edit "1"
            set location server
            set protocol HTTP
          next
        end
    next
    edit "protect_email_server"
      set comment "protect against EMail server-side vulnerabilities"
        config filter
          edit "1"
            set location server
            set protocol SMTP POP3 IMAP
          next
        end
    next
    edit "protect_client"
      set comment "protect against client-side vulnerabilities"
```

```
        config filter
          edit "1"
            set location client
          next
        end
    next
end
config firewall profile
    edit "strict"
        set log-ips enable
        set log-web-ftgd-err enable
        set ftp block oversize scan splice
        set http block oversize scan activexfilter bannedword cookiefilter javafilter rangeblock urlfilter
        unset https
        set imap block oversize scan bannedword spamemailbwl spamfsip spamfschksum spamfssubmit spamfsurl spamhdrcheck
spamraddrdns
        set pop3 block oversize scan bannedword spamemailbwl spamfsip spamfschksum spamfssubmit spamfsurl spamhdrcheck
spamraddrdns
        set smtp block oversize scan bannedword spamemailbwl spamfsip spamfschksum spamfssubmit spamfsurl spamhdrcheck
spamhelodns spamipbwl spamraddrdns spamrbl splice
        set nntp block oversize scan
        set ips-sensor-status enable
        set ips-sensor "all_default"
        set im block oversize scan
        set ftgd-wf-options strict-blocking
        set ftgd-wf-https-options strict-blocking
    next
    edit "scan"
        set log-ips enable
        set log-web-ftgd-err enable
        set ftp scan splice
        set http scan rangeblock
        unset https
        set imap scan
        set pop3 scan
        set smtp scan splice
        set nntp scan
        set ips-sensor-status enable
        set ips-sensor "all_default_pass"
        set im scan
        set ftgd-wf-options strict-blocking
        set ftgd-wf-https-options strict-blocking
    next
    edit "web"
        set log-web-ftgd-err enable
        set ftp splice
        set http scan bannedword fortiguard-wf rangeblock urlfilter
        set https fortiguard-wf
        set imap fragmail
        set pop3 fragmail
        set smtp fragmail splice
        set nntp no-content-summary
        unset im
        set ftgd-wf-options strict-blocking
        set ftgd-wf-https-options strict-blocking
    next
    edit "unfiltered"
        set log-web-ftgd-err enable
        set ftp splice
        set http rangeblock
        unset https
        set imap fragmail
        set pop3 fragmail
        set smtp fragmail splice
        unset nntp
        unset im
        set ftgd-wf-options strict-blocking
        set ftgd-wf-https-options strict-blocking
    next
    edit "election_commision"
        set log-web-ftgd-err enable
```

```
      set ftp splice
      set http bannedword exemptword fortiguard-wf urlfilter
      set https fortiguard-wf block-invalid-url urlfilter
      set imap fragmail spamfssubmit
      set pop3 fragmail spamfssubmit
      set smtp fragmail spamfssubmit splice
      set pop3-spamtagtype subject
      set imap-spamtagtype subject
      set weburlfiltertable 1
      set nntp no-content-summary
      unset im
      set p2p enable
      set bittorrent block
      set edonkey block
      set gnutella block
      set kazaa block
      set winny block
      set ftgd-wf-options strict-blocking
      set ftgd-wf-https-options strict-blocking
      set ftgd-wf-disable all
      set ftgd-wf-allow 18 20 23 68 69 70 71 g06 g07 g08 g21 g22 c01 c02 c03 c04 c05 c06
      set ftgd-wf-deny g01 g02 17 19 g04 g05
      set ftgd-wf-log g04 g05
    next
end
config user local
   edit "peter"
      set type password
      set passwd ENC
q9VUL9iFCQ4bXQPUmjvIryokSXee4CermoHPrldnFkx5+QPB/r52dGGE5yJDgM/JvaVLZsybVezS6UDdabNYnkIzo0jFCYeGsaEAsFIjk8
AapNl1
   next
end
config user group
   edit "PPTPVPN"
      set profile "unfiltered"
         set member "peter"
   next
end
config webfilter bword
end
config webfilter exmword
end
config webfilter urlfilter
   edit 1
         config entries
            edit "www.youtube.com"
               set action allow
            next
            edit "www.utorrent.com"
               set action block
            next
            edit "www.mininova.com"
               set action block
            next
            edit ".torrent"
               set action block
               set type regex
            next
            edit "thepiratebay.org"
               set action block
            next
            edit "www.torrentz.eu"
               set action block
            next
         end
      set name "Blocked Websites"
   next
end
config webfilter ftgd-ovrd
end
```

```
config webfilter ftgd-ovrd-user
end
config webfilter ftgd-local-rating
end
config vpn pptp
  set eip 10.0.2.90
  set sip 10.0.2.80
  set status enable
  set usrgrp "PPTPVPN"
end
config firewall service custom
  edit "IMAPS"
    set protocol TCP/UDP
    set tcp-portrange 993-993:1-65535
  next
end
config firewall service group
  edit "Web-Traffic"
      set member "DNS" "FTP" "HTTP" "HTTPS" "PING" "POP3" "SMTP" "IMAP" "SSH" "TELNET" "IMAPS"
  next
end
config firewall schedule recurring
  edit "always"
    set day sunday monday tuesday wednesday thursday friday saturday
  next
end
config firewall ippool
  edit "Primary-Pool"
    set endip 116.90.236.205
    set interface "wan1"
    set startip 116.90.236.205
  next
  edit "Secondary-Pool"
    set endip 116.90.236.206
    set interface "wan2"
    set startip 116.90.236.206
  next
end
config firewall vip
  edit "MailServer-SMTP"
    set extip 116.90.236.203
    set extintf "wan1"
    set portforward enable
    set mappedip 10.0.3.14
    set extport 25
    set mappedport 25
  next
  edit "Mailserver-POP"
    set extip 116.90.236.203
    set extintf "wan1"
    set portforward enable
    set mappedip 10.0.3.14
    set extport 110
    set mappedport 110
  next
  edit "MailServer-IMAP"
    set extip 116.90.236.203
    set extintf "wan1"
    set portforward enable
    set mappedip 10.0.3.14
    set extport 143
    set mappedport 143
  next
  edit "AnyConnect SSL VPN"
    set extip 116.90.236.203
    set extintf "wan1"
    set portforward enable
    set mappedip 10.0.6.1
    set extport 444
    set mappedport 444
  next
```

```
edit "AnyConnect SSL VPN - UDP"
    set extip 116.90.236.203
    set extintf "wan1"
    set portforward enable
    set protocol udp
    set mappedip 10.0.6.1
    set extport 444
    set mappedport 444
next
edit "MailServer-HTTP"
    set extip 116.90.236.203
    set extintf "wan1"
    set portforward enable
    set mappedip 10.0.3.14
    set extport 85
    set mappedport 80
next
edit "MailServer-HTTPS"
    set extip 116.90.236.203
    set extintf "wan1"
    set portforward enable
    set mappedip 10.0.3.14
    set extport 443
    set mappedport 443
next
edit "SSH"
    set extip 116.90.236.203
    set extintf "wan1"
    set portforward enable
    set mappedip 10.0.2.50
    set extport 1666
    set mappedport 22
next
edit "SSH-Backup"
    set extip 116.90.236.203
    set extintf "wan2"
    set portforward enable
    set mappedip 10.0.2.50
    set extport 1667
    set mappedport 22
next
edit "AnyConnet SSL VPN - Backup"
    set extip 116.90.236.203
    set extintf "wan2"
    set portforward enable
    set mappedip 10.0.6.1
    set extport 442
    set mappedport 444
next
edit "AnyConnet SSL VPN - Backup UDP"
    set extip 116.90.236.203
    set extintf "wan2"
    set portforward enable
    set protocol udp
    set mappedip 10.0.6.1
    set extport 442
    set mappedport 444
next
edit "MailServer-HTTPS-Backup"
    set extip 116.90.236.206
    set extintf "wan2"
    set portforward enable
    set mappedip 10.0.3.14
    set extport 443
    set mappedport 443
next
edit "WebVL"
    set extip 116.90.236.203
    set extintf "wan1"
    set portforward enable
    set mappedip 10.0.3.35
```

```
        set extport 80
        set mappedport 80
        set http enable
        set http-ip-header enable
    next
    edit "Test"
        set extip 116.90.236.203
        set extintf "wan1"
        set portforward enable
        set mappedip 10.0.2.50
        set extport 83
        set mappedport 80
    next
    edit "WebVL-SSH"
        set extip 116.90.236.203
        set extintf "wan1"
        set portforward enable
        set mappedip 10.0.3.35
        set extport 1668
        set mappedport 22
    next
end
config firewall vipgrp
    edit "Inbound SSL VPN"
        set interface "wan1"
            set member "AnyConnect SSL VPN" "AnyConnect SSL VPN - UDP"
    next
    edit "Inbound Mail_Webmail"
        set interface "wan1"
            set member "MailServer-HTTP" "MailServer-HTTPS" "MailServer-IMAP" "MailServer-SMTP" "Mailserver-POP" "WebVL"
    next
    edit "Backup VPN"
        set interface "wan2"
            set member "AnyConnet SSL VPN - Backup" "AnyConnet SSL VPN - Backup UDP" "SSH-Backup"
    next
end
config firewall policy
    edit 3
        set srcintf "internal"
        set dstintf "wan1"
            set srcaddr "black-list-23"
            set dstaddr "all"
        set schedule "always"
            set service "ANY"
    next
    edit 1
        set srcintf "internal"
        set dstintf "wan1"
            set srcaddr "EC_Network"
            set dstaddr "all"
        set action accept
        set schedule "always"
            set service "Web-Traffic"
        set profile-status enable
        set trafficshaping enable
        set profile "election_commision"
        set maxbandwidth 500
        set priority low
        set nat enable
    next
    edit 5
        set srcintf "internal"
        set dstintf "wan2"
            set srcaddr "black-list-23"
            set dstaddr "all"
        set schedule "always"
            set service "ANY"
    next
    edit 4
        set srcintf "internal"
        set dstintf "wan2"
```

```
        set srcaddr "EC_Network"
        set dstaddr "all"
    set action accept
    set schedule "always"
        set service "Web-Traffic"
    set profile-status enable
    set trafficshaping enable
    set profile "election_commision"
    set maxbandwidth 500
    set priority low
    set nat enable
next
edit 10
    set srcintf "wan1"
    set dstintf "loopback"
        set srcaddr "all"
        set dstaddr "Loop-Back"
    set action accept
    set schedule "always"
        set service "PING"
next
edit 11
    set srcintf "wan2"
    set dstintf "loopback"
        set srcaddr "all"
        set dstaddr "Loop-Back"
    set action accept
    set schedule "always"
        set service "PING"
next
edit 8
    set srcintf "dmz1"
    set dstintf "wan1"
        set srcaddr "ECN Data Center 1"
        set dstaddr "all"
    set action accept
    set schedule "always"
        set service "ANY"
    set nat enable
next
edit 9
    set srcintf "dmz1"
    set dstintf "wan2"
        set srcaddr "ECN Data Center 1"
        set dstaddr "all"
    set action accept
    set schedule "always"
        set service "ANY"
    set trafficshaping enable
    set gbandwidth 100
    set maxbandwidth 2000
    set nat enable
next
edit 12
    set srcintf "internal"
    set dstintf "dmz1"
        set srcaddr "all"
        set dstaddr "ECN Data Center"
    set action accept
    set schedule "always"
        set service "ANY"
next
edit 13
    set srcintf "dmz1"
    set dstintf "internal"
        set srcaddr "all"
        set dstaddr "all"
    set action accept
    set schedule "always"
        set service "ANY"
next
```

```
    edit 14
        set srcintf "wan1"
        set dstintf "dmz1"
            set srcaddr "all"
            set dstaddr "Inbound Mail_Webmail" "Inbound SSL VPN"
        set action accept
        set schedule "always"
            set service "ANY"
    next
    edit 15
        set srcintf "wan2"
        set dstintf "dmz1"
            set srcaddr "all"
            set dstaddr "ECN DC Server LAN"
        set action accept
        set schedule "always"
            set service "ANY"
    next
    edit 16
        set srcintf "wan1"
        set dstintf "dmz1"
            set srcaddr "all"
            set dstaddr "PPTPVPN_Int_Mgmt" "PPTPVPN_Int_Svr"
        set action accept
        set schedule "always"
            set service "ANY"
    next
    edit 17
        set srcintf "wan1"
        set dstintf "dmz1"
            set srcaddr "all"
            set dstaddr "SSH"
        set action accept
        set schedule "always"
            set service "ANY"
    next
    edit 18
        set srcintf "wan2"
        set dstintf "dmz1"
            set srcaddr "all"
            set dstaddr "SSH-Backup"
        set action accept
        set schedule "always"
            set service "ANY"
    next
    edit 19
        set srcintf "wan2"
        set dstintf "dmz2"
            set srcaddr "all"
            set dstaddr "Backup VPN"
        set action accept
        set schedule "always"
            set service "ANY"
    next
    edit 20
        set srcintf "dmz1"
        set dstintf "wan1"
            set srcaddr "WebVL-Host"
            set dstaddr "all"
        set action accept
        set schedule "always"
            set service "ANY"
        set trafficshaping enable
        set maxbandwidth 20
        set priority low
    next
end
config firewall policy6
end
config spamfilter bword
    edit 1
```

```
      set name "trojan.exe"
    next
    edit 2
      set name "torrent"
    next
end
config spamfilter ipbwl
end
config spamfilter dnsbl
end
config spamfilter emailbwl
end
config spamfilter mheader
end
config spamfilter iptrust
end
config ips DoS
    edit 1
        config address
            edit 1
            next
        end
        config anomaly
            edit "tcp_syn_flood"
                set status enable
                set threshold 2000
            next
            edit "tcp_port_scan"
                set status enable
                set threshold 1000
            next
            edit "tcp_src_session"
                set status enable
                set threshold 5000
            next
            edit "tcp_dst_session"
                set status enable
                set threshold 5000
            next
            edit "udp_flood"
                set status enable
                set threshold 2000
            next
            edit "udp_scan"
                set status enable
                set threshold 2000
            next
            edit "udp_src_session"
                set status enable
                set threshold 5000
            next
            edit "udp_dst_session"
                set status enable
                set threshold 5000
            next
            edit "icmp_flood"
                set status enable
                set threshold 50
            next
            edit "icmp_sweep"
                set status enable
                set threshold 100
            next
            edit "icmp_src_session"
                set status enable
                set threshold 300
            next
            edit "icmp_dst_session"
                set status enable
                set threshold 1000
            next
```

```
        end
      set name "all_default"
    next
    edit 2
        config address
          edit 1
          next
        end
        config anomaly
          edit "tcp_syn_flood"
            set status enable
            set action block
            set threshold 2000
          next
          edit "tcp_port_scan"
            set threshold 1000
          next
          edit "tcp_src_session"
            set threshold 5000
          next
          edit "tcp_dst_session"
            set threshold 5000
          next
          edit "udp_flood"
            set status enable
            set action block
            set threshold 2000
          next
          edit "udp_scan"
            set threshold 2000
          next
          edit "udp_src_session"
            set threshold 5000
          next
          edit "udp_dst_session"
            set threshold 5000
          next
          edit "icmp_flood"
            set status enable
            set action block
            set threshold 50
          next
          edit "icmp_sweep"
            set threshold 100
          next
          edit "icmp_src_session"
            set threshold 300
          next
          edit "icmp_dst_session"
            set threshold 1000
          next
        end
      set name "block_flood"
    next
end
config log memory setting
    set status enable
end
config log memory filter
    set event enable
    set auth enable
    set system enable
end
config gui topology
    unset background-image
    set database "VE9QT0xPR1kgMgoA8/N6kQG2qqoBf3wSLBpRTQ4AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAEAAABfX0ZvcnRpR2F0ZV9fAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAwAAAAQBAABUAQAAAAEAAAAAAAAACAAAAX19pbnRmX3dhbjFfXwAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAcAAABBAAAAQQAAAAAAAAAABAAAA
CQAAAAMAAABfX2ludGZfd2FuMl9fAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAABwAAAFAAAABQAAAAAAAAAAAEAAAAKAAAABAAAAF9faW50Zl9kbXoxX18AAAAAAAAA
```

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAHAAAAXwAAAF8AAAAAAAAA
AQAAAAgAAAAFAAAAX19pbnRmX2RtejJfXwAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAcAAABuAAAAbgAAAAAAAAAAAAAABgAAAF9faW50Zl9pbnRlcm5hbF9fAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAHAAAAfQAAAH0AAAAAAAAA
AQAAAAcAAAAHAAAARUNfTmV0d29yawAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAEAAADJAQAAuQAAAAABAAABAAAABgAAAAgAAABFQ04gRGF0YSBDZW50ZXIA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQAAAAkBAAAGAgAA
AAEAAAEAAAAEAAAACQAAAEludGVybmV0AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAABAAAAogAAADkAAAAAAQAAAQAAAAIAAAAKAAAASW50ZXJuZXRfV2ly
ZWxlc3MAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEAAAAVAQAA
PAAAAAABAAABAAAAAwAAAAsAAABMb29wLUJhY2sAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQAAAAAAAMAAAAYWxsAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEAAAAAAA
AAAAAEAAAAAAADQAAAGJsYWNrLWxpc3QtMjMAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABAAAAAQAAAAYAAAAOAAAAd3NuLWJncAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAEAAAABAAAAAgAAAA=="
```
   unset preferences
end
config router rip
      config redistribute "connected"
      end
      config redistribute "static"
      end
      config redistribute "ospf"
      end
      config redistribute "bgp"
      end
end
config router static
   edit 3
      set device "wan2"
      set distance 200
      set gateway 116.90.232.145
   next
   edit 2
      set device "dmz1"
      set distance 1
      set dst 10.0.2.0 255.255.255.0
      set gateway 10.0.6.1
   next
   edit 4
      set device "dmz1"
      set distance 1
      set dst 10.0.3.0 255.255.255.0
      set gateway 10.0.6.1
   next
   edit 5
      set device "dmz1"
      set distance 100
      set dst 10.0.6.0 255.255.255.0
      set gateway 10.0.6.1
   next
end
config router ospf
      config redistribute "connected"
      end
      config redistribute "static"
      end
      config redistribute "rip"
      end
      config redistribute "bgp"
      end
end
config router bgp
   set as 64528
   set holdtime-timer 60
      config neighbor
         edit 116.90.232.37
            set interface "wan1"
            set remote-as 24550
```

```
        next
      end
      config network
        edit 1
          set prefix 116.90.236.200 255.255.255.248
        next
      end
      config redistribute "connected"
      end
      config redistribute "rip"
      end
      config redistribute "ospf"
      end
      config redistribute "static"
      end
    set router-id 116.90.232.38
end
config router multicast
end
config antivirus filepattern
  edit 1
      config entries
        edit "*.bat"
        next
        edit "*.com"
        next
        edit "*.dll"
        next
        edit "*.doc"
        next
        edit "*.exe"
        next
        edit "*.gz"
        next
        edit "*.hta"
        next
        edit "*.ppt"
        next
        edit "*.rar"
        next
        edit "*.scr"
        next
        edit "*.tar"
        next
        edit "*.tgz"
        next
        edit "*.vb?"
        next
        edit "*.wps"
        next
        edit "*.xl?"
        next
        edit "*.zip"
        next
        edit "*.pif"
        next
        edit "*.cpl"
        next
      end
    set name "builtin-patterns"
  next
end
```

Cisco ASA 5520

```
: Saved
: Written by enable_15 at 16:08:21.140 NPT Sun Jan 29 2012
!
ASA Version 8.4(2)
!
hostname ecn-rtr
enable password e9vcwHf8b/CaTsR7 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0/0
 channel-group 1 mode active
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/1
 channel-group 1 mode active
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/2
 description To Old LAN
 shutdown
 nameif xoutside
 security-level 0
 ip address dhcp
!
interface GigabitEthernet0/3
 description Internet connection through Fortinet DMZ1
 nameif internet
 security-level 0
 ip address 10.0.6.1 255.255.255.0
!
interface Management0/0
 nameif management
 security-level 100
 ip address 10.0.2.1 255.255.255.0
!
interface Port-channel1
 nameif Trunk
 security-level 100
 no ip address
!
interface Port-channel1.100
 vlan 100
 nameif SAN
 security-level 100
 ip address 10.0.1.1 255.255.255.0
!
interface Port-channel1.300
 vlan 300
 nameif LAN
 security-level 100
 ip address 10.0.3.1 255.255.255.0
!
interface Port-channel1.400
 vlan 400
 nameif CVLALAN
 security-level 100
 ip address 10.0.4.1 255.255.255.0
!
interface Port-channel1.500
 shutdown
 vlan 500
 nameif UserLAN
 security-level 100
 ip address 10.0.5.254 255.255.255.0
```

```
!
ftp mode passive
clock timezone NPT 5 45
dns domain-lookup internet
dns server-group DefaultDNS
 name-server 116.90.227.65
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
object service WWW
 service tcp destination eq www
object network FortinetDMZ1
 host 10.0.6.2
 description Internet gateway
object network NETWORK_OBJ_10.0.2.80_28
 subnet 10.0.2.80 255.255.255.240
object-group network Inside-Networks
 network-object 10.0.0.0 255.255.255.0
 network-object 10.0.2.0 255.255.255.0
object-group network ECN_VLANs
 network-object 10.0.1.0 255.255.255.0
 network-object 10.0.2.0 255.255.255.0
 network-object 10.0.3.0 255.255.255.0
 network-object 10.0.4.0 255.255.255.0
 network-object 10.0.6.0 255.255.255.0
access-list inside_access_in extended permit ip any any
access-list inside_access_in extended permit icmp any any
access-list outside_access_in extended permit ip any any
access-list internet_access_in extended permit ip any any
access-list management_access_in extended permit ip any any
access-list LAN_access_in extended permit ip any any
pager lines 24
logging enable
logging asdm informational
mtu Trunk 1500
mtu SAN 9000
mtu xoutside 1500
mtu management 1500
mtu LAN 1500
mtu CVLALAN 1500
mtu internet 1500
mtu UserLAN 1500
ip local pool ECN_ADMIN_POOL 10.0.2.90-10.0.2.99 mask 255.255.255.0
ip local pool ECN_ADMIN_WIN 10.0.2.80-10.0.2.89 mask 255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
nat (management,xoutside) source dynamic any interface
nat (CVLALAN,xoutside) source static any any destination static NETWORK_OBJ_10.0.2.80_28 NETWORK_OBJ_10.0.2.80_28 no-
proxy-arp route-lookup
access-group outside_access_in in interface xoutside
access-group management_access_in in interface management
access-group LAN_access_in in interface LAN
access-group internet_access_in in interface internet
route internet 0.0.0.0 0.0.0.0 10.0.6.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
aaa authentication ssh console LOCAL
aaa authentication telnet console LOCAL
aaa authorization command LOCAL
http server enable
http 0.0.0.0 0.0.0.0 management
no snmp-server location
no snmp-server contact
```

```
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
crypto ipsec ikev1 transform-set TRANS_ESP_3DES_SHA esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set TRANS_ESP_3DES_SHA mode transport
crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto ipsec ikev2 ipsec-proposal DES
 protocol esp encryption des
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal 3DES
 protocol esp encryption 3des
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES
 protocol esp encryption aes
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES192
 protocol esp encryption aes-192
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES256
 protocol esp encryption aes-256
 protocol esp integrity sha-1 md5
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev1 transform-set ESP-AES-128-SHA ESP-AES-128-MD5 ESP-
AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-256-MD5 ESP-3DES-SHA ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5
TRANS_ESP_3DES_SHA
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev2 ipsec-proposal AES256 AES192 AES 3DES DES
crypto map internet_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP
crypto map internet_map interface internet
crypto ca trustpoint ASDM_TrustPoint0
 enrollment terminal
 subject-name CN=vpn.election.gov.np
 crl configure
crypto ca trustpoint ECNVPN
 enrollment self
 fqdn vpn.election.gov.np
 email admin@election.gov.np
 subject-name CN=vpn
 keypair ENCNVPN
 proxy-ldc-issuer
 crl configure
crypto ca certificate chain ECNVPN
 certificate 184acc4e
   30820345 3082022d a0030201 02020418 4acc4e30 0d06092a 864886f7 0d010105
   05003032 310c300a 06035504 03130376 706e3122 30200609 2a864886 f70d0109
   02161376 706e2e65 6c656374 696f6e2e 676f762e 6e70301e 170d3132 30313235
   30353032 34315a17 0d323230 31323230 35303234 315a3032 310c300a 06035504
   03130376 706e3122 30200609 2a864886 f70d0109 02161376 706e2e65 6c656374
   696f6e2e 676f762e 6e703082 0122300d 06092a86 4886f70d 01010105 00038201
   0f003082 010a0282 010100a7 e08e55a4 e1266c55 dd7d8acb 11feded6 4e5783ea
   90812f14 54e926a7 fd4d2a4c 3c7c0188 41fc8328 07bebfc1 54f140a0 7325f940
   e04bbbc6 8cda5171 3a4ec5ab 69f975c2 ccc19a5d b32b2732 49fa8ee5 47c9875f
   fa608d62 e68a6e49 aaa62408 4573b54a b206a5bb e81d41c7 1c5fafa3 452a82b4
   7e0ac635 aabf63b4 712176a1 6463b834 ab652c15 3edebf13 e527810a 6a30e192
   17b69ff4 4bc1fad1 2169698b 575972ad d0d17f61 00eca1c9 28a8c48d bb8f4d03
   37dc7244 14d30197 3bbf4ace 9e6781df 59b088f1 43d9b8fa 8a65c296 770b51b4
   bfab60c0 fb31db1a d5efe929 cb17c50d 2300523e 129a4cb2 bf5342f1 daa30b2b
   f2dc2788 3537be26 41603f02 03010001 a3633061 300f0603 551d1301 01ff0405
   30030101 ff300e06 03551d0f 0101ff04 04030201 86301f06 03551d23 04183016
   80146ddc e0d66968 1f30d4bb 18cc9673 036838e3 4da1301d 0603551d 0e041604
   146ddce0 d669681f 30d4bb18 cc967303 6838e34d a1300d06 092a8648 86f70d01
   01050500 03820101 003a8806 ee5e241d 07988b80 72faccbe 4f0e3ed7 ac51f2c9
   31649721 dde93573 03b38ece bf9d1d76 375426ab 556a43f1 17c7fbad f9374d90
   5ccba32e 69df9206 7d652e56 482a9c13 c4721a50 b1e91dc6 f883aa47 a9322164
   620c9dcc 940b096d b211c332 837b1d0c 484816bb b745e961 462f6207 0a959a8e
   c2d81bb5 35d1296d b9de2e74 2fd1a703 95abaea5 a9a7a413 5d3b8f5a ae2ee790
```

```
    10e5db37 e064b75a d41f1510 adc371b8 eb536ab9 ee96604a d092ce14 3ff369e8
    46f1c6a2 69287437 5bd91762 7cccf999 b2a1aaf8 039d4d1a 37cdc40c 87c163e0
    ed1a1cb6 641a1b92 cf18034b 0685ce06 8d39f232 3e8da1aa 232e13da 46c88e0a
    03dcdaa4 961c0c4f 6f
  quit
crypto ikev2 policy 1
 encryption aes-256
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 10
 encryption aes-192
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 20
 encryption aes
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 30
 encryption 3des
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 40
 encryption des
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 enable internet client-services port 443
crypto ikev2 remote-access trustpoint ECNVPN
crypto ikev1 enable xoutside
crypto ikev1 enable internet
crypto ikev1 policy 10
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
telnet timeout 5
ssh 0.0.0.0 0.0.0.0 management
ssh timeout 5
console timeout 0
management-access management
dhcpd address 10.0.2.100-10.0.2.120 management
dhcpd dns 116.90.227.65 interface management
dhcpd enable management
!
threat-detection basic-threat
threat-detection statistics port
threat-detection statistics protocol
threat-detection statistics access-list
threat-detection statistics tcp-intercept rate-interval 30 burst-rate 400 average-rate 200
ssl trust-point ECNVPN management
ssl trust-point ECNVPN xoutside
webvpn
 port 444
 enable internet
 anyconnect image disk0:/anyconnect-linux-2.5.2014-k9.pkg 1 regex "Linux"
 anyconnect image disk0:/anyconnect-macosx-i386-2.5.2014-k9.pkg 2 regex "Intel Mac OS X"
 anyconnect image disk0:/anyconnect-win-2.5.2014-k9.pkg 3 regex "Windows NT"
 anyconnect profiles ANYCONNECT_client_profile disk0:/ANYCONNECT_client_profile.xml
 anyconnect enable
 tunnel-group-list enable
group-policy DefaultRAGroup internal
```

```
group-policy DefaultRAGroup attributes
 dns-server value 116.90.227.65 116.90.227.15
 vpn-tunnel-protocol ikev1 l2tp-ipsec
group-policy GroupPolicy_ANYCONNECT internal
group-policy GroupPolicy_ANYCONNECT attributes
 wins-server none
 dns-server value 116.90.227.65
 vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client
 default-domain none
 webvpn
  anyconnect profiles value ANYCONNECT_client_profile type user
username peter password l5yHX4wBc.T9gS.R encrypted privilege 15
username ecnadmin password gh.xHwDJne2l75Sm encrypted
tunnel-group DefaultRAGroup general-attributes
 address-pool ECN_ADMIN_WIN
 default-group-policy DefaultRAGroup
tunnel-group DefaultRAGroup ipsec-attributes
 ikev1 pre-shared-key *****
tunnel-group DefaultRAGroup ppp-attributes
 authentication pap
 authentication ms-chap-v2
 authentication eap-proxy
tunnel-group ANYCONNECT type remote-access
tunnel-group ANYCONNECT general-attributes
 address-pool ECN_ADMIN_POOL
 default-group-policy GroupPolicy_ANYCONNECT
tunnel-group ANYCONNECT webvpn-attributes
 group-alias ANYCONNECT enable
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
!
service-policy global_policy global
privilege cmd level 3 mode exec command perfmon
privilege cmd level 3 mode exec command ping
privilege cmd level 3 mode exec command who
privilege cmd level 3 mode exec command logging
privilege cmd level 3 mode exec command failover
privilege cmd level 3 mode exec command packet-tracer
privilege show level 5 mode exec command import
privilege show level 5 mode exec command running-config
privilege show level 3 mode exec command reload
privilege show level 3 mode exec command mode
privilege show level 3 mode exec command firewall
privilege show level 3 mode exec command asp
privilege show level 3 mode exec command cpu
privilege show level 3 mode exec command interface
privilege show level 3 mode exec command clock
```

privilege show level 3 mode exec command dns-hosts
privilege show level 3 mode exec command access-list
privilege show level 3 mode exec command logging
privilege show level 3 mode exec command vlan
privilege show level 3 mode exec command ip
privilege show level 3 mode exec command ipv6
privilege show level 3 mode exec command failover
privilege show level 3 mode exec command asdm
privilege show level 3 mode exec command arp
privilege show level 3 mode exec command route
privilege show level 3 mode exec command ospf
privilege show level 3 mode exec command aaa-server
privilege show level 3 mode exec command aaa
privilege show level 3 mode exec command eigrp
privilege show level 3 mode exec command crypto
privilege show level 3 mode exec command ssh
privilege show level 3 mode exec command vpn-sessiondb
privilege show level 3 mode exec command vpn
privilege show level 3 mode exec command dhcpd
privilege show level 3 mode exec command blocks
privilege show level 3 mode exec command wccp
privilege show level 3 mode exec command dynamic-filter
privilege show level 3 mode exec command webvpn
privilege show level 3 mode exec command module
privilege show level 3 mode exec command uauth
privilege show level 3 mode exec command compression
privilege show level 3 mode configure command interface
privilege show level 3 mode configure command clock
privilege show level 3 mode configure command access-list
privilege show level 3 mode configure command logging
privilege show level 3 mode configure command ip
privilege show level 3 mode configure command failover
privilege show level 5 mode configure command asdm
privilege show level 3 mode configure command arp
privilege show level 3 mode configure command route
privilege show level 3 mode configure command aaa-server
privilege show level 3 mode configure command aaa
privilege show level 3 mode configure command crypto
privilege show level 3 mode configure command ssh
privilege show level 3 mode configure command dhcpd
privilege show level 5 mode configure command privilege
privilege clear level 3 mode exec command dns-hosts
privilege clear level 3 mode exec command logging
privilege clear level 3 mode exec command arp
privilege clear level 3 mode exec command aaa-server
privilege clear level 3 mode exec command crypto
privilege clear level 3 mode exec command dynamic-filter
privilege cmd level 3 mode configure command failover
privilege clear level 3 mode configure command logging
privilege clear level 3 mode configure command arp
privilege clear level 3 mode configure command crypto
privilege clear level 3 mode configure command aaa-server
prompt hostname context
no call-home reporting anonymous
hpm topN enable
Cryptochecksum:23d72f25795b265d71a83aeeb794835d

Dell PowerConnect 6224

```
1 : !Current Configuration:
2 : !System Description "PowerConnect 6224, 3.3.2.3, VxWorks 6.5"
3 : !System Software Version 3.3.2.3
4 : !Cut-through mode is configured as disabled
5 : !
6 : configure
7 : vlan database
8 : vlan 100,200,300,400,500
9 : vlan routing 200 1
10 : vlan routing 100 2
11 : vlan routing 300 3
12 : vlan routing 400 4
13 : vlan routing 500 5
14 : exit
15 : hostname "ecn-sw"
16 : stack
17 : member 1 1
18 : exit
19 : ip address 10.0.0.2 255.255.255.0
20 : ip default-gateway 10.0.0.1
21 : ip domain-name election.gov.np


22 : ip name-server 116.90.227.65
23 : logging file error
24 : lacp system-priority 120
25 : ip routing
26 : interface vlan 100
27 : name "Storage"
28 : routing
29 : ip address 10.0.1.2 255.255.255.0
30 : bandwidth 10000
31 : no ip proxy-arp
32 : ip mtu 9000
33 : exit
34 : interface vlan 200
35 : name "Management"
36 : routing
37 : ip address 10.0.2.2 255.255.255.0
38 : exit
39 : interface vlan 300
40 : name "LAN"
41 : routing
42 : ip address 10.0.3.2 255.255.255.0


43 : exit
44 : interface vlan 400
45 : name "CVLALAN"
46 : routing
47 : ip address 10.0.4.2 255.255.255.0
48 : bandwidth 10000
49 : ip local-proxy-arp
50 : ip mtu 1500
51 : exit
52 : interface vlan 500
53 : name "ULAN"
54 : routing
55 : ip address 10.0.5.2 255.255.255.0
56 : ip local-proxy-arp
57 : exit
58 : username "admin" password 5234ac46260f7a3ddd0860fed7813f1b level 15 encrypted
59 : username "peter" password b867103677e10f918172b15b1e515f59 level 15 encrypted
60 : !
61 : interface ethernet 1/g1
62 : channel-group 1 mode auto
63 : spanning-tree cost 20000
```

64 : spanning-tree mst 0 external-cost 20000
65 : exit
66 : !
67 : interface ethernet 1/g2
68 : channel-group 1 mode auto
69 : spanning-tree cost 20000
70 : spanning-tree mst 0 external-cost 20000
71 : exit
72 : !
73 : interface ethernet 1/g3
74 : switchport access vlan 500
75 : exit
76 : !
77 : interface ethernet 1/g4
78 : switchport access vlan 500
79 : exit
80 : !
81 : interface ethernet 1/g5
82 : description 'ECN1_SAN_G0'
83 : spanning-tree disable
84 : spanning-tree portfast

85 : mtu 9000
86 : switchport access vlan 100
87 : exit
88 : !
89 : interface ethernet 1/g6
90 : spanning-tree disable
91 : spanning-tree portfast
92 : switchport access vlan 300
93 : exit
94 : !
95 : interface ethernet 1/g7
96 : spanning-tree disable
97 : spanning-tree portfast
98 : exit
99 : !
100 : interface ethernet 1/g8
101 : description 'ECN2_SAN_G0'
102 : spanning-tree disable
103 : spanning-tree portfast
104 : mtu 9000
105 : switchport access vlan 100

106 : exit
107 : !
108 : interface ethernet 1/g9
109 : spanning-tree disable
110 : spanning-tree portfast
111 : switchport access vlan 300
112 : exit
113 : !
114 : interface ethernet 1/g10
115 : spanning-tree disable
116 : spanning-tree portfast
117 : exit
118 : !
119 : interface ethernet 1/g11
120 : spanning-tree disable
121 : spanning-tree portfast
122 : switchport access vlan 300
123 : exit
124 : !
125 : interface ethernet 1/g12
126 : spanning-tree disable

127 : spanning-tree portfast
128 : switchport access vlan 300

129 : exit
130 : !
131 : interface ethernet 1/g13
132 : spanning-tree disable
133 : spanning-tree portfast
134 : exit
135 : !
136 : interface ethernet 1/g14
137 : spanning-tree disable
138 : spanning-tree portfast
139 : switchport access vlan 200
140 : exit
141 : !
142 : interface ethernet 1/g15
143 : spanning-tree disable
144 : spanning-tree portfast
145 : exit
146 : !
147 : interface ethernet 1/g16

148 : spanning-tree disable
149 : spanning-tree portfast
150 : exit
151 : !
152 : interface ethernet 1/g17
153 : spanning-tree disable
154 : spanning-tree portfast
155 : exit
156 : !
157 : interface ethernet 1/g18
158 : spanning-tree disable
159 : spanning-tree portfast
160 : switchport access vlan 200
161 : exit
162 : !
163 : interface ethernet 1/g19
164 : spanning-tree disable
165 : spanning-tree portfast
166 : exit
167 : !
168 : interface ethernet 1/g20

169 : switchport access vlan 200
170 : exit
171 : !
172 : interface ethernet 1/g23
173 : switchport access vlan 200
174 : exit
175 : !
176 : interface ethernet 1/g24
177 : switchport access vlan 200
178 : exit
179 : !
180 : interface ethernet 1/xg1
181 : spanning-tree disable
182 : spanning-tree portfast
183 : mtu 9000
184 : switchport access vlan 100
185 : exit
186 : !
187 : interface ethernet 1/xg2
188 : spanning-tree disable
189 : spanning-tree portfast

190 : mtu 9000
191 : switchport access vlan 100
192 : exit
193 : !

```
194 : interface ethernet 1/xg3
195 : channel-group 2 mode auto
196 : lacp port-priority 247
197 : mtu 9000
198 : exit
199 : !
200 : interface ethernet 1/xg4
201 : channel-group 2 mode auto
202 : lacp port-priority 247
203 : mtu 9000
204 : exit
205 : !
206 : interface port-channel 1
207 : description 'to ASA5520 firewall'
208 : switchport mode general
209 : switchport general allowed vlan add 100,300,400 tagged
210 : exit


211 : !
212 : interface port-channel 2
213 : description 'to 8024 SAN switch'
214 : switchport mode general
215 : switchport general allowed vlan add 100,200,300,400,500 tagged
216 : exit
217 : exit
```

Dell PowerConnect 8024F

```
!Current Configuration:
!System Description "Powerconnect 8024F, 4.2.0.4, VxWorks 6.6"
!System Software Version 4.2.0.4
!Cut-through mode is configured as disabled
!
configure
vlan database
vlan 100,200,300,400,500
vlan routing 1 1
vlan routing 100 2
vlan routing 200 3
vlan routing 300 4
vlan routing 400 5
vlan routing 500 6
exit
stack
member 1 2    ! PC8024F
exit
interface out-of-band
ip address 10.0.10.4 255.255.255.0 10.0.10.1
exit

lacp system-priority 120
ip routing
ip default-gateway 10.0.0.1
ip route 0.0.0.0 0.0.0.0 10.0.0.1 253
interface vlan 1
ip address 10.0.0.3 255.255.255.0
exit
interface vlan 100
ip address 10.0.1.3 255.255.255.0
bandwidth 100000
no ip proxy-arp
ip mtu 9000
exit
interface vlan 200
ip address 10.0.2.3 255.255.255.0
bandwidth 100000
exit
interface vlan 300
ip address 10.0.3.3 255.255.255.0
bandwidth 100000
exit

interface vlan 400
ip address 10.0.4.3 255.255.255.0
bandwidth 100000
ip local-proxy-arp
exit
interface vlan 500
ip address 10.0.5.3 255.255.255.0
bandwidth 100000
ip local-proxy-arp
exit
username "admin" password 5234ac46260f7a3ddd0860fed7813f1b privilege 15 encrypted
username "peter" password b867103677e10f918172b15b1e515f59 privilege 15 encrypted
iscsi cos vpt 5
!
interface Te1/0/1
spanning-tree disable
spanning-tree portfast
mtu 9216
switchport access vlan 100
exit
!

interface Te1/0/2
spanning-tree disable
spanning-tree portfast
```

```
mtu 9216
switchport access vlan 100
exit
!
interface Te1/0/3
spanning-tree disable
spanning-tree portfast
mtu 9216
switchport access vlan 100
exit
!
interface Te1/0/4
spanning-tree disable
spanning-tree portfast
mtu 9216
switchport access vlan 100
exit
!

interface Te1/0/5
spanning-tree disable
spanning-tree portfast
mtu 9216
switchport access vlan 100
exit
!
interface Te1/0/6
spanning-tree disable
spanning-tree portfast
mtu 9216
switchport access vlan 100
exit
!
interface Te1/0/7
description 'ECN1 SAN F0'
spanning-tree disable
spanning-tree portfast
spanning-tree cost 2000
mtu 9216
switchport access vlan 100

exit
!
interface Te1/0/8
spanning-tree disable
spanning-tree portfast
mtu 9216
switchport access vlan 300
exit
!
interface Te1/0/9
spanning-tree disable
spanning-tree portfast
mtu 9216
switchport general allowed vlan add 500
switchport general allowed vlan remove 1
switchport mode general
exit
!
interface Te1/0/10
description 'ECN2 SAN F0'
spanning-tree disable

spanning-tree portfast
mtu 9216
switchport access vlan 100
exit
!
interface Te1/0/11
spanning-tree disable
spanning-tree portfast
```

```
mtu 9216
switchport access vlan 300
exit
!
interface Te1/0/12
spanning-tree disable
spanning-tree portfast
mtu 9216
switchport general allowed vlan add 500
switchport general allowed vlan remove 1
switchport mode general
exit
!

interface Te1/0/13
description 'Backup Server F0'
spanning-tree disable
spanning-tree portfast
mtu 9216
switchport access vlan 100
exit
!
interface Te1/0/14
spanning-tree disable
spanning-tree portfast
mtu 9216
switchport access vlan 300
exit
!
interface Te1/0/15
spanning-tree disable
spanning-tree portfast
mtu 9216
switchport access vlan 300
exit

!
interface Te1/0/16
spanning-tree disable
spanning-tree portfast
mtu 9216
switchport access vlan 400
exit
!
interface Te1/0/17
spanning-tree disable
spanning-tree portfast
mtu 9216
switchport access vlan 100
exit
!
interface Te1/0/18
spanning-tree disable
spanning-tree portfast
mtu 9216
switchport access vlan 300
exit

!
interface Te1/0/19
channel-group 2 mode active
description 'Trunk 1 to 6224'
spanning-tree portfast
mtu 9216
exit
!
interface Te1/0/20
channel-group 2 mode active
description 'Trunk 2 to 6224'
spanning-tree portfast
mtu 9216
```

```
exit
!
interface Te1/0/21
spanning-tree disable
spanning-tree portfast
mtu 9216
switchport access vlan 200
exit

!
interface Te1/0/22
spanning-tree portfast
mtu 9216
switchport access vlan 200
exit
!
interface Te1/0/23
spanning-tree disable
spanning-tree portfast
mtu 9216
switchport access vlan 500
exit
!
interface Te1/0/24
spanning-tree disable
spanning-tree portfast
mtu 9216
switchport access vlan 500
exit
!

interface port-channel 1
mtu 9216
exit
!
interface port-channel 2
description 'To core switch'
switchport general allowed vlan add 100,200,300,400,500 tagged
switchport mode general
mtu 9216
exit
!
interface port-channel 3
mtu 9216
exit
!
! Interface port-channels 4-127 as port-channel 128
!
interface port-channel 128
mtu 9216
exit
exit
```

Management Server

Exports (/etc/exports)

```
/opt/share/iso          10.0.0.0/16(insecure,rw,sync,no_root_squash,no_all_squash)
/opt/share/ha           10.0.0.0/16(insecure,rw,sync,no_root_squash,no_all_squash)
```

Crontab

```
*/5 * * * * flock -n /var/run/upsload.lock -c /root/scripts/ups_load_check.sh >/dev/null 2>&1
@weekly /root/scripts/xe_dump_pool.sh
```

Bacula File and Storage Daemons

```
#
# Default  Bacula File Daemon Configuration file
#
#  For Bacula release 5.2.7 (02 June 2012) -- redhat Enterprise release
#
# There is not much to change here except perhaps the
# File daemon Name to
#

#
# List Directors who are permitted to contact this File daemon
#
Director {
  Name = bacula-dir
  Password = "electi0n"
}

#
# Restricted Director, used by tray-monitor to get the
#   status of the file daemon
#
Director {
  Name = bacula-mon
  Password = "electi0n"
  Monitor = yes
}

#
# "Global" File daemon configuration specifications
#
FileDaemon {                          # this is me
  Name = bacula-fd
  FDport = 9102                  # where we listen for the director
  WorkingDirectory = /var/spool/bacula
  Pid Directory = /var/run
  Maximum Concurrent Jobs = 20
}

# Send all messages except skipped files back to Director
Messages {
  Name = Standard
  director = bacula-dir = all, !skipped, !restored
}


#
# Default Bacula Storage Daemon Configuration file
#
#  For Bacula release 5.2.4 (18 January 2012) -- redhat Enterprise release
#
# You may need to change the name of your tape drive
#   on the "Archive Device" directive in the Device
#   resource.  If you change the Name and/or the
#   "Media Type" in the Device resource, please ensure
```

```
#   that dird.conf has corresponding changes.
#

Storage {                       # definition of myself
  Name = TL2000
  SDPort = 9103                 # Director's port
  WorkingDirectory = "/var/spool/bacula"
  Pid Directory = "/var/run"
  Maximum Concurrent Jobs = 20
}

#
# List Directors who are permitted to contact Storage daemon
#
Director {
  Name = bacula-dir
  Password = "electi0n"
}

#
# Restricted Director, used by tray-monitor to get the
#   status of the storage daemon
#
Director {
  Name = bacula-mon
  Password = "electi0n"
  Monitor = yes
}

#
# Note, for a list of additional Device templates please
#  see the directory <bacula-source>/examples/devices
# Or follow the following link:
#  http://bacula.svn.sourceforge.net/viewvc/bacula/trunk/bacula/examples/devices/
#

#
# Devices supported by this Storage daemon
# To connect, the Director's bacula-dir.conf must have the
#  same Name and MediaType.
#
# DELL TL2000 autochanger device with two drives
#
Autochanger {
  Name = AC2000
  Device = ML2000-LTO5-0
  Device = ML2000-LTO5-1
  Changer Command = "/usr/libexec/bacula/mtx-changer %c %o %S %a %d"
  Changer Device = /dev/sg1
}

Device {
  Name = ML2000-LTO5-0              #
  Drive Index = 0
  Media Type = LTO5
  Archive Device = /dev/nst0
  AutomaticMount = yes              # when device opened, read it
  AlwaysOpen = yes
  RemovableMedia = yes
  RandomAccess = no
  AutoChanger = yes
  Label Media = no
#Maximum Changer Wait = 600
#Maximum Rewind Wait = 600
#Maximum Open Wait = 600
#  #
#  # Enable the Alert command only if you have the mtx package loaded
#  # Note, apparently on some systems, tapeinfo resets the SCSI controller
#  #  thus if you turn this on, make sure it does not reset your SCSI
#  #  controller.  I have never had any problems, and smartctl does
#  #  not seem to cause such problems.
```

```
# #
#  Alert Command = "sh -c 'tapeinfo -f /dev/sg0 |grep TapeAlert|cat'"
#  If you have smartctl, enable this, it has more info than tapeinfo
  Alert Command = "sh -c 'smartctl -H -l error /dev/sg0'"
Maximum Spool Size =  214748364800
Maximum Job Spool Size = 214748364800
Spool Directory = /opt/bacula/spool
Maximum Concurrent Jobs = 2
Maximum Network Buffer Size = 65536
Maximum File Size = 5368709120

}

Device {
  Name = ML2000-LTO5-1             #
  Drive Index = 1
  Media Type = LTO5
  Archive Device = /dev/nst1
  AutomaticMount = yes             # when device opened, read it
  AlwaysOpen = yes
  RemovableMedia = yes
  RandomAccess = no
  AutoChanger = yes
  Label Media = no
#Maximum Changer Wait = 600
#Maximum Rewind Wait = 600
#Maximum Open Wait = 600
#  # Enable the Alert command only if you have the mtx package loaded
#  Alert Command = "sh -c 'tapeinfo -f /dev/sg2 |grep TapeAlert|cat'"
#  If you have smartctl, enable this, it has more info than tapeinfo
  Alert Command = "sh -c 'smartctl -H -l error /dev/sg2'"

Maximum Spool Size = 214748364800
Maximum Job Spool Size = 214748364800
Spool Directory =  /opt/bacula/spool
Maximum Concurrent Jobs = 2
Maximum Network Buffer Size = 65536
Maximum File Size = 5368709120
}


#
# Send all messages to the Director,
# mount messages also are sent to the email address
#
Messages {
  Name = Standard
  director = bacula-dir = all
}
```

Bacula Server

Mounts (/etc/fstab)

```
10.0.1.40:/backups /mnt/backups cifs credentials=/root/.smbpasswd,uid=ecnadmin,gid=ecnadmin  0 0

10.0.1.19:/media/sdfs-pool-01/nfs /mnt/backupsXVA nfs defaults  0 0
```

Bacula Director Configuration

```
#
# Default Bacula Director Configuration file
#
#  The only thing that MUST be changed is to add one or more
#   file or directory names in the Include directive of the
#   FileSet resource.
#
#  For Bacula release 5.2.5 (26 January 2012) -- redhat Enterprise release
```

```
#
#  You might also want to change the default email address
#   from root to your address.  See the "mail" and "operator"
#   directives in the Messages resource.
#

Director {                      # define myself
  Name = bacula-dir
  DIRport = 9101                # where we listen for UA connections
  QueryFile = "/etc/bacula/query.sql"
  WorkingDirectory = "/var/spool/bacula"
  PidDirectory = "/var/run"
  Maximum Concurrent Jobs = 10
  Password = "electi0n"         # Console password
  Messages = Daemon
}
#Jobs
@/etc/bacula/bacula-jobs.inc
#Clients and file sets - from where and what
@/etc/bacula/bacula-clients.inc
#Schedules - when
@/etc/bacula/bacula-schedule.inc
#Storage resources - to where do we back up
@/etc/bacula/bacula-storage.inc



# Generic catalog service
Catalog {
  Name = MyCatalog
# Uncomment the following line if you want the dbi driver
# dbdriver = "dbi:postgresql"; dbaddress = 127.0.0.1;
dbname = "bacula"; dbuser = "bacula"; dbpassword = "";
}

# Reasonable message delivery -- send most everything to email address
#  and to the console
Messages {
  Name = Standard
#
# NOTE! If you send to two email or more email addresses, you will need
#  to replace the %r in the from field (-f part) with a single valid
#  email address in both the mailcommand and the operatorcommand.
#  What this does is, it sets the email address that emails would display
#  in the FROM field, which is by default the same email as they're being
#  sent to.  However, if you send email to more than one address, then
#  you'll have to set the FROM address manually, to a single address.
#  for example, a 'no-reply@mydomain.com', is better since that tends to
#  tell (most) people that its coming from an automated source.

#
  mailcommand = "/usr/sbin/bsmtp -h localhost -f \"\(Bacula\) \<%r\>\" -s \"Bacula: %t %e of %c %l\" %r"
  operatorcommand = "/usr/sbin/bsmtp -h localhost -f \"\(Bacula\) \<%r\>\" -s \"Bacula: Intervention needed for %j\" %r"
  mail = admin@election.gov.np  = all, !skipped
  operator = root@localhost = mount
  console = all, !skipped, !saved
#
# WARNING! the following will create a file that you must cycle from
#          time to time as it will grow indefinitely. However, it will
#          also keep all your messages if they scroll off the console.
#
  append = "/var/log/bacula/bacula.log" = all, !skipped
  catalog = all
}


#
# Message delivery for daemon messages (no job).
Messages {
  Name = Daemon
```

```
  mailcommand = "/usr/sbin/bsmtp -h localhost -f \"\(Bacula\) \<%r\>\" -s \"Bacula daemon message\" %r"
  mail = admin@election.gov.np = all, !skipped
  console = all, !skipped, !saved
  append = "/var/log/bacula/bacula.log" = all, !skipped
}

@/etc/bacula/bacula-pool.inc

#
# Restricted console used by tray-monitor to get the status of the director
#
Console {
  Name = bacula-mon
  Password = "electi0n"
  CommandACL = status, .status
}
```

Bacula Director Include files

```
# From WHERE and WHAT do we backup

# Files for CVLA backup
FileSet {
  Name = "CVLA Set"
  Enable VSS = no
  Include {
    Options {
      signature = md5
    }
    File = "K:/"
  }
  Exclude {
    File = "K:/Coldbackups"
  }
}
# List of files to be backed up on bacula.election.gov.np
FileSet {
  Name = "Full Set"
  Include {
    Options {
      signature = MD5
    }
#
#  Put your list of files here, preceded by 'File =', one per line
#    or include an external list with:
#
#    File = <file-name
#
#  Note: / backs up everything on the root partition.
#    if you have other partitions such as /usr or /home
#    you will probably want to add them too.
#
#  By default this is defined to point to the Bacula binary
#    directory to give a reasonable FileSet to backup to
#    disk storage during initial testing.
#
    File = /
    File = /home
    File = /boot
    File = /opt
  }

#
# If you backup the root directory, the following two excluded
#   files can be useful
#
  Exclude {
    File = /var/spool/bacula
    File = /tmp
    File = /proc
```

```
   File = /tmp
   File = /.journal
   File = /.fsck
   File = /opt/bacula/spool
  }
}


# This is the backup of the catalog
FileSet {
  Name = "Catalog"
  Include {
    Options {
     signature = MD5
    }
    File = "/var/spool/bacula/bacula.sql"
  }
}

# Client (File Services) to backup
Client {
  Name = bacula-fd
  Address = localhost
  FDPort = 9102
  Catalog = MyCatalog
  Password = "electi0n"         # password for FileDaemon
  File Retention = 180 days           # 30 days
  Job Retention = 12 months           # six months
  AutoPrune = yes                     # Prune expired Jobs/Files
  Maximum Concurrent Jobs = 10
}

# Management Server Client
Client {
                Name = mgmt-fd
                Address = 10.0.1.50
                FDPort = 9102
                Catalog = MyCatalog
                Password = "electi0n"
                File Retention = 180 days
                Job Retention = 12 months
                AutoPrune = yes
                Maximum Concurrent Jobs = 20
}

# CVLA Server Client
Client {
        Name = cvla-fd
        Address = 10.0.1.13
        FDPort = 9102
        Catalog = MyCatalog
        Password = "electi0n"
        File Retention = 180 days
        Job Retention = 12 months
        AutoPrune = yes
                Maximum Concurrent Jobs = 20
}

# CVLA Backup Management Server Client
Client {
        Name = cvlabackup-fd
        Address = 10.0.1.17
        FDPort = 9102
        Catalog = MyCatalog
        Password = "electi0n"
        File Retention = 180 days
        Job Retention = 12 months
        AutoPrune = yes
                Maximum Concurrent Jobs = 20
}
```

```
#Backup VHD images of VMs
FileSet {
  Name = "PHD"
  Include {
    Options {
     signature = MD5
    }
     File = /mnt/backups/LatestOfEach/
    }
                Exclude {
                }
}

#Backup XVA images of VMs
FileSet {
  Name = "SDFS"
  Include {
    Options {
     signature = MD5
    }
     File = /mnt/backupsXVA/
    }
                Exclude {
                }
}

#Backup CVLA DB files.
FileSet {
  Name = "CVLADB"
  Include {
    Options {
     signature = MD5
    }
     File = d:/
    }
                Exclude {
                }
}
# JOB definitions (includes Fileset, Client  Schedule, Pool):

JobDefs {
  Name = "DefaultJob"
  Type = Backup
  Level = Incremental
  Client = bacula-fd
  FileSet = "Full Set"
  Schedule = "WeeklyCycle"
  Storage = TL2000
  Messages = Standard
  Pool = Weekly
  Priority = 10
  Write Bootstrap = "/var/spool/bacula/%c.bsr"
}


#
# Define the main nightly save backup job
#   By default, this job will back up to disk in /tmp
Job {
  Name = "BackupClient1"
  JobDefs = "DefaultJob"
}

# Backup the catalog database (after the nightly save)
Job {
  Name = "BackupCatalog"
  JobDefs = "DefaultJob"
  Level = Full
  FileSet="Catalog"
  Schedule = "WeeklyCycleAfterBackup"
```

```
  # This creates an ASCII copy of the catalog
  # Arguments to make_catalog_backup.pl are:
  #  make_catalog_backup.pl <catalog-name>
  RunBeforeJob = "/usr/libexec/bacula/make_catalog_backup.pl MyCatalog"
  # This deletes the copy of the catalog
  RunAfterJob  = "/usr/libexec/bacula/delete_catalog_backup"
  Write Bootstrap = "/var/spool/bacula/%n.bsr"
  Priority = 11                   # run after main backup
}

#
# Standard Restore template, to be changed by Console program
#  Only one such job is needed for all Jobs/Clients/Storage ...
#
Job {
  Name = "RestoreFiles"
  Type = Restore
  Client=bacula-fd
  FileSet="Full Set"
  Storage = File
  Pool = Default
  Messages = Standard
  Where = /tmp/bacula-restores
}

Job {
                Name = "VHDBackup"
                Type = Backup
                Client = bacula-fd
                FileSet = "PHD"
                Schedule = "PHD_Weekly"
                Storage = TL2000
                Messages = Standard
                Priority = 1
#               SpoolData = yes
                Pool = Monthly
                Maximum Concurrent Jobs = 6
}


Job {
                Name = "XVABackup"
                Type = Backup
                Client = bacula-fd
                FileSet = "SDFS"
                Schedule = "ECNMonthly"
                Storage = TL2000
                Messages = Standard
                Priority = 1
#               SpoolData = yes
                Pool = Monthly
                Maximum Concurrent Jobs = 6
                Reschedule On Error = yes
                Reschedule Interval = 3 hours
                Reschedule Times = 3
}

Job {
                Name = "MgmtBackup"
                Type = Backup
                Client = mgmt-fd
                FileSet = "Full Set"
      Schedule = "ECNMonthly"
      Storage = TL2000
      Messages = Standard
      Priority = 1
#       SpoolData = yes
                Pool = Monthly
                Reschedule On Error = yes
                Reschedule Interval = 3 hours
                Reschedule Times = 3
```

```
}

Job {
      Name = "CVLABackup"
      Type = Backup
      Client = cvla-fd
      FileSet = "CVLA Set"
      Schedule = "ECNMonthly"
      Storage = TL2000
      Messages = Standard
      Priority = 1
#       SpoolData = yes
      Pool = Monthly
            Client Run Before Job = "\"C:/Program Files/Bacula/working/CVLAstart.cmd\""
            Client Run After Job =  "\"C:/Program Files/Bacula/working/CVLAend.cmd\""
            Maximum Concurrent Jobs = 6
            Reschedule On Error = yes
            Reschedule Interval = 3 hours
            Reschedule Times = 3

}
# WHERE to back up TO (which tapes)


# Default pool definition
Pool {
  Name = Default
  Pool Type = Backup
  Recycle = yes                 # Bacula can automatically recycle Volumes
  AutoPrune = yes                 # Prune expired volumes
  Volume Retention = 365 days       # one year
  LabelFormat="Default-"
}

# File Pool definition
Pool {
  Name = File
  Pool Type = Backup
  Recycle = yes                 # Bacula can automatically recycle Volumes
  AutoPrune = yes                 # Prune expired volumes
  Volume Retention = 365 days       # one year
  Maximum Volume Bytes = 1G        # Limit Volume size to something reasonable
  Maximum Volumes = 10            # Limit number of Volumes in Pool
  LabelFormat = "File-"
}


# Scratch pool definition
Pool {
  Name = Scratch
  Pool Type = Backup
}

# ECN Backup Schedule

Pool {
  Name = Monthly
  Pool Type = Backup
  Recycle = yes                 # Bacula can automatically recycle Volumes
  AutoPrune = yes                 # Prune expired volumes
  Volume Retention = 460 days       # one year and 3 months
  Maximum Volumes = 12            # Limit number of Volumes in Pool
#  LabelFormat = "Monthly-"
}

Pool {
  Name = Weekly
  Pool Type = Backup
  Recycle = yes                 # Bacula can automatically recycle Volumes
  AutoPrune = yes                 # Prune expired volumes
```

```
  Volume Retention = 3 months       # one year and 3 months
  Maximum Volumes = 6               # Limit number of Volumes in Pool
#  LabelFormat = "Weekly-"
}

Pool {
  Name = Daily
  Pool Type = Backup
  Recycle = yes                     # Bacula can automatically recycle Volumes
  AutoPrune = yes                   # Prune expired volumes
  Volume Retention = 5 weeks        # one year and 3 months
  Maximum Volumes = 3               # Limit number of Volumes in Pool
#  LabelFormat = "Daily-"
}

# WHEN to back up

#
# When to do the backups, full backup on first sunday of the month,
#  differential (i.e. incremental since full) every other sunday,
#  and incremental backups other days
Schedule {
  Name = "WeeklyCycle"
  Run = Full 1st sun at 23:05
  Run = Differential 2nd-5th sun at 23:05
  Run = Incremental mon-sat at 23:05
}

# This schedule does the catalog. It starts after the WeeklyCycle
Schedule {
  Name = "WeeklyCycleAfterBackup"
  Run = Full sun-sat at 06:00
}

Schedule {
  Name = "ECNMonthly"
  Run = Level=Full Pool=Monthly on 1 at 20:00
  Run = Level=Differential FullPool=Monthly Pool=Weekly 2nd-5th sat at 20:00
  Run = Level=Incremental FullPool=Monthly DifferentialPool=Weekly Pool=Daily sun-fri at 20:00
}
Schedule {
   Name = "PHD_Weekly" # Backup latest VMs on a weekly basis
   Run = Level = Full Pool = Monthly on 1st sat at 20:00
   Run = Level = Full Pool = Weekly 2nd-5th sat at 20:00
}

# To WHAT device do we back up

# Definition of file storage device
Storage {
  Name = File
# Do not use "localhost" here
  Address = 10.0.1.51               # N.B. Use a fully qualified name here
  SDPort = 9103
  Password = "electi0n"
  Device = FileStorage
  Media Type = File
}



# Definition of LTO5 tape storage device
Storage {
  Name = TL2000
#  Do not use "localhost" here
  Address = 10.0.1.50               # N.B. Use a fully qualified name here
  SDPort = 9103
  Password = "electi0n"         # password for Storage daemon
  Device = AC2000                   # must be same as Device in Storage daemon
  Media Type = LTO5                 # must be same as MediaType in Storage daemon
  Autochanger = yes                 # enable for autochanger device
```

```
  Maximum Concurrent Jobs = 20                    # 2 drives in the tape library
}

# Definition of DVD storage device
#Storage {
#  Name = "DVD"
#  Do not use "localhost" here
#  Address = localhost                # N.B. Use a fully qualified name here
#  SDPort = 9103
#  Password = "@@SD_PASSWORD@@"
#  Device = "DVD Writer"
#  MediaType = "DVD"
#}
```

Scripts

CVLA DB - Database Backup (AutoSnapshot)

C:\Program Files\Bacula\working\CVLAstart.cmd

```
"C:\Program Files\EqualLogic\bin\ASMCLI" -smart  -volume="D:\" -
shadowtype=transportable -backuptype=copy -smartcopytype=snapshot -
keepcount=1 -noemail
"C:\Program Files\EqualLogic\bin\ASMCLI" -mount -volume="D:\" -location="K:\" -
uselatest
exit 0
```

C:\Program Files\Bacula\working\CVLAend.cmd

```
"C:\Program Files\EqualLogic\bin\ASMCLI" -unmount  -location="K:\" -deletesnap
exit 0
```

Management

/root/scripts/ups_load_check.sh

```
#!/bin/bash
#UPS settings
HOSTS="10.0.2.41 10.0.2.42 10.0.2.43 10.0.2.44"
COMMUNITY="public"
#minimal voltage sufficient for your UPS model to not switch to batteries
VOLTS_MIN=160
#minimal runtime you need to properly shutdown all VMs and Xen hosts
MINUTES_MIN=15
#administrator email (better if it's crossposted to sms in case shutdown is initiated)
EMAIL="admin@election.gov.np"
SNMPGET=`which snmpget`
LOW_VOLT=999
LOW_RUN=99999

LOGFILE=/var/log/ups_shutdown.log

#LOG functions
f_LOG() {
echo "`date`:$@" >> $LOGFILE
}

f_INFO() {
```

```
echo "$@"
f_LOG "INFO: $@"
}

f_WARNING() {
echo "$@"
f_LOG "WARNING: $@"
}


for HOST in `echo $HOSTS`
do
        SNMPOPTS="-Ov -Oq -v1 -r10 -t2 -c $COMMUNITY $HOST"
        #Input voltage OID
        OID_VOLTS_IN=".1.3.6.1.4.1.318.1.1.1.3.2.1.0"
        #Battery runtime remaining OID
        OID_RUNTIME="1.3.6.1.4.1.318.1.1.1.2.2.3.0"
        VALUE_VOLTS_IN=`$SNMPGET $SNMPOPTS $OID_VOLTS_IN`
        VALUE_RUNTIME=`${SNMPGET} ${SNMPOPTS} $OID_RUNTIME`
        #SNMP runtime value reported as D:H:M:S.00
        #let's convert it into minutes for convenience
        OFS="$IFS"
        IFS=":"
        arr=( $VALUE_RUNTIME )
        IFS="$OFS"
        DAYS=${arr[0]}
        HOURS=${arr[1]}
        MINUTES=${arr[2]}
        MINUTES_LEFT=$((10#$DAYS*24*60+10#$HOURS*60+10#$MINUTES))
   if [ $VALUE_VOLTS_IN -lt $LOW_VOLT ]
        then
                LOW_VOLT=$VALUE_VOLTS_IN
   fi
   if [ $MINUTES_LEFT -lt $LOW_RUN ]
        then
                LOW_RUN=$MINUTES_LEFT
   fi
done

BATTERY=`${SNMPGET} ${SNMPOPTS} 1.3.6.1.4.1.318.1.1.1.4.1.1.0`

f_INFO "Runtime:$LOW_RUN Volt:$LOW_VOLT Battery: $BATTERY"

if [ $LOW_VOLT -lt $VOLTS_MIN ]
  then
   echo "Input voltage is too low ($LOW_VOLT). $LOW_RUN minutes of UPS runtime
remaining." | mail -s "UPS: Power failure report" $EMAIL
```

```
   f_WARNING "Input voltage is too low ($LOW_VOLT). $LOW_RUN minutes of UPS
runtime remaining. Running on 2=Online, 3=Battery: $BATTERY"
   sleep 3
   if [ $LOW_RUN -lt $MINUTES_MIN ] && [$BATTERY -eq 3 ]
     then
     echo "Warning! $LOW_RUN minutes of UPS runtime remaining - shutdown
initiated." | mail -s "UPS: Xenserver pool shutdown initiated." $EMAIL
     f_WARNING "Warning! $LOW_RUN minutes of UPS runtime remaining -
shutdown initiated."
     #let the message pass through:
     sleep 3
     # Run system shutdown script if not already running
     flock -n /var/run/ups.lock -c /root/scripts/ups_system_shutdown.sh
  fi
fi
```

/root/scripts/Ups_system_shutdown.sh

```
#!/bin/bash
#exit

IFS=","
XENHOST="10.0.2.10"
XENUSER="root"
XENPWD="electi0n"
LOG="/var/log/ups_shutdown.log"

LOGFILE=/var/log/ups_shutdown.log

#LOG functions
f_LOG() {
echo "`date`:$@" >> $LOGFILE
}

f_INFO() {
echo "$@"
f_LOG "INFO: $@"
}

f_WARNING() {
echo "$@"
f_LOG "WARNING: $@"
}

f_INFO "Shutdown sequence started"
```

```
###Shutdown HA###
f_INFO " Disabling HA on pool master"
xe -s $XENHOST -u $XENUSER -pw $XENPWD pool-ha-disable
if [ $? -eq 0 ]; then
        f_INFO Pool HA disabled successfully"
else
        f_WARNING "Disabling Pool HA failed!"
fi
###
f_INFO "Starting shutdown of all VMs"
for VM in `xe -s $XENHOST -u $XENUSER -pw $XENPWD vm-list is-control-
domain=false power-state=running params=uuid --minimal`
do
        f_INFO "Shutting down VM: $VM"
        xe -s $XENHOST -u $XENUSER -pw $XENPWD vm-shutdown vm=$VM
        if [ $? -eq 0 ]; then
                f_INFO "$VM shutdown successfully"
        else
                f_WARNING "Graceful shut down failed. Force Shutdown for VM:
$VM"
                xe -s $XENHOST -u $XENUSER -pw $XENPWD vm-shutdown vm=$VM
force=true
        fi
done
f_INFO "Forcefully shutting down all suspended VMs"
for VM in `xe -s $XENHOST -u $XENUSER -pw $XENPWD vm-list is-control-
domain=false power-state=suspended params=uuid --minimal`
do
        f_INFO " Force Shutdown for VM: $VM"
                xe -s $XENHOST -u $XENUSER -pw $XENPWD vm-shutdown vm=$VM
force=true
        fi
done
f_INFO "Shutting down all pool members"
###get uuid of pool master - it must be the very last to shut down
MASTER_UUID=`xe -s $XENHOST -u $XENUSER -pw $XENPWD pool-list
params=master --minimal`

###enumerate of all xen hosts in the pool except master
for HOST in `xe -s $XENHOST -u $XENUSER -pw $XENPWD host-list params=uuid --
minimal`
do
   if [ $HOST != $MASTER_UUID ]
   then
      ###(uncomment following line to perform actual shutdown)
      f_INFO "Shutting down pool member: $HOST"
      xe host-disable host=$HOST
```

```
      xe host-shutdown host=$HOST
   if [ $? -eq 0 ]; then
         f_INFO "Shut down pool member: $HOST successfully"
   else
         f_WARNING "Shutting down pool member: $HOST failed"
   fi
done



###finally shutdown pool master
f_INFO "Shutting down pool master: $MASTER_UUID"
xe -s $XENHOST -u $XENUSER -pw $XENPWD host-disable host=$MASTER_UUID
xe -s $XENHOST -u $XENUSER -pw $XENPWD host-shutdown host=$MASTER_UUID
if [ $? -eq 0 ]; then
         f_INFO "Shut down pool master $HOST successfully"
   else
         f_WARNING "Shutting down pool master: $HOST failed"
   fi
###Shutdown SAN###
/usr/bin/expect -c 'expect "\n" { eval spawn telnet 10.0.2.30; expect "ogin:"; send
"grpadmin\n"; expect "assword:"; send "electi0n\n";expect "ECNHQ>";send
"shutdown\r\n";expect "\[no\]"; send "yes\r\n";}'
if [ $? -eq 0 ]; then
         f_INFO "Shutdown SAN"
fi
##Finally shutdown self
f_INFO "Shutting down self"
/sbin/shutdown -h now
```

/root/scripts/xe_pool_dump.sh

```
xe pool-dump-database file-name=/opt/bacula/local_backup_data/xenpool/`date
'+pool_database-%d_%m_%y'` -s 10.0.2.10 -u root -pw electi0n
```