Global Information Assurance Certification Paper

Securing an HP-UX 11.11 Cluster

Steve Ball
GIAC Certified UNIX Security Administrator (GCUX) Practical Assignment
2.0
December 13, 2003

Description

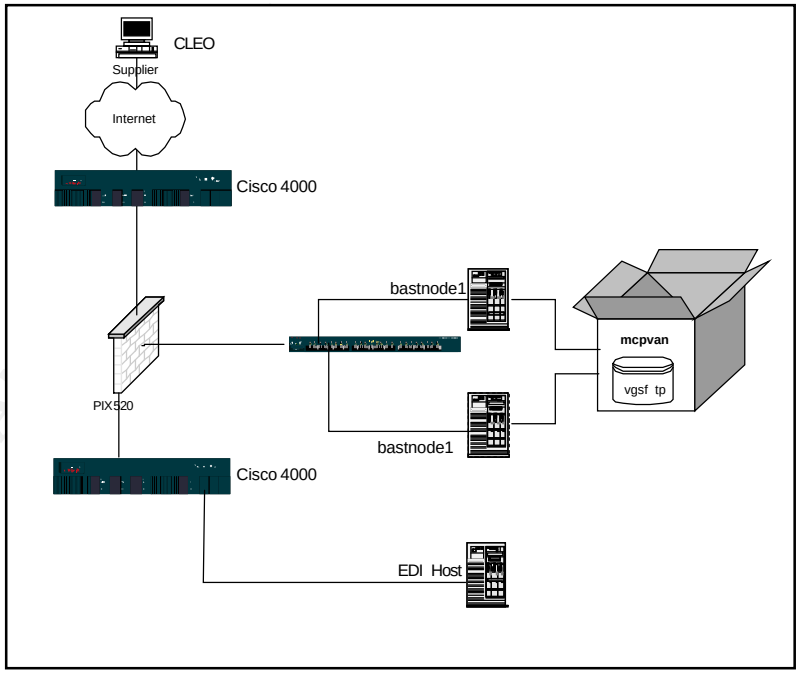
A request has been approved for the IT staff to provide a secure and highly available proxy server to pass secure FTP requests for secure EDI mailbox data exchange.

The server will be accessible from the Internet for approved trading partners using a third party product from Cleo Corporation, Cleo FTP Client Software. The software will utilize authentication and encryption to provide the secure connection. The installation and configuration of this product in not in the direct scope, although, the securing of the used TCP services through the proxy server are.

The system will be installed with minimum operating system requirements and various tools will be deployed to monitor and prevent the system from being compromised by unauthorized users. The EDI application is business critical, for this reason the proxy server must be highly available and redundant.

Infrastructure Overview

The following diagram represents the overall infrastructure of the proxy landscape design. All components are redundant, only bastnode1 and bastnode2 are in scope.



Hardware

- 2 HP9000/SD64000 (Superdome) partitions

- Two PA-RISC 875 Mhz processors
- 4 GB memory
- One XP1024 13.5GB Disk dedicated
- One XP1024 13.5GB Disk shared for the cluster
- Two HP PCI 1000Base-SX Network Interface Card in each Partition

Operating System

- HP-UX 11.11 Mission Critical June 2003 Release

Applications

Application	Release	Purpose
Security Patch Check	B.01.01	Security Patch Check is an HP-UX tool that will scan the system against a security patch list database. Any security patches required by the system will be identified.
HP-UX Secure Shell	A.03.61.001	Provide ssh access for administrators and to tunnel system logs out.
Tripwire	1.3.5	Will be used to provide a snapshot list of the system files. The base listing will be checked against the current system each hour. Any finding will be placed into the syslog.
HP IPFilter/9000	A.03.05.05	IP filter is a stateful firewall for filtering IP packets. This product is used not only to provide an extra layer of protection, but to also control the IP packets passed between the nodes in the cluster.
lsof	4.69	Will be used to list open sockets and investigate processes. Download the source from this site and compile it. The depot file is for 32 bit systems only.
logrotate	2.5	Will be used to manage the size of system logs.
CISscan		Will be used to assist in evaluating the hardening of the system.
hp_checkperms		Will be used to assist in evaluating the hardening of the system.
TCP_Wrappers	B.11.11.01.001	Will be used to provide access control to requested TCP services.

Risk Analysis

The customer of this system has their business depending on it. The risks are high and all precautions must be taken.

Setting up a clustered environment reduces the risk of hardware, network and operating system failure, yet security always remains a risk.

The system is physically secure in a data center with personal card reader access and logging. An operations team that monitors all activity staffs the data center.

A Root privilege belongs to a very small team of administrators and is not provided to anyone. A sealed envelope copy is in a safe in the security office.

To allow the customer to believe they have made a good business decision and save a great deal of money, the systems will be hardened to prevent and/or detect the following vulnerabilities:

- Unauthorized Access
- Unauthorized Privileges
- Buffer Overflow attacks
- Trojan Horse attacks
- Denial of Service attacks

The system administrators have worked closely with the network team and IT security officials to develop the strategy deployed.

Step by Step Guide

Overview

Since the systems are Virtual Partitions on the HP Superdome, the installation must be performed from an ignite/ux server. The procedure to create the depot is not part of the scope and only the actual install process will be explain. The Ignite-UX depot does include the HP-UX application CD, Latest Patch CD and Latest Firmware CD.

- Installing O/S Security Patches, Security applications
  - Installing Base HP-UX 11.11
  - Installing Additional Applications
  - Remove Unnecessary Applications
  - Install Latest Security Patches from Hewlett Packard
  - Securing Saved Patches
  - Mount file systems securely
- Securing the O/S
  - Converting to a Trusted System
  - Remove Global Privileges
  - Fix PAM CDE issues
  - Set the default umask
  - Delete Unnecessary Accounts
  - Modify the home directory for the root account
  - Configure nsswitch.conf
  - Allow root login to console only
  - Secure the console
  - Protecting against remote logins
  - Disable console logging
  - Disable password and group caching and hashing
  - Disable ptydaemon
  - Modify setuid and setgid privileges
  - Change World Writeable Files and Directories
  - Restrict at and cron to authorized users
  - Create warning banners
  - Modify login profiles
  - Kernel Level Stack Buffer Overflow protection
  - Enable enhanced security options
  - System Logging
  - Resolve Issues found by CIS scan tool
- Securing the Network
  - Configure network time daemon
  - Disable rbootd

    - Disable unnecessary inetd services
    - Stop syslogd from listening on the network
    - Disable SNMP Daemons
    - Disable sendmail
    - Disable NFS
    - Disable DCE
    - Disable NIS comsec
    - Disable samd
    - Secure FTP
    - Network Tuning for Security
- Validating the System
    - Center for Internet Security (CIS) scan tool
    - Review output of netstat
    - Investigate open ports with lsof
- Cluster Implementation
- Maintenance

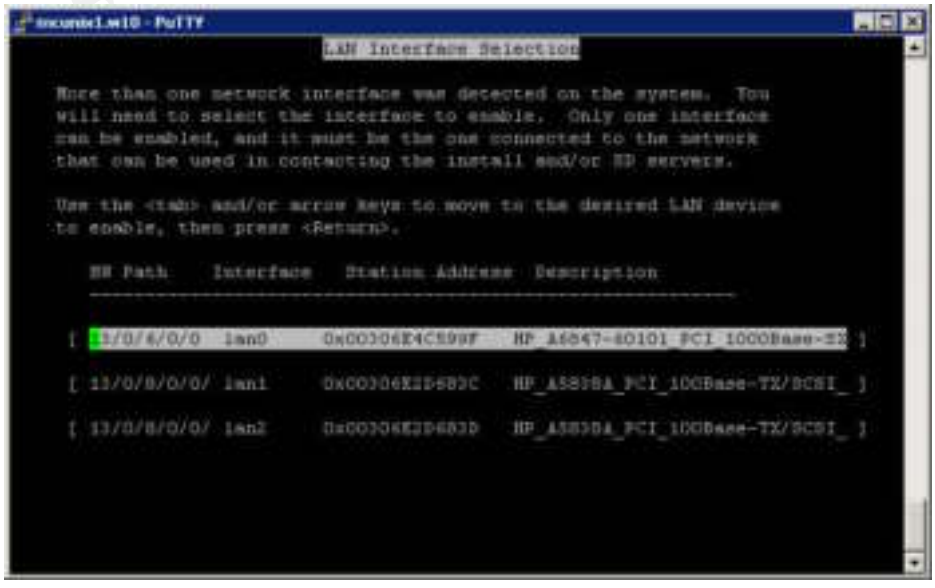
System Installation

1. Installing Base HP-UX 11.11

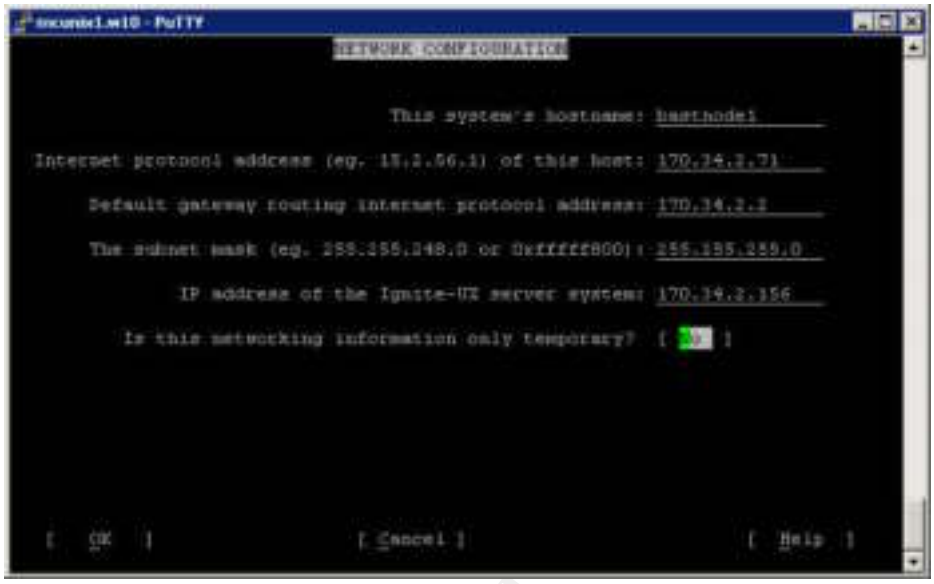
To insure the system is not compromised during the installation, perform the installation on a secure network, or even better, a standalone network switch. From a node within the npar, perform a vparboot and instruct the vpar to boot from the ignite server

- vparboot –p vparnode1 –I ignitenode1,,/opt/ignite/boot/WINSTALL
- Use ^A to access the console of vparnode1
- Select Ignite-UX server based installation and Advanced User interface options

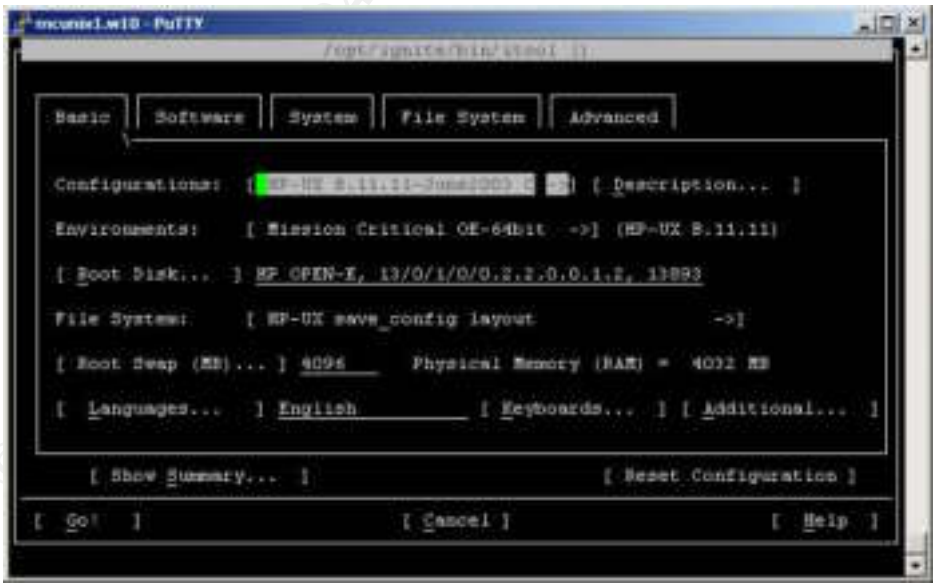
- Select the appropriate LAN interface to use for the installation.



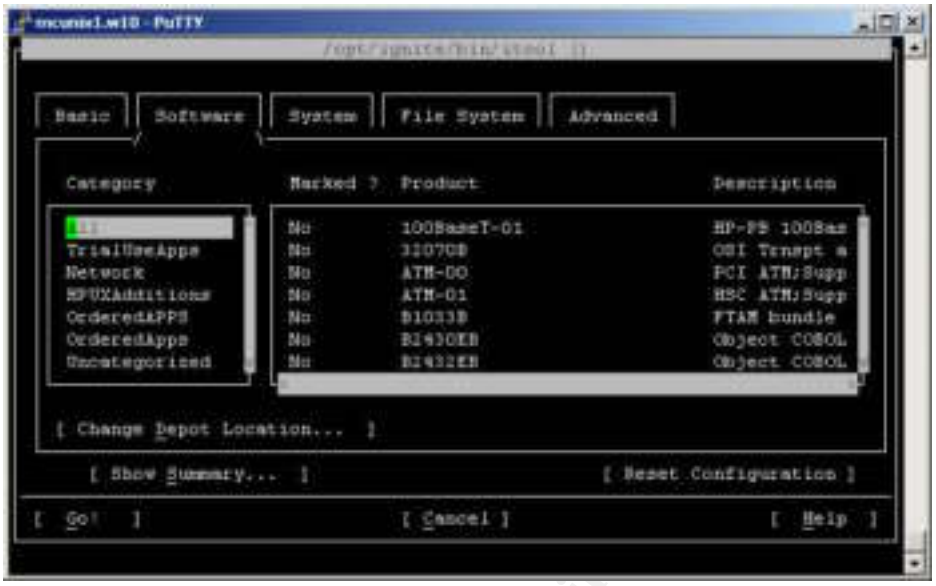
- Provide all the TCP/IP information for the ignite server to use when setting up the new server named bastnode1



- Select the correct configuration to install and proper boot disk. Since this is a highly available cluster, the mission critical install is selected as well.



- The software selection is important and will save time later by reducing the amount of software to remove. Activate the software tab and add/remove as shown below.



- Deselect the following by marking them as NO
  - Ximian GNOME 1.4 GTK+
  - Java 2 RTE for HP-UX (700/800), PA1.1 + PA2.0
  - Java 2 Plugin for HP-UX (700/800)
  - Java2 1.3 RTE for HP-UX
  - HyprFabrc-00
  - MOZILLA
  - MOZILLAsrc
  - Java2 1.3 Netscape Plugin for HP-UX
  - HpuxwsApache
  - HpuxwsTomcat
  - HpuxwsWebmin
  - HpuxwsXml
- Select the following by marking them as YES
  - MirrorDisk/UX
    - To mirror the disks
  - HP C/ANSI C Developer's Bundle for HP-UX 11.i (S800)
    - Required to compile some application source
  - HP GlancePlus/UX for s800 11i
    - For system monitoring
  - HP OnLineJFS
    - Online file system management
  - MC / ServiceGuard
    - Clustering
  - HP IPFilter 3.5alpha5
    - IP filtering
  - Ignite-IA-11-11
    - To create bootable/restorable system image

- Perl Programming Language
  - Used with various tools
- Partition Manager - HP-UX
  - Used to enable the partition to boot
- HP-UX Virtual Partitions
  - Used to enable the partition to boot
- Virtual Partition Manager HP-UX
  - Used to enable the partition to boot.

- Activate the System tab and set the root password, timezone, the other information will be completed later.
- In the File System tab area, setup and/or modify the sizes of the file systems. The following was setup for this particular system:

/stand	300 MB
/	500 MB
/home	300 MB
/opt	1500 MB
/tmp	200 MB
/usr	1500 MB
/var	1500 MB
/var/adm/crash	2000 MB
/var/logs	1500 MB

- Select Go to begin the installation

2. Installing Additional Applications

- Using swinstall, install the following applications
  - HP-UX Security Management Suite B.01.01
  - HP-UX Secure Shell A.03.61.002
  - TCP-WRAPPERS special release B.11.11.01.00
  - Tripwire 1.3.5
  - logrotate 2.5
- Verify the installation by executing the following
  - swlist –l product | grep –I secure_shell
  - swlist –l product | grep –I secpatchchk
  - swlist –l product | grep –I tcpwrap
  - swlist –l product | grep –I tripwire
  - swlist –l product | grep –I logrotate
- Compile and install lsof
  - Download the lsof source

- tar xvf lsof-4.55-ss-11.00.tar
- cd lsof-4.55
- ./Configure hpux
- Respond y to Take Inventory?
- Respond y to customize
  - HASSECURITY=y
    - We will only allow root to execute this command
  - Accept the default values for all others
- Execute make
- Install lsof
  - mkdir /usr/contrib./man/man8
  - chmod 700 /usr/c ontrib./man/man8
  - cp -p lsof.man /usr/contrib/man/man8/lsof.8
  - cp –p lsof /usr/contrib./bin/lsof
  - cp -p lsof /usr/contrib/bin/lsof
  - chmod 500 /usr/c ontrib/bin/lsof
  - cp -p lsof /usr/contrib/bin/lsof
  - chmod 500 /usr/c ontrib/bin/lsof

- Install tools from the Center for Internet Security
  - gunzip cis-hpux.tar.Z
  - tar xvf cis-hpux.tar
  - cd cis
  - swinstall -s `pwd`/CISscan.pkg CISscan
  - swlist -l product | grep -i cisscan

3. Remove Unnecessary Applications

The following application are not needed, or pose opportunities to compromise the system should be removed

Package Name	Comment
Asian*	
AudioSubsystem	
CDE	
CPS	
Contrib_Tools	
DDE	
DMI	Partial: Keep: DMI.DMI-RUN Keep: DMI.DMI-SHLIBS
DebugPrg	
DigitalVideo	
GSS-API	
Sup-Tool-Mgr	Removed so X11 can be removed
TechPrintServ	X11 is dependent on this product
Measureware	Do not want to collect history performance data
MSDOS-Utils	
NS-communicate	

OE	
PAM*	
PrinterMgmt	
Workload-Mgr	Removed so Proc-Resrc-Mgr could be removed
Proc-Resrc-Mgr	
SCR	
SG-Db2-Tool	
SG-FasTrack-Tool	
SG-Informix-Tool	
SG-NFS-Tool	
SG-Oracle-Tool	
SG-Progress-Tool	
SG-Sgosb-Tool	
SG-Sybase-Tool	
SG-Domain-Tool	
SysMgmt*	
SystemComm	
UUCP	
VUEtoCDE	
WLM-Toolkits	
mysql	
CDE	
CIFS*	
DMI	
ImagingSubsystem	
PRM*	
VRTS*	
X11	
Xserver	

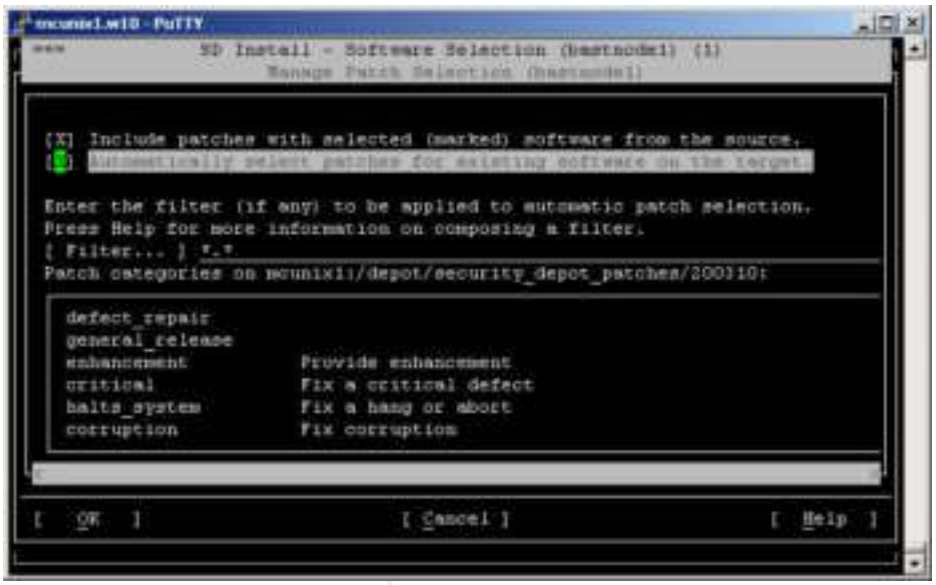
4. Install Latest Security Patches from Hewlett Packard

Using the security_patch_check tool installed with the HP Product HP-UX Security Management Suite B.01.01, the most recent security patches from HP can be determined and then installed. The tool requires the download of a patch catalog for the analysis to be performed. The security catalog is obtainable from ftp://ftp.itrc.hp.com/export/patches/security_catalog.gz . The following is the process to download catalog and execute the tool.

- Download and install the security catalog
  - ftp://ftp.itrc.hp.com/export/patches/security_catalog.gz
  - gunzip security_catalog.gz
- Execute security_patch_check
  - `security_patch_check -c security_catalog`
  - `accept`
- Analyze the output

```
WARNING: There are group- and world-writable directories in your path
         to perl and/or your PATH environment variable.  This represents a
         security vulnerability (especially if running as root) that may
         compromise the effective use of this tool.  Please use the command:
         chmod og-w <directory name>
         to ensure this tool can be used safely in the future.  A list of the
         vulnerable directories follows:
                /usr/local
                /usr/local/bin
WARNING: /tmp/ is group/world writable and the sticky bit is not on.

WARNING: Recalled patch PHCO_27408 is active on the target system. Its record,
         including the Warn field, is available from security_catalog, through
         the Patch Database area of the ITRC or by using the -m flag
         (security_patch_check -m ...).

WARNING: Recalled patch PHKL_24551 is active on the target system. Its record,
         including the Warn field, is available from security_catalog, through
         the Patch Database area of the ITRC or by using the -m flag
         (security_patch_check -m ...).

WARNING: Recalled patch PHKL_26979 is active on the target system. Its record,
         including the Warn field, is available from security_catalog, through
         the Patch Database area of the ITRC or by using the -m flag
         (security_patch_check -m ...).

WARNING: Recalled patch PHKL_27156 is active on the target system. Its record,
         including the Warn field, is available from security_catalog, through
         the Patch Database area of the ITRC or by using the -m flag
         (security_patch_check -m ...).

WARNING: Recalled patch PHNE_25644 is active on the target system. Its record,
         including the Warn field, is available from security_catalog, through
         the Patch Database area of the ITRC or by using the -m flag
         (security_patch_check -m ...).


*** BEGINNING OF SECURITY PATCH CHECK REPORT ***
Report generated by: /opt/sec_mgmt/spc/bin/security_patch_check.pl, run as root
Analyzed localhost (HP-UX 11.11) from bastnode1
Security catalog: security_catalog
Security catalog created on: Fri Dec 26 21:13:03 2003
Time of analysis: Sat Dec 27 01:36:39 2003

List of recommended patches for most secure system:

#  Recommended  Bull(s) Spec? Reboot? PDep? Description
-------------------------------------------------------------------------------
1  PHCO_23492   159     No    Yes     No    Kernsymtab
2  PHCO_25918   237     No    No      No    sort(1) cumulative
3  PHCO_26061   153     No    No      No    Kernel configuration commands
4  PHCO_26561   275     No    No      No    csh(1) cumulative
5  PHCO_27019   275     No    No      No    ksh(1)
6  PHCO_27037   191     No    No      Yes   libpam_unix cumulative
7  PHCO_27345   275     No    No      Yes   cumulative sh-posix(1)
8  PHCO_27694   160     No    No      No    login(1) cumulative
9  PHCO_28481   252     Yes   No      Yes   cumulative 10.20 libc compatibility support
10 PHCO_28719   258     No    No      No    wall(1M)
11 PHCO_28848   293     No    No      No    Software Distributor Cumulative
12 PHCO_29010   304     No    No      No    shar(1)
13 PHCO_29495   294     Yes   No      Yes   libc cumulative
14 PHKL_23423   156     No    Yes     No    improper core dump msg
15 PHKL_27179   206     No    Yes     No    Corrected reference to thread register state
16 PHKL_28990   183     No    Yes     No    Cumulative VM
17 PHNE_24512   232     Yes   No      No    NTP timeservices upgrade plus utilities
18 PHNE_27703   271     No    Yes     Yes   Cumulative STREAMS
19 PHNE_27765   162     No    No      No    ftpd(1M)
20 PHNE_27796   209     Yes   No      Yes   libnss_dns DNS backend
21 PHNE_28444   270     No    Yes     No    nettl(1M), netfmt(1M) and nettladm(1M)
22 PHNE_28983   252     Yes   Yes     Yes   ONC/NFS General Release/Performance
23 PHNE_29774   281     Yes   No      No    sendmail(1m) 8.9.3
24 PHNE_30068   303     No    No      No    Bind 8.1.2
25 PHSS_27858   208     Yes   No      No    OV EMANATE14.2 Agent Consolidated
26 PHSS_29964   276 299 Yes   No      Yes   HP DCE/9000 1.8 DCE Client IPv6
27 PHSS_30011   297     Yes   No      No    CDE Base
-------------------------------------------------------------------------------
*** END OF REPORT ***
```

- Download and install the identified patches and repeat the security_patch_check. Also note and address any warning provided by the command, such as world write-able directories. Patches can be obtained from the HP Patch Database web site. The site allows all patches to be downloaded in one bundle and installed in a depot. Use swinstall and manage patch selection action to verify only the patches the system requires are marked for install.



After the patches have been marked and the analysis has succeeded continue with the install. The system may or may not require a reboot.

- Execute security_patch_check
  - `security_patch_check -c security_catalog`

```
*** BEGINNING OF SECURITY PATCH CHECK REPORT ***
Report generated by: /opt/sec_mgmt/spc/bin/security_patch_check.pl, run as root
Analyzed localhost (HP-UX 11.11) from bastnode1
Security catalog: security_catalog
Security catalog created on: Fri Dec 26 21:13:03 2003
Time of analysis: Sat Dec 27 02:44:12 2003

List of recommended patches for most secure system:

#  Recommended  Bull(s) Spec? Reboot? PDep? Description
-------------------------------------------------------------------------------
Security patches are up to date with the security patch catalog used
-------------------------------------------------------------------------------
*** END OF REPORT ***
```

5. Securing Saved Patches

When patches are installed on HP-UX, copies are maintained and saved in /var/adm/sw/save. To prevent the old software from becoming available for use in attacks, it should be secured. There are two methods:

1. Commit the patches
2. Lock them down with security permissions

The first method will prevent the system from every using the old version again. The second method will still allow the patches to be rolled back if needed. We will choose the second method.

```
find /var/adm/sw/save \( -perm -4000 -o -perm -2000 \) -type f -exec
chmod a-s {} \;
```

Installation of the HP-UX 11.11 and required applications is complete.

6. Mount file systems securely

Make sure mounted file systems will ignore files containing setuid and setgid permissions. This will prevent and intruder from placing a file on the system.

```
/dev/vg00/lvol3 / vxfs delaylog 0 1
/dev/vg00/lvol1 /stand hfs nosuid,defaults 0 1
/dev/vg00/lvol4 /home vxfs nosuid,delaylog 0 2
/dev/vg00/lvol5 /opt vxfs delaylog 0 2
/dev/vg00/lvol7 /tmp vxfs nosuid,delaylog 0 2
/dev/vg00/lvol8 /usr vxfs delaylog 0 2
/dev/vg00/lvol9 /var vxfs nosuid,delaylog 0 2
/dev/vg00/lvol11 /var/logs vxfs nosuid,delaylog 0 2
/dev/vg00/lvol10 /var/adm/crash vxfs nosuid,delaylog 0 2
```

Securing the O/S

1. Converting to a Trusted System

HP-UX by default does not implement a shadow password file. The shadow password file stores the encrypted passwords and is only readable by the root user. In contrast, the /etc/passwd file is readable by all users. To implement the shadow password file (and some other nice features) the system should be converted to a trusted system.

```
# /usr/lbin/tsconvert

Creating secure password database...
Directories created.
Making default files.
System default file created...
Terminal default file created...
Device assignment file created...
Moving passwords...
secure password database installed.
Converting at and crontab jobs...
At and crontab files converted.
```

Converting to a trusted system automatically expires passwords and forces users to change their passwords, including root. Now is a good time to reset the root password.

```
# passwd root
Changing password for root
Old password:
Last successful password change for root: NEVER
Last unsuccessful password change for root: NEVER

Do you want (choose one letter only):
        pronounceable passwords generated for you (g)
        a string of letters generated (l) ?
        to pick your passwords (p) ?

Enter choice here: p
New password:
Re-enter new password:
Passwd successfully changed
```

Verify: System is trusted, will indicate and return a value of 4 if not a trusted system.

```
# /usr/lbin/getprdef -r
NO, 0, 8, 182, 196, -1, 7, YES, YES, NO, NO, NO, YES, 3, 10, 2, 0
# echo $?
0
```

Verify: Check Password File – Resolve any conflicts

```
# pwck -s
```

2. Remove Global Privileges

Prevent non-privileged users from performing change ownership (chown) on files.

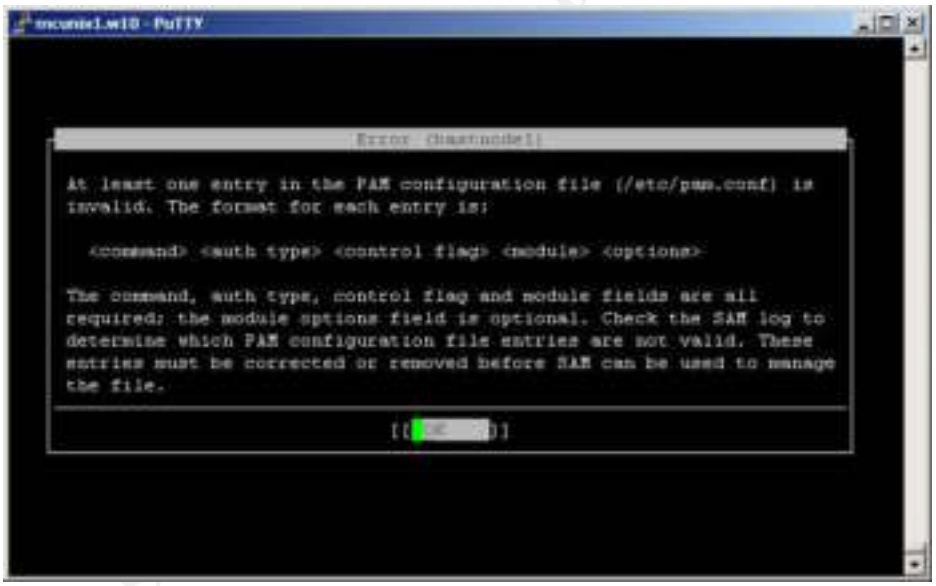
```
# getprivgrp
global privileges: CHOWN
# echo -n >/etc/privgroup
# chmod 400 /etc/privgroup
# getprivgrp
global privileges: CHOWN
# /sbin/init.d/set_prvgrp start
```

Verify: CHOWN privileges are removed

```
# getprivgrp
global privileges:
```

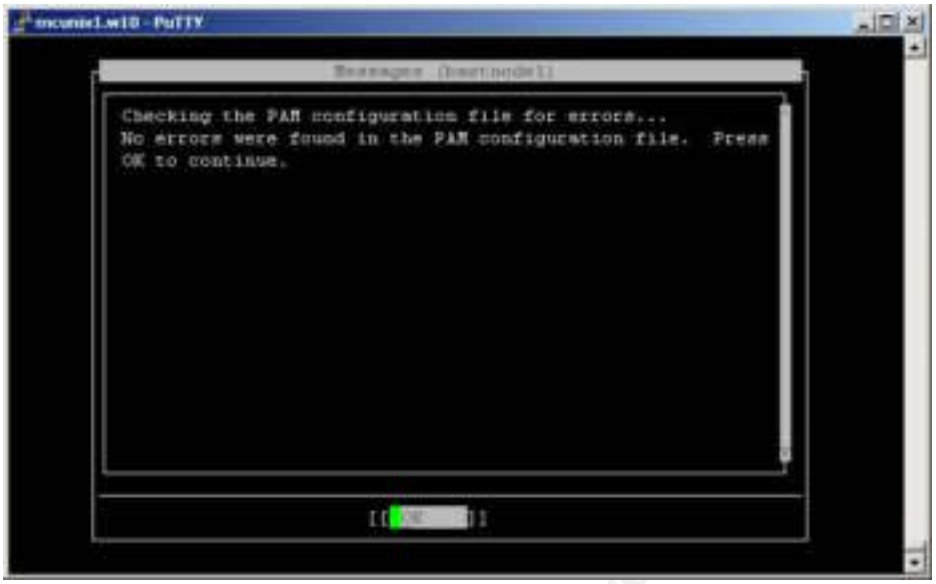
3. Fix PAM CDE issues

When SAM performs authentication checks, it will complain about CDE entries in the PAM file. The following will steps will resolve the issue.




```
# cp -p /etc/pam.conf /etc/pam.conf.SAVE
# grep -Ev '^(dtlogin|dtaction)'  /etc/pam.conf.SAVE >/etc/pam.conf
```

Verify: SAM -> Auditing -> Authenticated Commands -> Account Management



4. Set the default umask

Add entries to set the default umask to 0770 or 600.

```
cd /etc
for file in profile csh.login d.profile d.login
do echo umask 077 >> "$file"
done
```

Verify:

```
cd /etc
for file in profile csh.login d.profile d.login
do
echo $file
tail -1 $file
done
```

5. Delete Unnecessary Accounts

Remove all accounts that are not required for the system to function as a secure proxy server.

Identify the candidates for group removal, if they own no file, remove it.

root - keep
other - keep
bin - keep
sys - keep
adm - keep
daemon - remove

mail - keep
lp - remove
tty - keep
nuucp - remove
users - remove
nogroup - remove
sshd - keep
mysql – remove

```
for g in `echo daemon lp nuucp users nogroup sshd mysql`
do
groupdel $g
done
```

Change ownership of /etc/group from bin:bin to root:sys

```
# chown root:sys /etc/group
```

Identify the candidates for user removal, if they own no file, remove it.
root - keep
daemon - remove
bin - keep
sys - remove
adm - keep
uucp - remove
lp - remove
nuucp - remove
hpdb - remove
www - remove
webadmin - remove
sshd - keep
mysql - remove

```
for g in `echo sys uucp daemon lp nuucp hpdb www webadmin sshd mysql`
do
userdel $g
done
```

Secure the login shell for the remaining accounts, / is good candidate since it is a valid path that would very difficult to replace with a Trojan program.

```
root:*:0:3::/:/sbin/sh
bin:*:2:2:NO LOGIN:/usr/bin:/
adm:*:4:4:NO LOGIN:/var/adm:/
```

Verify:

```
# su - bin
su: No shell
```

6. Modify the home directory for the root account

To reduce the chance of a compromised root account landing in / and the intruder being able to place files in /, the root home directory will be relocated.

```
# cat /etc/passwd
root:*:0:3::/:/sbin/sh
bin:*:2:2:NO LOGIN:/usr/bin:/
adm:*:4:4:NO LOGIN:/var/adm:/
sshd:*:101:101:sshd privsep:/var/empty:/bin/false
vipw (change the root directory from / to /home/root)
# mkdir /home/root
# chown 700 /home/root
# mv /.profile /home/root/.profile
# pwconv
```

Verify: Connect to bastnode1

```
# pwd
/home/root
```

7. Configure nsswitch.conf

The system should control as much as possible how much information is available to both invited and un-invited guests. Domain resolution is nothing any guest needs on this system, therefore the host names will be controlled by the /etc/hosts file and not DNS.

If /etc/resolv.conf exists, remove it.

HP-UX provides a default config file from nsswitch.conf that will instruct name resolution to go to etc hosts. The file is /etc/nsswitch.files, and it should be copied to /etc/nsswitch.conf

```
# cp /etc/nsswitch.files /etc/nsswitch.conf
# nslookup
Using /etc/hosts on:  bastnode1
```

Verify:

```
# nslookup
Using /etc/hosts on:  bastnode1
```

8. Allow root login to console only

Privileged administrators should only use the root account. Since it is not much to ask, administrators should su to root and therefore the root account only needs to login to the console. This will provide and audit trail of any user accessing the root account.

```
# echo console >/etc/securetty
# chmod 400 /etc/securetty
```

Verify:

```
# telnet bastnode1
Trying...
```

```
Connected to bastnode1.w10.
Escape character is '^]'.
Local flow control on
Telnet TERMINAL-SPEED option ON

HP-UX bastnode1 B.11.11 U 9000/800 (ta)

login: root
Password:
Login incorrect

Wait for login retry: ..
login:
```

9. Secure the console

Ensure there is a password on all accounts for the LAN console. It is also a good idea to only connect a physical console only when needed.

telnet to the LAN Console and access with the default ID and password or the established ID and password

```
GSP:CM> so

    1. GSP wide parameters

    2. User parameters

       Which do you wish to modify? ([1]/2) 2

Current users:
      LOGIN            USER NAME                ACCESS        PART.
  1   Admin            Administrator            Admin
  2   Oper             Operator                 Operator

1 to 2 to edit, A to add, D to delete, Q to quit : 1

    Current User parameters are:
    Login             : Admin
    Name              : Administrator
    Organization      :
    Access Level      : Administrator
    Mode              : Multiple Use
    State             : Enabled
    Default Partition :
    Dialback          : (disabled)

    Enter Login [Admin] :
    Enter Name [Administrator] :
    Enter Organization [] :
    Valid Access Levels:  Administrator, Operator, Single Partition User
    Enter Access Level ([A]/O/S) :
    Valid Modes:  Single Use, Multiple Use
    Enter Mode (S/[M]) :
    Valid States:  Disabled, Enabled
    Enter State (D/[E]) :
    Enable Dialback ? (Y/[N])
    Enter Password [unchanged] :CHANGETHIS
```

Repeat for all accounts.

10. Protecting against remote logins

All users should have a .rhosts file in their home directory to protect against accidental remote login. Even though remote login services will be disabled, you never know when an unknowing administrator may turn them on temporarily and forget to turn them off.

```
# touch /home/root/.rhosts
# chmod 000 /home/root/.rhosts
```

Verify:

```
# ls -l /home/root/.rhosts
----------   1 root  sys      0 Dec 28 17:39 /home/root/.rhosts
```

11. Disable console logging

Log messages on the console are annoying and get in the way productivity when there is a problem. Since root is only allowed to log on to the console and it is typically not connected, there is no need to display any messages to it. If the console was connected, nobody needs to see this information but the administrator.

```
# nettlconf -L -console 0
# /usr/sbin/nettl -sp
# /usr/sbin/nettl -st
Initializing Network Tracing and Logging...
Done.
```

To prevent syslog from sending messages to the console, edit /etc/syslog.conf
Remove the following lines

```
*.alert                 /dev/console
*.alert                 root
```

Verify:
To verify, pull a lan connection and also send a logger message

```
# logger -p local0.alert test2
```

12. Disable password and group caching and hashing

The pwgrd daemon caches the password and group information for faster lookups. The password file on this system is so small, caching is not needed.

```
# ps -ef | grep pwgr
    root  1156     1  0  Dec 27  ?         0:05 /usr/sbin/pwgrd
```

Edit the /etc/rc.config.d/pwgr file and set the value of PWGR to 0.

```
# /sbin/init.d/pwgr stop
pwgrd stopped
# /sbin/init.d/pwgr start
```

Remove unnecessary pwgr files

```
# rm /var/spool/pwgr/*
```

```
# rm /var/spool/sockets/pwgr/*
```

Verify:

```
# ps -ef | grep pwgr
#
```

13. Disable ptydaemon

The ptydaemon is used by the shl application. shl is a shell layer application that allows interaction between shells from one terminal session.

Edit /etc/rc.config.d/ptydaemon and set the value of PTYDAEMON_START to 0.

Verify:

```
# ps -ef | grep ptydaemon
    root   541     1  0  Dec 27  ?         0:00 /usr/sbin/ptydaemon
# /sbin/init.d/ptydaemon stop
Ptydaemon stopped
# /sbin/init.d/ptydaemon start
# ps -ef | grep ptydaemon
#
```

14. Modify setuid and setgid privileges

Remove the setuid and setgid permissions on unused and unneeded files. If the file will only be used by root, the setuid and setgid bits can be turn off. Since this is a secure server with no user accounts, we will not need may programs with these permissions.

Obtain a complete list of files with the setuid and setgid permissions.

```
find / -perm -4000 -type f >/tmp/setuid.txt
find / -perm -2000 -type f >/tmp/setgid.txt
```

Review the files then turn off all setuid and setgid permissions

```
find / -perm -4000 -type f -exec chmod u-s {} \; >/tmp/setuid.txt
find / -perm -2000 -type f -exec chmod g-s {} \; >/tmp/setgid.txt
```

Add back the setgid and setuid as needed

```
# chmod u+s /usr/bin/su
# chmod u+s /usr/bin/passwd
```

15. Change World Writeable Files and Directories

World writeable files are pose a great hazard to the system. The system and its applications need to write to files and directories, but intruders do not.

Locate all world writeable files and directories.

```
find / \( -perm -002 -a \( -type f -o -type d \) \) -exec ls -ld {} \;
>/tmp/worldwrite.txt
```

Remove all world writes

```
# find / \( -perm -002 -a \( -type f -o -type d \) \) -exec chmod o-w {}
\;
```

Verify:

```
find / \( -perm -002 -a \( -type f -o -type d \) \) -exec ls -ld {} \;
```

Add back world writes to the following, adding the sticky bit prevents users other than root from deleting files from the directories and removing the files:

```
# chmod 1777 /tmp /var/tmp /var/preserve /var/stm/logs
/var/spool/cron/tmp
# chmod 666 /dev/null
```

Verify:

```
find / \( -perm -002 -a \( -type f -o -type d \) \) -exec ls -ld {} \;
```

Prevent /usr/local and /usr/local/bin from being owner and group writeable

```
# chmod 555 /usr/local /usr/local/bin
```

Verify: Execute hp_checkperms to verify against the HP and CIS standards

```
# /opt/CIS/hp_checkperms

Starting hp_checkperms Phase 1.

The following file contains error messages from a ll on a system
file. The system file was specified in an INFO file located in the IPD.
The "file not found" messages have been excluded.
Please review these messages for possible problems.
=>/tmp/cis/LL.errormsgs

Starting hp_checkperms Phase 2.

The following file lists system files which have differing
permission settings in the IPD, ie. HP can not decide what they
should be. So, you can decide what to do !!
=>/tmp/cis/MULTIPLE.permissions

Starting hp_checkperms Phase 3.

The file noted below contains file names that have MORE RESTRICTIVE
permissions than specified in the IPD.
=>/tmp/cis/MORE.restricted

Please review the script below for files which have LESS RESTRICTIVE
permissions than the IPD. Once you are comfortable with the specified
changes, please execute.
=>/tmp/cis/FIX_permissions

hp_checkperms finished.....
```

Based on the output in the three log files make adjustments as necessary and/or executer the /tmp/cis/FIX_permissions script.

```
# ./FIX_permissions

Starting to CORRECT permissions !
drwxr-xr-x   7 root       sys            96 Dec 26 19:48 /usr/contrib/man
dr-xr-xr-x   7 root       sys            96 Dec 26 19:48 /usr/contrib/man
drwxr-xr-x   2 root       sys          8192 Dec 27 02:38 /usr/contrib/man/man1.Z
dr-xr-xr-x   2 root       sys          8192 Dec 27 02:38 /usr/contrib/man/man1.Z
-rw-r--r--   1 root       sys         22395 Dec 26 23:47 /usr/lib/nls/iconv/config.iconv
-r--r--r--   1 root       sys         22395 Dec 26 23:47 /usr/lib/nls/iconv/config.iconv
-rw-r--r--   1 root       sys         30013 Dec 12 16:45 /usr/newconfig/usr/obam/server/conf/httpd.conf
-r--r--r--   1 root       sys         30013 Dec 12 16:45 /usr/newconfig/usr/obam/server/conf/httpd.conf
```

16. Restrict at and cron to authorized users

The system does not want to allow any user other than root to use cron, it is not necessary.

Make sure that cron.deny and at.deny files do not exist, rather setup cron.allow and at.allow.

```
# cd /var/adm/cron
# echo root >./at.allow
# echo root >./cron.allow
# chown root:sys at.allow cron.allow
# chmod 400 at.allow cron.allow
```

17. Create warning banners

Even though there are still great debates on the value of warning banners, they will be put in place to error on the side they are of value.

Create a text file containing the warning banner message (/tmp/warn_banner.txt).

```
******************************************************************************
                              NOTICE TO USERS

This computer system is private property and it is for
authorized use only. Users (authorized or unauthorized) have no explicit
or implicit expectation of privacy.

Any or all uses of this system and all files on this system may be
intercepted, monitored, recorded, copied, audited, inspected, and disclosed to
authorized site owner. By using this system, the user consents to such
interception, monitoring, recording, copying, auditing, inspection,
and disclosure at the discretion of the owner.

Unauthorized or improper use of this system may result in administrative
disciplinary action and civil and criminal penalties. By continuing to use
this system you indicate your awareness of and consent to these terms and
conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions
stated in this warning.

******************************************************************************
```

Install the banner

```
# grep -i bmw warn_banner.txt
# cat warn_banner.txt >/etc/motd
# cat warn_banner.txt >/etc/issue
# echo "banner=/etc/issue" >> /etc/ftpd/ftpaccess
```

18. Modify login profiles

The file login profiles can display information about the system and communicate the users session. Make the following changes to

/etc/profile
/etc/csh.login
/etc/d.profile
/etc/d.login

Remove the following:

```
# This is to meet legal requirements...

     cat /etc/copyright

# Notify if there is news

     if [ -f /usr/bin/news ]
     then news -n
     fi

# Change the backup tape

     if [ -r /tmp/changetape ]
     then    echo "\007\nYou are the first to log in since backup:"
             echo "Please change the backup tape.\n"
            rm  -f /tmp/changetape
     fi

fi
```

Add the following:

```
# echo "mesg n" >>/etc/profile
# echo "mesg n" >>/etc/d.profile
# echo "mesg n" >>/etc/csh.login
# echo "mesg n" >>/etc/d.login
```

19. Kernel Level Stack Buffer Overflow protection

HP-UX 11i has a kernel parameter to prevent buffer overflow attacks. By default the parameter is not active and must be set and the kernel rebuilt.

```
# kmtune -s executable_stack=0
# mk_kernel
Generating module: krm...
Generating module: pfil...
Generating module: ipf...
Compiling /stand/build/conf.c...
Loading the kernel...
Generating kernel symbol table...
# kmupdate
```

```
  Kernel update request is scheduled.

  Default kernel /stand/vmunix will be updated by
  newly built kernel /stand/build/vmunix_test
  at next system shutdown or startup time.

# shutdown -r 0
# kmtune | grep stack
```

Verify:

```
executable_stack            0  -  0
```

20. Enable enhanced security options

HP-UX 11i has a file /etc/default/security that enables some additional security features.

Create /etc/default/security and the following

```
# If the user account has no home directory exit
  ABORT_LOGIN_ON_MISSING_HOMEDIR=1

# Change the minimum password length from the default of 8
  MIN_PASSWORD_LENGTH=10

# Make sure /etc/nologin is not displayed.  Possible location
# for creating a denial of service attack.
  NOLOGIN=0

# Control the number of concurrent logins for a user
  NUMBER_OF_LOGINS_ALLOWED=1

# Control the number of time a password can be reused
  PASSWORD_HISTORY_DEPTH=7

# chmod 444 /etc/default/security
```

21. System Logging

For forensic and auditing purposes, system logging will be enabled for Accounting, Auditing, and inetd.

Accounting

```
# echo START_ACCT=1 >> /etc/rc.config.d/acct
# /sbin/init.d/acct start
Accounting started
```

Auditing

Edit /etc/rc.config.d/auditing be set the value of AUDITING to 1

```
# /sbin/init.d/auditing start
warning: /.secure/etc/audnames does not exist
created audit file: /.secure/etc/audfile1
created audit file: /.secure/etc/audfile2
```

```
created/repaired /.secure/etc/audnames
```

Verify:

```
# ps -ef | grep aud
    root  7298  1  0 21:02:58 ?  0:00 /usr/sbin/audomon -p 20 -t 1 -w 90
#
```

inetd

Edit /etc/rc.config.d/netdaemons and set the value of INETD_ARGS to "-l" (ell)

```
# /sbin/init.d/inetd stop
Internet Services stopped
# /sbin/init.d/inetd start
Internet Services started
```

Verify:

```
# ps -ef | grep inetd
    root  7335     1  0 21:08:54 ?         0:00 /usr/sbin/inetd -l
```

22. Resolve Issues found by CIS scan tool

Now is a good time to execute a cis-scan and resolve any O/S related issues. The following should be corrected as a result of the cis-scan report.

File /usr/bin/bdf shouldn't be Set-UID.

```
chmod 555 /usr/bin/bdf
```

Create /etc/shells – The system will default posix and korn as the only available shells.

```
# echo "/usr/bin/sh" >/etc/shells
# echo "/usr/bin/ksh" >>/etc/shells
# echo "/sbin/sh" >>/etc/shells
# chmod 444 /etc/shells
```

Minimum password life is 0, but should not be less than 7.

Maximum password life is 182, but should not exceed 90.

User sshd has a world-executable homedir!
User sshd has a world-readable homedir!

```
chmod 750 /var/empty
```

/tcb/files/auth/system/default should not be world-writable, readable or executable.

```
# chmod 400 /tcb/files/auth/system/default
```

/tcb/files/auth/system/maxaid should not be world-writable, readable or executable.

```
# chmod 400 /tcb/files/auth/system/maxaid
```

/var/dt/Xerrors should not be group-writable.

```
# chmod 640 Xerrors
```

/var/sam/log/samagent.log should not be group-writable..

```
# chmod 644 /var/sam/log/samagent.log
```

Securing the Network

1. Configure network time daemon

Accurate time is very important for system forensics, logging and monitoring. For this reasons, the network time daemon will be configured.

Edit the /etc/inet/ntp.conf and add the following

```
driftfile /var/adm/ntp.driftfile
server timeserver
restrict default nomodify
restrict 127.0.0.1

chmod go-w,a-s /etc/inet/ntp.conf

# /sbin/init.d/xntpd start
28 Dec 21:50:44 ntpdate[7385]: step time server 172.16.49.13 offset -
7.562423 sec
```

Verify:

```
tail /var/adm/syslog/syslog.log
Dec 28 21:54:10 bastnode1 xntpd[7420]: tickadj = 625, tick = 10000, tvu_maxslew = 61875
Dec 28 21:54:10 bastnode1 xntpd[7420]: precision = 11 usec
```

2. Disable rbootd

rbootd is a predecessor to bootpd that s700 workstations used with the RMP protocol. This is not needed.

Edit /etc/rc.config.d/netdaemons file to set the value of START_RBOOTD to 0.

```
# ps -ef | grep rbootd
    root  1145     1  0  Dec 27  ?         0:00 /usr/sbin/rbootd
# /sbin/init.d/rbootd stop
Remote boot daemon stopped
```

Verify:

```
# /sbin/init.d/rbootd start
# ps -ef | grep rbootd
```

3. Disable unnecessary inetd services

The following entries are required by this system have been reconfigured to use tcpd (TCP Wrappers).

tftpd - for use by ingnite/UX

instl_bootc – for use by ignite/UX

instl_boots – for use by ignite/UX

hacl-probe - for use by MC/Service Guard

hacl-cfg - for use by MC/Service Guard

/etc/inetd.conf

```
#All of the following call /usr/lbin/tcpd

tftp   dgram  udp wait root /usr/lbin/tcpd /usr/lbin/tftpd  tftpd /opt/ignite\
        /var/opt/ignite
hacl-probe  stream  tcp  nowait  root  /usr/lbin/tcpd /opt/cmom/lbin/cmomd
/opt/cmom/lbin/cmomd -f /var/opt/cmom/cmomd.log -r/var/opt/cmom
hacl-cfg    dgram   udp  wait    root  /usr/lbin/tcpd /usr/lbin/cmclconfd cmclconfd -p
hacl-cfg    stream  tcp  nowait  root  /usr/lbin/tcpd /usr/lbin/cmclconfd cmclconfd -c
instl_boots dgram   udp  wait    root  /usr/lbin/tcpd /opt/ignite/lbin/instl_bootd
instl_bootd

# /sbin/init.d/inetd stop
Internet Services stopped
# /sbin/init.d/inetd start
Internet Services started
```

Create /etc/hosts.allow and /etc/hosts.deny for the inetd services

```
echo "ALL: ALL" >/etc/hosts.deny

echo "ALL: 172.16." >/etc/hosts.allow
```

Verify:

Add the following to /etc/inetd.conf

```
# For Testing only
telnet       stream tcp nowait root /usr/lbin/tcpd /usr/lbin/telnetd  telnetd
```

Attempt a telnet session from inside and outside the network defined in /etc/hosts.allow

4. Stop syslogd from listening on the network

To prevent the syslog daemon from accepting the role of central syslog server, disable its ability to listen to network requests.

Edit /etc/rc.config.d/syslogd and change the value of SYSLOGD_OPTS to "-D -N"

Note: If /etc/rc.config.d/syslogd does not exist, the option can be added in /sbin/init.d/syslogd.

```
# ps -ef | grep syslogd
    root  9801     1  0 18:03:40 ?         0:00 /usr/sbin/syslogd -D
# /sbin/init.d/syslogd stop
syslogd stopped
# /sbin/init.d/syslogd start
System message logger started
```

Verify:

```
# ps -ef | grep syslogd
    root  7581     1  0 22:59:59 ?         0:00 /usr/sbin/syslogd -D -N
```

5. Disable SNMP Daemons

SNMP is well known for vulnerabilities, this is an applications that does not need to execute on this system.

Make the following edits to the following files:

/etc/rc.config.d/SnmpHpunix	SNMP_HPUIX_START=0
/etc/rc.config.d/SnmpMaster	SNMP_MASTER_START=0
/etc/rc.config.d/SnmpMib2	SNMP_MIB2_START=0
/etc/rc.config.d/SnmpTrpDst	SNMP_TRAPDEST_START=0

```
# ps -ef | grep snm
    root  1064     1  0  Dec 27  ?         0:00 /usr/sbin/snmpdm
    root  1097     1  0  Dec 27  ?         0:00 /usr/lbin/cmsnmpd
# ls -l Snmp*
-r-xr-xr-x   1 bin        bin           2553 Jun 19  2001 SnmpFddi4
-r-xr-xr-x   1 bin        bin           6617 Dec 28 23:27 SnmpHpunix
-r-xr-xr-x   1 bin        bin           4558 Dec 28 23:27 SnmpMaster
-r-xr-xr-x   1 bin        bin           6727 Dec 28 23:27 SnmpMib2
-r-xr-xr-x   1 root       sys           6631 Dec 28 23:27 SnmpTrpDst
# ./SnmpHpunix stop
# ./SnmpMaster stop
snmpdm stopped
# ./SnmpMib2 stop
# ./SnmpTrpDst stop
# ps -ef | grep snm
    root  1097     1  0  Dec 27  ?         0:00 /usr/lbin/cmsnmpd
# ./SnmpHpunix start
# ./SnmpMaster start
# ./SnmpMib2 start
# ./SnmpTrpDst start
```

Verify:

```
# ps -ef | grep snm
    root  1097     1  0  Dec 27  ?         0:00 /usr/lbin/cmsnmpd
```

6. Disable sendmail

A server only requires sendmail to execute if it is a mail server. The sendmail daemon is not required to send mail, only to manage it. Sendmail will be disabled.

Set the variable SENDMAIL_SERVER to 0 in /etc/rc.config.d/mailservs

Remove the –bd option from /sbin/init.d/sendmail

```
# ps -ef | grep sendmail
    root  1056     1  0  Dec 27  ?         0:20 sendmail: accepting
connections on port 25
# /sbin/init.d/sendmail stop
Sendmail pid is 1056
Killing sendmail
Please wait .....
Sendmail killed.
```

Verify:

```
# /sbin/init.d/sendmail start
 Sendmail server is disabled, You cannot start it manually using
 sendmail script.
```

7. Disable NFS

The system will perform no nfs mounts, therefore all NFS RPC services can be turned off.

First stop all the nfs daemons

```
# ./nfs.client stop
killing nfsd
killing rpc.mountd
    starting NFS SERVER networking

    starting up the rpcbind daemon
        /usr/sbin/rpcbind
    starting up the mount daemon
        /usr/sbin/rpc.mountd
    starting up the NFS daemons
        nfsd(s) already started, using pid(s): 1365 1374 1385 1364 1360
1361 1363 1373 1369 1370 1372 1382 1378 1379 1383 1381
    starting up the Status Monitor daemon
        rpc.statd already started, using pid: 749
    starting up the Lock Manager daemon
        rpc.lockd already started, using pid: 755
    starting up the PC-NFS daemon
        /usr/sbin/rpc.pcnfsd
killing biod
killing automount
# ./nfs.server stop
killing rpc.lockd
killing rpc.statd
killing rpc.pcnfsd
killing nfsd
killing rpc.mountd
# ./nfs.core stop
stopping rpcbind
```

Edit the file /etc/rc.config.d/nfsconf and set the following values to 0

NFS_CLIENT=0
NFS_SERVER=0
PCNFS_SERVER=0
AUTOMOUNT=0
START_MOUNTD=0

Relocate /sbin/init.d/nfs.core and /usr/sbin/rpcbind to another location to prevent it from starting up rpcbind.

```
# mv nfs.core nfs.core.NO
```

```
# chmod 400 nfs.core.NO
# mv /usr/sbin/rpcbind /usr/sbin/rpcbind.NO
```

Verify:

```
# ./nfs.client start
NFS_CLIENT not set to one in /etc/rc.config.d/nfsconf, exiting.
# ./nfs.server start
NFS_SERVER not set to one in /etc/rc.config.d/nfsconf, exiting.
# ps -ef | grep rpc
    root  1137     1  0  Dec 27  ?         0:05 /opt/dce/sbin/rpcd
# ps -ef | grep nfs
    root   707     0  0  Dec 27  ?         0:00 nfskd (Requires a reboot
to remove)
```

8. Disable DCE

The exact purpose of this daemon (dced) is unclear, the man page states

" The DCE Host daemon is a process that provides services for the local host, and is also the server used by remote applications to access these host services. "

It also appears to have ties to measureware on HP-UX systems. The startup of this daemon was removed and no adverse effects have been identified.
Set the value of START_RPCD to 0 in /etc/rc.config.d/Rpcd

```
# /sbin/init.d/dce stop
# mv /sbin/init.d/dce /sbin/init.d/dce.NO

# /sbin/init.d/Rpcd stop
# mv /sbin/init.d/Rpcd /sbin/init.d/Rpcd.NO
```

Verify:

```
# ps -ef | grep dced
#
```

9. Disable NIS comsec

The startup script /sbin/init.d/comsec starts the ttsyncd daemon used by NIS. The system will not use NIS so the daemon can be disabled.

```
/sbin/init.d
# ./comsec stop
stopping ttsyncd
```

Edit the value TTSYNCD in /etc/rc.config.d/comsec to be 0.

10. Disable samd

Remote SAM clients use the samd daemon. This system will not support remote SAM connections.

Edit /etc/inittab and comment out the samd entry

```
#samd:23456:respawn:/usr/sam/lbin/samd  # system mgmt daemon
```

Force inittab to re-read /etc/inittab

```
# ps -ef | grep samd
    root  1072     1  0 01:07:26 ?         0:00 /usr/sam/lbin/samd
# init q
```

Verify:

```
# ps -ef | grep samd
```

11. Secure FTP

Prevent any user from attempting a remote ftp connection. Add all local user accounts to /etc/ftpd/ftpusers.

```
# chmod 444 /etc/ftpd/ftpusers
```

12. Network Tuning for Security

HP-UX provides the ndd command to set and adjust how TCP/IP handles certain packets. The values are edited in /etc/rc.config.d/nddconf. The networking staff has reviewed and approved of these settings.

Add the following entries to /etc/rc.config.d/nddconf

```
TRANSPORT_NAME[0]=ip
NDD_NAME[0]=ip_forward_directed_broadcasts
NDD_VALUE[0]=0
#
TRANSPORT_NAME[1]=ip
NDD_NAME[1]=ip_forward_src_routed
NDD_VALUE[1]=0
#
TRANSPORT_NAME[2]=ip
NDD_NAME[2]=ip_forwarding
NDD_VALUE[2]=0
#
TRANSPORT_NAME[3]=ip
NDD_NAME[3]=ip_ire_gw_probe
NDD_VALUE[3]=0
#
TRANSPORT_NAME[4]=ip
NDD_NAME[4]=ip_pmtu_strategy
NDD_VALUE[4]=1
#
TRANSPORT_NAME[5]=ip
NDD_NAME[5]=ip_send_redirects
NDD_VALUE[5]=0
#
TRANSPORT_NAME[6]=ip
NDD_NAME[6]=ip_send_source_quench
NDD_VALUE[6]=0
#
TRANSPORT_NAME[7]=tcp
NDD_NAME[7]=tcp_conn_request_max
NDD_VALUE[7]=4096
#
TRANSPORT_NAME[8]=ip
NDD_NAME[8]=ip_respond_to_address_mask_broadcast
```

```
NDD_VALUE[8]=0
#
TRANSPORT_NAME[9]=ip
NDD_NAME[9]=ip_respond_to_echo_broadcast
NDD_VALUE[9]=0
#
TRANSPORT_NAME[10]=ip
NDD_NAME[10]=ip_check_subnet_addr
NDD_VALUE[10]=0
#
TRANSPORT_NAME[11]=ip
NDD_NAME[11]=ip_respond_to_timestamp_broadcast
NDD_VALUE[11]=0
#
TRANSPORT_NAME[12]=ip
NDD_NAME[12]=ip_respond_to_timestamp
NDD_VALUE[12]=0
#
TRANSPORT_NAME[13]=tcp
NDD_NAME[13]=tcp_text_in_resets
NDD_VALUE[13]=0
#
TRANSPORT_NAME[14]=arp
NDD_NAME[14]=arp_cleanup_interval
NDD_VALUE[14]=50000
#
TRANSPORT_NAME[15]=tcp
NDD_NAME[15]=tcp_syn_rcvd_max
NDD_VALUE[15]=4096
#
TRANSPORT_NAME[16]=tcp
NDD_NAME[16]=tcp_ip_abort_cinterval
NDD_VALUE[16]=50000
```

Apply the changes and verify:

```
# /usr/bin/ndd -c
# ndd -get /dev/tcp tcp_syn_rcvd_max
4096

#
```

Validating the System

Once the system has been hardened there are some additional tools to execute to validate the procedures performed. Most steps have been verified after they were performed.

1. Center for Internet Security (CIS) scan tool

Execute the CISscan tool.

```
Now a final check for non-standard world-writable files, Set-UID and Set-
GID
programs -- this can take a whole lot of time if you have a large
filesystem.
Your score if there are no extra world-writable files or SUID/SGID
programs
found will be 9.38 / 10.00 .  If there are extra SUID/SGID programs or
world-writable files, your score could be as low as 9.06 / 10.00 .

The preliminary log can be found at: /var/opt/CIS/tester.logs/cis-most-
recent-log

            Rating = 9.38 / 10.00

To learn more about the results, do the following:

   All results/diagnostics:
        more /var/opt/CIS/tester.logs/cis-ruler-log.20031229-16:01:47.681
   Positive Results Only:
        egrep "^Positive" /var/opt/CIS/tester.logs/cis-ruler-
log.20031229-16:01:47.681
   Negative Results Only:
        egrep "^Negative" /var/opt/CIS/tester.logs/cis-ruler-
log.20031229-16:01:47.681

For each item that you score or fail to score on, please reference the
corresponding item in the CIS Benchmark Document.

# egrep "^Negative" /var/opt/CIS/tester.logs/cis-ruler-log.20031229-
16:01:47.681
Negative: 3.2 inetd is still active.
```

Yes – using TCP Wrappers

```
Negative: 5.1 /opt is not mounted read-only.
```

Some applications in /opt have problems with this.

```
Negative: 5.9 checkperms has not been run on this system.
```

Ran hp_checkperms.

2. Review output of netstat

Execute netstat –af inet and look for open listening ports

```
# netstat -af inet
```

```
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp        0      0  *.22                    *.*
LISTEN
tcp        0      0  *.hacl-probe            *.*
LISTEN
tcp        0      0  *.hacl-cfg              *.*
LISTEN
tcp        0      0  bastnode1.22            .54299
ESTABLISHED
tcp        0      0  *.2121                  *.*
LISTEN
udp        0      0  *.*                     *.*
udp        0      0  *.hacl-cfg              *.*
udp        0      0  *.2121                  *.*
udp        0      0  *.ntp                   *.*
udp        0      0  localhost.ntp           *.*
udp        0      0  bastnode1.ntp           *.*
```

3. Investigate open ports with lsof

```
# lsof -i
COMMAND   PID USER   FD   TYPE     DEVICE SIZE/OFF NODE NAME
sshd      614 root    3u  inet 0x481c9040      0t0  TCP *:22 (LISTEN)
inetd     632 root    6u  inet 0x481c9340      0t0  TCP *:hacl-probe (LISTEN)
inetd     632 root    7u  inet 0x481c94c0      0t0  UDP *:hacl-cfg (Idle)
inetd     632 root    8u  inet 0x481c9640      0t0  TCP *:hacl-cfg (LISTEN)
xntpd     936 root    4u  inet 0x481c9ac0      0t0  UDP *:ntp (Idle)
xntpd     936 root    5u  inet 0x481c9c40      0t0  UDP bastnode1.W10:ntp (Idle)
xntpd     936 root    6u  inet 0x481c9dc0      0t0  UDP localhost:ntp (Idle)
```

Cluster Implementation

The cluster portion of this paper will focus on using HP IPFilter to allow the communication between the two nodes in the cluster.

In order to build the cluster, the second node must be locked down per the above procedures.

The quickest way to complete the task is via ignite-ux. ignite-ux is not in scope but the install of the second node can be accomplished sever ways.

1. /opt/ignite/data/scripts/make_sys_image
2. /opt/ignite/bin/make_net_recovery
3. /opt/ignite/bin/make_tape_recovery

When installing the recovery image, be sure to interrupt the process, perform and advanced installation, and change the networking parameters.

After the second node is up, the following will need to be accomplished:

1. Verify /etc/services
2. Verify /etc/inetd.conf
3. Build the ipf.conf file
4. Setup the cluster files
5. Create the cluster
6. Test the failover of the package
7. Review the Service ports

1. Verify /etc/services

The following entries should be listed in /etc/services. Since MC/Service Guard was installed, they should already be there.

```
hacl-hb     5300/tcp                # High Availability (HA) Cluster heartbeat
hacl-gs     5301/tcp                # HA Cluster General Services
hacl-cfg    5302/tcp                # HA Cluster TCP configuration
hacl-cfg    5302/udp                # HA Cluster UDP configuration
hacl-probe  5303/tcp                # HA Cluster TCP probe
hacl-probe  5303/udp                # HA Cluster UDP probe
hacl-local  5304/tcp                # HA Cluster Commands
hacl-test   5305/tcp                # HA Cluster Test
hacl-dlm    5408/tcp               # HA Cluster distributed lock manager
```

2. Verify /etc/inetd.conf

The following entries are required in /etc/inetd.conf

```
hacl-probe  stream  tcp  nowait  root  /usr/lbin/tcpd /opt/cmom/lbin/cmomd
/opt/cmom/lbin/cmomd -f /var/opt/cmom/cmomd.log -r /var/opt/cmom
hacl-cfg    dgram   udp  wait    root  /usr/lbin/tcpd /usr/lbin/cmclconfd cmclconfd -p
hacl-cfg    stream  tcp  nowait  root  /usr/lbin/tcpd /usr/lbin/cmclconfd cmclconfd -c
```

3. HP IPFilter ipf.conf file

Since we are using ipf to filter cluster packets between nodes, we will build the file with options to function as a firewall as well. This is just an added level of security. Note that each node in the cluster will have a different ipf.conf. The rules that are

specific to node 172.16.2.71 will be configured as 172.16.2.73 in the ipf.conf on the second node.

/etc/opt/ipf/ipf.conf

```
# cat ipf.conf
#
# Thu Sep 24 2002
#
# IPFilter configuration file for bastnode1 172.16.2.71
#                                 package   172.16.2.72
#                                 bastnode2 172.16.2.73
#
# Notes:
#
# Remember that IPF reads the rules from top down
# but uses the LAST matching rule.
#
############################################################
#
# Allow communication over localhost
#
pass in quick on lo0 all
pass out quick on lo0 all

#
# Allow Cluster to comminicate via both lan devices
#
pass out log level auth.alert quick on lan0 proto udp from 172.16.2.71/32 to
255.255.255.255/32 port = 5302 keep state
pass out log level auth.alert quick on lan2 proto udp from 172.16.2.71/32 to
255.255.255.255/32 port = 5302 keep state

pass out quick on lan0 from 172.16.2.73/32 to 172.16.2.71/32
pass out quick on lan2 from 172.16.2.73/32 to 172.16.2.71/32

pass in quick on lan0 from 172.16.2.71/32 to 172.16.2.73/32
pass in quick on lan2 from 172.16.2.71/32 to 172.16.2.73/32

#
# Pass Cluster Heartbeat (crossover cable connection)
#

pass in quick on lan1 from 10.1.2.1 to 10.1.2.2
pass out quick on lan1 from 10.1.2.2 to 10.1.2.1


#
# Anti-Spoofing Rules you should never see traffic from these networks
#
block in log level auth.alert quick on lan0 from 192.168.0.0/16 to any
block in log level auth.alert quick on lan0 from 172.16.0.0/12 to any
block in log level auth.alert quick on lan0 from 10.0.0.0/8 to any
block in log level auth.alert quick on lan0 from 127.0.0.0/8 to any
# block in log level auth.alert quick on lan0 from 169.254.0.0/16 to any
block in quick on lan0 from 169.254.0.0/16 to any
block in log level auth.alert quick on lan0 from 192.0.2.0/24 to any
block in log level auth.alert quick on lan0 from 204.152.64.0/23 to any
block in log level auth.alert quick on lan0 from 224.0.0.0/3 to any
block in log level auth.alert quick on lan0 from any to 172.16.2.128/32
block in log level auth.alert quick on lan0 from any to 172.16.2.255/32

#
# Allows ICMP (ping) to and from this system
#
pass in quick on lan0 proto icmp from 172.16.2.64/32 to 172.16.2.73/25 icmp-type 0 keep
state
```

```
pass in quick on lan0 proto icmp from 172.16.2.64/32 to 172.16.2.73/25 icmp-type 8 keep
state
pass out quick on lan0 proto icmp from 172.16.2.73/25 to any icmp-type 0 keep state
pass out quick on lan0 proto icmp from 172.16.2.73/25 to any icmp-type 8 keep state

#
# Allow SSH from the internal network to this system
#
pass in quick on lan0 proto tcp from 172.16.2.64/32 to 172.16.2.73/32 port = 22 flags S
keep state

#
# Allow NTP from this host
#
pass out log level auth.info quick on lan0 proto udp from 172.16.2.73/32 to any port = 123
keep state

#
# Allow SYSLOG from this host
#
pass out quick on lan0 proto udp from 172.16.2.73/32 to 172.16.2.64/32 port = 514 keep
state

#
#       Block NetBIOS Traffic from local net but DO NOT LOG!
#
block in quick proto udp from 172.16.2.135/32 to 172.16.2.255/32 port = 138
block in quick proto udp from 172.16.2.153/32 to 172.16.2.255/32 port = 138

#
#       Block BOOTP(S)(port 67,68) Traffic from 0.0.0.0 to 255.255.255.255
#
block in quick proto udp from 0.0.0.0 to 255.255.255.255 port = 67

#
# This is the catch all rule that BLOCK EVERYTHING!
#
block in log level auth.alert quick all
block out log level auth.alert quick all
```

Start HP IPFilter

```
# /sbin/init.d/ipfboot stop
kmadmin: Module 2 unloaded
# /sbin/init.d/ipfboot start
```

4. Build the cluster files

The cluster configuration file /etc/cmcluster/cmclconf.ascii is created as follows:

```
# cat cmclconf.ascii
# ********************************************************************
# ********* HIGH AVAILABILITY CLUSTER CONFIGURATION FILE ***************
# ***** For complete details about cluster parameters and how to    ****
# ***** set them, consult the cmquerycl(1m) manpage or your manual. ****
# ********************************************************************

# Enter a name for this cluster.  This name will be used to identify the
# cluster when viewing or manipulating it.

CLUSTER_NAME mcpincl


# Cluster Lock Device Parameters.  This is the volume group that
```

```
# holds the cluster lock which is used to break a cluster formation
# tie.  This volume group should not be used by any other cluster
# as cluster lock device.

#FIRST_CLUSTER_LOCK_VG
FIRST_CLUSTER_LOCK_VG /dev/vgpkg
SECOND_CLUSTER_LOCK_VG /dev/vgapp


# Definition of nodes in the cluster.
# Repeat node definitions as necessary for additional nodes.

NODE_NAME                       bastnode1
  NETWORK_INTERFACE             lan0
    HEARTBEAT_IP                172.16.2.146
  NETWORK_INTERFACE             lan1
    HEARTBEAT_IP                10.1.2.1
    NETWORK_INTERFACE           lan2
    FIRST_CLUSTER_LOCK_PV       /dev/dsk/c5t0d0
    SECOND_CLUSTER_LOCK_PV      /dev/dsk/c6t2d0

NODE_NAME                       bastnode2
  NETWORK_INTERFACE             lan0
    HEARTBEAT_IP                172.16.2.148
  NETWORK_INTERFACE             lan1
    HEARTBEAT_IP                10.1.2.2
    NETWORK_INTERFACE           lan2
    FIRST_CLUSTER_LOCK_PV       /dev/dsk/c5t0d0
    SECOND_CLUSTER_LOCK_PV      /dev/dsk/c6t2d0

# List of serial device file names
# For example:
# SERIAL_DEVICE_FILE    /dev/tty0p0


# Cluster Timing Parmeters (microseconds).

HEARTBEAT_INTERVAL      8000000
NODE_TIMEOUT            20000000


# Configuration/Reconfiguration Timing Parameters (microseconds).

AUTO_START_TIMEOUT              600000000
NETWORK_POLLING_INTERVAL        2000000

# Package Configuration Parameters.
# Enter the maximum number of packages which will be configured in the
cluster.
# You can not add packages beyond this limit.
# This parameter is required.
MAX_CONFIGURED_PACKAGES         5
```

```
# List of cluster aware Volume Groups. These volume groups will
# be used by package applications via the vgchange -a e command.
# For example:
# VOLUME_GROUP          /dev/vgdatabase.
# VOLUME_GROUP          /dev/vg02.
VOLUME_GROUP            /dev/vgpkg
VOLUME_GROUP            /dev/vgapp
```

The contents of /etc/cmcluster/cmclnodelist, this avoids the .rhosts dependency.

```
bastnode1  root
bastnode2  root
```

The package conf file and control scripts are very text book and will not be detailed.

5. Build the Cluster

Check and create and start the cluster.

```
cmcheckconf -v -C /etc/cmcluster/cmclconf.ascii
-P /etc/cmcluster/packages/package.conf

cmapplyconf -v -C /etc/cmcluster/cmclconf.ascii \
-P /etc/cmcluster/packages/package.conf

cmruncl
```

If the cluster fails to form due to connectivity, check the ipf.conf file and inetd.conf file.

6. Test the failover

Perform all failover tests:

- starting the package on each node
- network interface failure, pull each network cable
- power failure (have a backup)

7. Review the Network Service Ports

Double check only the daemon and ports that were configured on the ones executing and listening.

```
# lsof -i | grep LIST
sshd       630 root    3u  inet 0x42609640      0t0  TCP *:22 (LISTEN)
inetd      643 root    5u  inet 0x426097c0      0t0  TCP *:hacl-probe (LISTEN)
inetd      643 root    7u  inet 0x42609ac0      0t0  TCP *:hacl-cfg (LISTEN)
cmcld      980 root    4u  inet 0x4276b800      0t0  TCP loopback:hacl-local (LISTEN)
cmcld      980 root   17u  inet 0x42951240      0t0  TCP bastnode2:hacl-hb (LISTEN)
cmcld      980 root   19u  inet 0x42951540      0t0  TCP 10.1.2.2:hacl-hb (LISTEN)
cmcld      980 root   21u  inet 0x42951840      0t0  TCP bastnode2:hacl-gs (LISTEN)
cmcld      980 root   23u  inet 0x42951b40      0t0  TCP 10.1.2.2:hacl-gs (LISTEN)
cmlvmd     985 root    7u  inet 0x42972d00      0t0  TCP loopback:1476 (LISTEN)
```

Maintenance

To insure the system continue to function well we will perform setup the following actions.

1. Configure and execute tripwire. A database will be created before the system is placed into production.

2. Perform a final backup of the system using Ignite/UX

3. Configure logrotate to rotate out the system logs. Another server will use Secure Shell Copy to pull the logs back to a central repository. Since the site has custom system monitors for processes, file systems, etc. that log to syslog, the servers will be monitored as well.

4. System and application patching. The security_patch_check tool will continue to be used as presented earlier. Email alerts have been setup with Hewlett Packard, SANS, and CERT to receive notice of any security alert as they are available.

1. Tripwire

Tripwire was installed during the initial system installation. The tripwire config file must be created and the tripwire setup to execute from cron.

The initial template used was obtained from http://www.deer-run.com/~hal/tw.config and then customized for local site.

Customized tw.config file

```
#  First, root's "home"

=/                      L
/.rhosts                R       # may not exist
/.profile               R       # may not exist
/.cshrc                 R       # may not exist
/.login                 R       # may not exist
/.exrc                  R       # may not exist
/.logout                R       # may not exist
/.emacs                 R       # may not exist
/.forward               R       # may not exist
/.netrc                 R       # may not exist
/.mailrc                R       # may not exist

/.ssh                   R
/.ssh/known_hosts       L
/.ssh/prng_seed         E
/.ssh/random_seed       E

# Now, some critical directories and files
#  Some exceptions are noted further down

/dev                    L

/etc                    R
```

```
/etc/dumpdates          L
/etc/motd               L
/etc/passwd             L
/etc/rmtab              L
/etc/syslog.pid         E
/etc/utmp               L
/etc/utmpx              L

=/tcb                   L

=/var                   L
=/var/adm               L
/var/adm/ntp.drift      E
/var/adm/wtmp           L
/var/adm/wtmpx          L
/var/adm/sulog          L
=/var/adm/sa            L
=/var/spool             L

# put entries in for /var/yp if you need it
# put entries for uucp if you need them
# put entries for /var/adm if you need it

=/tmp                   L
=/var/tmp               L
=/usr                   R

/stand                  R
/opt                    R-2
/sbin                   R-2
/usr/sbin               R-2
/usr/bin                R-2
/usr/dt/bin             R-2
/usr/local/bin          R-2
/usr/lib                R-2
/usr/ccs                R-2

# Sensitive programs

/usr/bin/sh             R
/usr/bin/csh            R
/usr/bin/ksh            R
/usr/bin/crontab        R
/usr/bin/diff           R
/usr/bin/df             R
/usr/bin/du             R
/usr/bin/find           R
/usr/bin/finger         R
/usr/bin/kill           R
/usr/bin/login          R
/usr/bin/ls             R
/usr/bin/netstat        R
/usr/bin/passwd         R
/usr/bin/ps             R
/usr/bin/su             R
/usr/bin/sum            R
/usr/bin/w              R
/usr/bin/who            R
/usr/sbin/cron          R
/usr/sbin/ifconfig      R
/usr/sbin/inetd         R
/usr/sbin/in.ftpd       R
/usr/sbin/in.telnetd    R
/usr/sbin/in.rshd       R
/usr/sbin/in.rlogind    R
/usr/sbin/syslogd       R
/usr/lib/sendmail       R
/opt/ssh/sbin/sshd      R
```

Initialize the database

```
/opt/tw/tripwire -initialize -c /opt/tw/tw.config -d
/opt/tw/databases/tw.db_bastnode1
```

Schedule the report to run from cron and log output to /var/adm/tripwire

```
# execute tripwire
18 20 * * * /opt/tw/tripwire -c /opt/tw/tw.config -d
/opt/tw/databases/tw.db_bastnode1 >/var/adm/tripwire/tripwire.`date +%j`
2>&1
```

2. Logrotate

Logrotate was also part of the initial installation. The logrotate.config remains to be configured and the application scheduled in cron. The rotated logs will be collected by a process on another host.

Create /etc/opt/logrotate/logrotate.config

```
compress

/var/adm/syslog/mail.log {
     rotate 1
     daily
     delaycompress
     olddir /var/adm/logrotate/mail
     create 444 root root
     postrotate
               /sbin/init.d/sendmail stop
               /sbin/init.d/sendmail start
     endscript
}

/var/adm/cron/log {
     rotate 1
     daily
     delaycompress
     olddir /var/adm/logrotate/cronlog
     create 444 root root
     postrotate
               /sbin/init.d/cron stop
               /sbin/init.d/cron start
     endscript
}

/var/adm/syslog/syslog.log {
     rotate 1
     daily
     olddir /var/adm/logrotate/syslog
     delaycompress
     postrotate
               cat /var/run/syslog.pid | xargs -i /usr/bin/kill -HUP {}
     endscript
}
```

Create necessary directories

```
# mkdir /var/adm/logrotate
# chmod 700 /var/adm/logrotate
```

Schedule to execute in cron

```
# execute logrotate
```

```
35 20 * * * /opt/logrotate/bin/logrotate -v
/etc/opt/logrotate/logrotate.config >> /var/adm/logrotate/logrotate.`date
+%j` 2>&1
```

Appendix A: References

1. Wong, Chris. hp-ux 11i security. Upper Saddle River: Prentice Hall PTR, 2002

2. Skagen, Martin & Jones, Walt.. "How-to secure HPUX 11i for use in a DMZ environment version 1.6". Hewlett Packard Enterprise Support Services Organization. October 8, 2002

3. Steves, Kevin. "Building a Bastion Host Using HP-UX 11". August 2002. http://www.hp.com/products1/unix/operating/infolibrary/whitepapers/building_a_bastion_host.pdf

4. Conoboy, Brenden & Fichtner, Erik. "IP Filter Based Firewalls HOWTO" December 11, 2002. http://www.obfuscation.org/ipf/ipf-howto.txt

5. Garfinkel, Simson & Spafford, Gene. Practical Unix & Internet Security. Cambridge: O'Reilly and Associates, Inc, 1996.

6. Hewlett-Packard Company. HP-UX Reference (Volume 8 of 9). Hewlett-Packard Company, L.P. 2003

7. Hewlett-Packard Company. Installing and Administering HP-UX IPFilter. Hewlett-Packard Company, L.P. 2003

8. Hewlett-Packard Software Depot. "Security Patch Check". http://www.software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=B6834AA

9. Hewlett-Packard Software Depot. "HP-UX Secure Shell". http://www.software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=T1471AA

10. Hewlett-Packard Software Depot. "HP-UX IPFilter". http://www.software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=B9901AA

11. Hewlett-Packard Software Depot. "HP-UX TCP Wrappers". http://www.software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=TCPWRAP

12. The HP-UX Porting and Archive Center. "lsof-4.69". November 21, 2003. http://hpux.connect.org.uk/hppd/hpux/Sysadmin/lsof-4.69/

13. The HP-UX Porting and Archive Center. "logrotate-2.5". March 8, 2000. http://hpux.connect.org.uk/hppd/hpux/Sysadmin/logrotate-2.5/

14. the Center for Internet Security. “CIS Level-1 Benchmark and Scoring Tool for HP-UX” October 2003. http://www.cisecurity.org/bench_hpux.html

15. SOURCEFORGE.net. “Tripwire”. February 28, 2000. http://sourceforge.net/projects/tripwire/

16. Pomeranz, Hal. “SANS Institute Track 6 – Securing Unix”. 2003.

17. Deer Run Associates. “tripwire.config”. http://www.deer-run.com/~hal/tw.config

Last Updated: October 24th, 2017

Upcoming Training

SANS 2018	**Orlando, FL**	**Apr 03, 2018 - Apr 10, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**