Jackie Andrason

HP-UX 11.00 INSTALLATION CHECKLIST

This checklist has been developed for installing HP-UX 11.0 on an application server. An HP D220 with 2 4 GB disks and 250 MB memory served as the installation server. The purpose of this machine was just as a testbed for developing this list, which will be used to install real servers, therefore, it is more generic based on what the needs might be for each individual server installed. Once this is done, we can create a tape of the clean operating system we just installed, and then this tape can be used it to ignite (clone) other HP systems that are being installed for application use.

The requirements for the application servers that will be installed are per MyCompany's standards for application servers and will serve as the methodology for this installation checklist. We know that all systems will be DNS clients only, will not run NIS, there will be no NFS mounted or exported filesystems, and that there may be users in addition to any system administrators logging in to the system. However, no mail will be received on this system by any user. Therefore, we will install the minimal OS minus anything we don't need (and adding some additional things we do), any additional drivers and the C compiler from the application CD, and then install the latest patches from the Support Plus CD. Then there will be some additional tweaking to do.

HARDWARE

The server must be set up in the computer facility which is accessed by security badge. Only authorized personnel can come into the computer facility, and must sign in.

OPERATING SYSTEM INSTALLATION

Most HP systems will be shipped with an OS ignited from the factory. Do not use this operating system version. Instead, overwrite the default installation using the using the HP-UX 11.0 Core OS CD. Then install the latest patches and the Ignite-UX software using the most current Support Plus CD. Also needed is the HP-UX 11.0 Application Software CD for the C compiler software and possibly any drivers (such as lan) that might be needed.

_____ Boot system from Core OS Installation CD
_____ Enter term type and default language
_____ Select "Install HP-UX"
_____ Under Media Options choose "Media only installation"
_____ Under User Interface Options choose "Advanced Installation"

This is going to bring up the Ignite-UX interface
BASIC TAB
_____ Configurations: HP-UX B.11.00 Default
_____ Environments: 32-Bit Minimal HP-UX (English) (or 64-bit if appropriate)
_____ Root Disk: Get listing and choose the appropriate disk
_____ File System: Logical Volume manager with VxFS (choose as appropriate)

_____ Root Swap (MB): Figure how much swap you want, write it here ____________
SOFTWARE TAB, This should be changed to use the CD and so that unneeded filesets can be deselected and filesets that are needed for C, tcb, and system administration can be selected.
_____ Select Change Depot Location
_____ Change Interactive swinstall to “Yes”
_____ Select Modify
NETWORK TAB:
__________________ enter your IP address
__________________ enter your netmask
_____ check date
_____ set TimeZone
_____ Set root password
FILE SYSTEM:
Enter the sizes for logical volumes:
_________ MB /
_________ MB /stand (HFS filesystem)
_________ MB /usr
_________ MB /var
_________ MB /opt
_________ MB /tmp
_________ MB /home

Go!

SD INSTALL
Since NIS, NFS, and PPP are not needed, these can be deselected before the install. SAM, SecurityMon, SOE, and the X11 shared libraries all need to be selected to install them. These are needed to run the sam system administration tool and convert the system to a trusted system (tcb). The X11 shared libraries and the include files are needed with the C compiler which will be installed after the system install is complete. The NFS shared libraries and header files also need to be installed for the C compiler.

Change software view to products: view->change software view->start with products
Unmark for Install:
_____ NFS->Runtime->NIS-CLIENT
_____ NFS->Runtime->NFS-CLIENT
_____ Networking->MinimumRuntime->PPP-RUN

Mark for install:
_____ MailUtilities->Runtime
_____ Networking->Development->NET-PRG
_____ ProgSupport->Runtime
_____ SOE
_____ SecurityMon
_____ Streams->Runtime->STREAMS-32SLIB

_____ SystemAdmin->Runtime
_____ TextEditors->Runtime
_____ X11->MinimumRuntime->MOTIF-SHLIB, X11R5-SHLIBS, X11R6-SHLIBS
_____ X11->Runtime-> MOTIF-SHLIB, X11R5-SHLIBS, X11R6-SHLIBS
_____ NFS->Runtime->NFS-CORE, NFS-KRN, NFS-SHLIBS
_____ NFS->Development->NFS-PRG

Actions->Install (analysis)

After the system installs and reboots, log in and change the networking startup variables so that the machine will be on the network whenever the system reboots.

Add route to /etc/rc.config.d/netconf:
_____ Uncomment ROUTE_DESTINATION[0]=default
_____ Uncomment ROUTE_GATEWAY[0] and add the IP address of the gateway
_____ Uncomment ROUTE_COUNT[0]= and add the count (usually 1 if using a router on the same subnet)

INSTALL ADDITIONAL PRODUCTS
The C compiler is needed to compile ssh, lsof, and tcp_wrapper. Since this is a prototype for a generic application server, the compiler is usually needed for the application development. The bundle for the C compiler is on Application CD #3 (part number B3782-10465). This software needs to be purchased when the system is purchased, and a codeword is sent with the four application CDs (which is depicted in the command below as THECODEWORD).

_____ mount the CD (replace CD_DEVICE with correct device):
mount /dev/dsk/CD_DEVICE /cdrom
_____ /usr/sbin/swinstall –x autoreboot=true -codeword=THECODEWORD -s /cdrom B3901BA

INSTALL LATEST PATCHES FROM CD
Patch the system with the support plus bundle CD. Bring up swinstall in interactive mode. (fileset XSWGR1100) (this will choose the appropriate patches for what is currently installed)

_____ mount /dev/dsk/CD_DEVICE /cdrom
_____ /usr/sbin/swinstall –x autoreboot=true –x match_target=true –s /cdrom XSWGR1100

INSTALL IGNITE-UX
Also on the Support Plus CD is the Ignite-UX bundle for backup and to make an Ignite Golden Image. Start swinstall in interactive mode, choose and mark the following filesets and install.

_____ Ignite-UX.BOOT-KERNEL

_____ Ignite-UX.FILE-SRV-11-00
_____ Ignite-UX.MGMT-TOOLS
_____ Ignite-UX.RECOVERY

INSTALL SECURITY PATCHES

_____Check new security patches at ftp://europe-ffs.external.hp.com/export/patches/hp-ux_patch_matrix under Current Patches for Security Issues – s800 11.00 and compare against what is on the system by running the swlist –l fileset command.
_____ ftp the security patches that are needed on the system from: ftp://us-ffs.external.hp.com/hp-ux_patches/s700_800/11.X[1] and install.

CONVERT TO TCB AND TURN ON AUDITING

Once this is done and the system comes back up, the first thing that should be done is to convert the passwd file to the tcb (trusted computing base) format, which creates a "shadow" passwd database in /tcb/files/auth and enables rules related to the passwords that can be used. This will also enable the use of auditing. Another advantage from converting to the trusted system is that the default umask changes to 07077. The root password needs to be changed, because converting to tcb replaces all current passwords with a "*". This can also be done through sam (System Administration Manager). The /.secure directory is the default directory to use for auditing logs, but it is preferable to have this information in /var rather than the root filesystem. The directory needs to be created and the data moved to the new directory. Use the command line to convert to tcb, and then use sam to enable the auditing. The log locations, sizes, and events to be monitored can be chosen here, however, in this case the default sizes are sufficient, and the events of admin (monitoring all administrative and privileged events) and login (monitoring all logins and logouts) are sufficient as well.

_____ /usr/lbin/tsconvert
_____ passwd root (*do not write root password here*!)
_____ mkdir /var/.secure
_____ chmod 500 /var/.secure
_____ mv /.secure/* /var/.secure
_____ rm –r /.secure; ln –s /var/.secure /.secure
_____ sam
Auditing and Security ->Audited Events ->Actions->Turn auditing on

CHANGE ROOT HOME DIRECTORY

The home directory for root should be changed to /root and the directory created and updated in the tcb.

_____ mkdir /root
_____ chmod 700 /root
_____ mv /.profile /root
_____ vi /etc/passwd (change home directory to /root)

[1] See appendix A for a list of the current (as of 2/14/01) security patches that are out for HP-UX 11.0

_____ pwconv

RESTRICT ROOT LOGIN

The root user should not be able to log in from a remote machine. This can be restricted to allow root to log in on the console only. Create an account for yourself so you can log in remotely if needed.

_____ useradd –u UID –g GID –d YOUR_DIRECTORY –s /usr/bin/sh –m –k /etc/skel YOUR_USERID
_____ echo “console” > /etc/securetty
_____ chown root:root /etc/securetty
_____ chmod 400 /etc/securetty

NETWORK TUNING

HP-UX, with release 11.00, now supports the use of ndd for network turning. The below changes can be made to protect from various network attacks. Unless there has been a patch, as far as I know, ndd –c can only handle 10 tunables in the nddconf.

_____ edit /etc/rc.conf.d/nddconf and add the following (there should only be comments in the file that came with the system):

```
        TRANSPORT_NAME[1]=ip
        NDD_NAME[1]=ip_forward_directed_broadcasts
        NDD_VALUE[1]=0

        TRANSPORT_NAME[2]=ip
        NDD_NAME[2]=ip_forward_src_routed
        NDD_VALUE[2]=0

        TRANSPORT_NAME[3]=ip
        NDD_NAME[3]=ip_forwarding
        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]=ip
        NDD_NAME[7]=ip_check_subnet_address
        NDD_VALUE[7]=0

        TRANSPORT_NAME[8]=ip
        NDD_NAME[8]=ip_respond_to_echo_broadcast
        NDD_VALUE[8]=0
```

_____ ndd -c

RESTRICT GLOBAL PRIVILEGES

In HP-UX there is a feature known as privilege groups, which assigns a privilege to a group. By default, the CHOWN privilege is a global privilege which applies to all groups, and would allow non-privileged users to chown files to other users. To turn this "feature" off, the /etc/privgroup file needs to be created. The /sbin/init.d/set_prvgrp is run by default at system startup if the /etc/privgroup file exists.

_____ echo –n > /etc/privgroup
_____ chown root :root /etc/privgroup
_____ chmod 400 /etc/privgroup
_____ /sbin/init.d/set_privgrp start

REMOVE UNNEEDED USERS

The HP-UX install comes with default users installed, all of which have "*" in the password field in the passwd file. However, it is best to remove them since they are not needed. Two default userids that should be removed are hpdb and www.

_____ userdel hpdb
_____ userdel www

BECOME DNS CLIENT

Because this machine is to be a DNS client, and it is inside the firewall, create the resolv.conf file with trusted internal DNS servers and with the local domain set and the domain to search. Then create the nsswitch.conf file by copying the default and modifying it to look at DNS when looking up a hostname.

_______________ Local domain of internal network ($LOCALDOMAIN)
_______________ Search domainname ($SEARCHDOMAIN)
_______________ IP address of internal DNS server ($IPADDRESS)
_____ echo "domain $LOCALDOMAIN" > /etc/resolv.conf (replace $LOCALDOMAIN with Local domain written above)
_____ echo "search $SEARCHDOMAIN" >> /etc/resolv.conf (replace $SEARCHDOMAIN with Search domain written above)
_____ echo "nameserver $IPADDRESS" >> /etc/resolv.conf (replace $IPADDRESS with IP address written above)
_____ cp /etc/nsswitch.files /etc/nsswitch.conf
_____ edit /etc/nsswitch.conf and change hosts entry from files to dns

_____ chown root:root /etc/resolv.conf /etc/nsswitch.conf
_____ chmod 444 /etc/resolv.conf /etc/nsswitch.conf

DISABLE SENDMAIL STARTUP

Sendmail will be used only to send mail out from the machine, such as application userids sending email to their internal exchange accounts. Therefore, the sendmail that comes with the operating system is sufficient. The startup for sendmail has to be disabled, and this will be done by changing the startup variable and, as a precaution, removing the startup and shutdown symbolic links. A cron job to run the sendmail queue every hour needs to be put in place as well.

_____ edit /etc/rc.config.d/mail and change the following line to look like this:
export SENDMAIL_SERVER=0
_____ rm /sbin/rc2.d/S540sendmail /sbin/rc1.d/K460sendmail
_____ crontab –e (add the following line and save:)
0 * * * * /usr/sbin/sendmail –q

DISABLE UNNEEDED SERVICES

There are several startup scripts that should be disabled as the services they start up are not needed for this installation, or are insecure. This will be done by editing the variables that are read at boot time in the files in the /etc/rc.config.d directory. Even though changing the variables in the /etc/rc.config.d scripts will stop the services from starting, the /sbin/rc*.d links for startup and shutdown will be removed as added protection, so that if these variables get changed by someone in the future, the services still will not start up.

_____ cd /etc/rc.config.d
Edit each of the below files and change the value of the VARIABLE to 0:

	FILE	VARIABLE
_____	SnmpHpunix	SNMP_HPUNIX_START
_____	SnmpMaster	SNMP_MASTER_START
_____	SnmpMib2	SNMP_MIB2_START
_____	SnmpTrpDst	SNMP_TRAPDEST_START
_____	comsec	TTSYNCD
_____	hparamgr	HPARAMGR_START_STOP
_____	hparray	HPARRAY_START_STOP
_____	netconf	All daemon variables in this file should be 0 (default)

_____ cd /etc/rc2.d
_____ rm S560SnmpMaster S565SnmpHpunix S565SnmpMib2 S565SnmpTrpDst
_____ rm S440comsec S710hparamgr S710 hparray
_____ rm S370named S490mrouted S510gated S565OspfMib
_____ rm S520rdpd S525rarpd S530rwhod S610rbootd
_____ cd /etc/rc1.d
_____ rm K435SnmpHpunix K435SnmpMib2 K435SnmpTrpDst K440SnmpMaster
_____ rm K560comsec K290hparamgr K290hparray K435OspfMib
_____ rm K630named K510mrouted K490gated

______ rm K390rbootd K470rwhod K475rarpd K480rdpd

OTHER STARTUP CHANGES and NTP CONFIGURATION

In order to see what it starting up at boot time via the console, it is a good idea to have list_mode turned on. Logging for the inetd daemon should be turned on and the variable for xntp changed so that xntp will startup up at boot time. The configuration file for xntp must be created for the to become a client to the internal NTP servers, which are in a master/slave relationship with an "Outside Server" that gets its timing information from the external internet. Get the IP addresses of the internal NTP servers; we use three internal ntp servers which are peered with other internal servers.

______ edit list_mode file and change LIST_MODE variable value to 1
______ edit netdaemons file and change INETD_ARGS variable value to "-l", and XNTP to 1
______________________ INTERNAL NTP SERVER #1 ($NTPSERVER1)
______________________ INTERNAL NTP SERVER #2 ($NTPSERVER2)
______________________ INTERNAL NTP SERVER #3 ($NTPSERVER3)
______ touch /etc/ntp.conf
______ edit /etc/ntp.conf and add the following:

```
driftfile /etc/ntp.drift

server $NTPSERVER1
server $NTPSERVER2
server $NTPSERVER3

restrict default nomodify
```

______ chown bin:bin /etc/ntp.conf
______ chmod 444 /etc/ntp.conf

______ At this point, reboot the system and make sure all the changes made above have taken effect.

COMPILE and INSTALL TCP_WRAPPER

To compile tcp_wrapper some changes will need to be made to a couple of the .c files to comment out yp_get_default_domain since NIS is not installed on this system.

______ Download tcp_wrapper source from ftp://ftp.porcupine.org/pub/security/tcp_wrappers_7.6.tar.gz
______ Unpack: /usr/contrib/bin/gunzip –c tcp_wrappers_7.6.tar | tar xvf –
______ cd tcp_wrappers_7.6
______ Changes to the Makefile:

```
Uncomment and change: REAL_DAEMON_DIR=/usr/lbin
Change: FACILITY=LOG_AUTH
```

______ Copy hosts_access.c to hosts.access.c.orig
______ Edit hosts.access.c to remove the following lines (line numbers 261-269).

```
#ifdef NETGROUP
```

```
                static char *mydomain = 0;
                if (mydomain == 0)
                        yp_get_default_domain(&mydomain);
                return (innetgr(tok + 1, eval_hostname(host), (char *) 0, mydomain));
        #else
                tcpd_warn("netgroup support is disabled");      /* not tcpd_jump() */
                return (NO);
        #endif
```

_____ Edit workarounds.c and remove the following lines (line numbers 189-200).

```
        #ifdef USE_GETDOMAIN

        int     yp_get_default_domain(ptr)
        char  **ptr;
        {
                static char mydomain[MAXHOSTNAMELEN];

                *ptr = mydomain;
                return (getdomainname(mydomain, MAXHOSTNAMELEN));
        }

        #endif /* USE_GETDOMAIN */
```

_____ make hpux10 (NOTE: There was no hpux11 in the Makefile, hpux10 works fine)

_____ Copy the compiled tcpd, tcpdmatch, tcpdchk, safe-finger, and try-from to /opt/local/bin

_____ Change permissions on the above to 555 and the owner to root:bin

_____ mkdir /opt/local /opt/local/lib /opt/local/include

_____ chmod –R 755 /opt/local; chown –R root:bin /opt/local

_____ cp libwrap.a /opt/local/lib/

_____ chmod 444 /opt/local/lib/libwrap.a; chown root:bin/opt/local/lib/libwrap.a

_____ cp tcpd.h /opt/local/include/

_____ chmod 555 /opt/local/include/tcpd.h; chown root:bin /opt/local/include/tcpd.h

_____ ln –s /opt/local/include/tcpd.h /usr/include/tcpd.h

Now that tcp_wrapper is on the machine, it needs to be enabled. A hosts.allow file needs to be put in place to ensure that only machines from the required domains can log in, and a host.deny can also be put in place to deny certain machines as well. In this case, hosts in our domain will be allowed to connect using telnet, and everyone will be denied ftp. If ftp is needed in the future, as it is for some applications, the allowed hosts can be added to the /etc/hosts.allow. The inetd.conf file needs to be edited to install the wrapper and all unneeded services should be disabled, and the inetd daemon restarted. The only thing that needs to be active on the application systems is telnet and ftp.

_____ cp /etc/inetd.conf /etc/inetd.conf

_____ edit /etc/inetd.conf and remove (or comment out) everything BUT the following 2 lines:

```
        ftp          stream tcp nowait root /usr/lbin/ftpd  ftpd -l
```

        telnet   stream tcp nowait root /usr/lbin/telnetd telnetd
______ Change the above 2 lines to add tcpd:
        ftp   stream tcp nowait root /opt/local/bin/tcpd /usr/lbin/ftpd ftpd -l
        telnet   stream tcp nowait root /opot/local/bin/tcpd /usr/lbin/telnetd telnetd
______ chmod 600 /etc/hosts.allow
________________ Internal domain (starts with . , eg, .us.nortel.com) ($DOMAIN)
_______ echo "telnetd: ALL : $DOMAIN" > /etc/hosts.allow (replace $DOMAIN with the domain written above)
______ touch /etc/hosts.deny
______ chown root:root /etc/hosts.allow /etc/hosts.deny
______ chmod 600 /etc/hosts.allow /etc/hosts.deny
______ echo "ftpd: ALL : ALL > /etc/hosts.deny
______ /etc/inetd –c (to re-read the configuration file)

COMPILE and INSTALL SSH

To make connections to and from the machine as secure as possible, ssh will be used. It will be compiled using the tcp_wrapper libwrap.a. Remote telnet connections to the machine from internal machines will not be forced to use ssh, because some systems within the company do not yet use ssh. Connections from machines other than machines on the internal domains listed in the hosts.allow will only be allowed to connect using ssh. Users on the system can be forced to use ssh. However, in the HP-UX operating system, rsh is restricted shell to restrict users during login, and the command remsh is remote shell. In order to compile using using the links to ssh, rsh is copied to another location and rsh will be linked to remsh. ssh1 is being used on other systems in this company, so ssh1 is what will be downloaded and compiled for compatability reasons. Because unix daemons can sometimes die unexpectedly, a script will be created and run from inittab, rather than from /sbin/rc3.d.

______ mv /usr/bin/rsh /bin/rsh_shell
______ cd /usr/bin
______ mkdir orig
______ chmod 755 orig; chown root:bin orig
______ cp remsh rsh; chmod 4555 rsh; chown root:bin rsh
______ cp remsh orig
______ cp rsh orig
______ cp rlogin orig
______ cp rcp orig
______ cd /home/your_directory
______ download ssh-1.2.31.tar.gz from ftp://metalab.unc.edu/pub/packages/security/ssh/
______ Unpack: /usr/contrib/bin/gunzip –c ssh-1.2.31.tar.gz | tar xvf –
______ cd ssh-1.2.31
______ ./configure --prefix=/opt/local --with-none --with-libwrap=/opt/local/lib –with-rsh=/usr/bin/orig/rsh --program-transform-name='s/^s/r/' --with-etcdir=/opt/local/etc --without-x --disable-server-x11-forwarding --disable-client-x11-forwarding --disable-suid-ssh
______ make

______ Edit server-config.sample (becomes sshd_config), and change the following lines (changes in blue)

```
        PermitRootLogin        no
        IgnoreRhosts           yes
        X11Forwarding          no
        PermitEmptyPasswords        no
```

______ make –n install (to verify file destinations)

______ make install

______ cd /usr/bin

______ rm rsh remsh rcp rlogin

______ ln –s /opt/local/bin/ssh rsh

______ ln –s /opt/local/bin/ssh remsh

______ ln –s /opt/local/bin/ssh rlogin

______ ln –s /opt/local/bin/scp rcp

______ touch /opt/local /etc/sshd_start.sh

______ edit /opt/local/etc/sshd_start.sh and insert the following lines:

```
        /opt/local/sbin/sshd

        sleep 60

        while [ `(echo hello ; sleep 5) | telnet localhost 22 2>/dev/null | wc -l` -ne 1 ]
        do
                sleep 300
        done
```

______ chown root:bin /opt/local/etc/sshd_start.sh; chmod 755 /opt/local/etc/sshd_start.sh

______ echo “sshd:234:respawn:/opt/local/etc/sshd_start.sh” >> /etc/inittab

______ init q

______ echo “ssh : ALL” >> /etc/hosts.allow

COMPILE and INSTALL LSOF

Another tool that is good to have on the system is lsof. This will help not only with security, but with system administration as well. AUTHOR NOTE: Normally, the lsof source would be downloaded from ftp://vic.cc.purdue.edu/pub/tools/unix/lsof/, but I was unable to retrieve it from this location.

______ Download lsof-4.51-ss-11.00.tar.gz from http://hpux.cs.utah.edu/hppd/hpux/Sysadmin/lsof-4.51/

______ Unpack: /usr/contrib/bin/gunzip –c lsof-4.51-ss-11.00.tar.gz | tar xvf –

______ ../Configure hpux and answer the below questions as follows:

```
        Do you want to take inventory?  Y
        Do you want to customize? N
```

______ make

______ cp lsof /opt/local/bin

______ chown bin:sys /opt/local/bin/lsof

______ chmod 2755 /opt/local/bin/lsof

MISCELLANEOUS

There are a few miscellaneous things that can be done to tighten up the security and space on the system. The saved patches can be removed which will recover a lot of space in /var, which will be needed for logs. There is a patch for syslogd that can prevent it from listening on the network for remote log messages that needs to be installed, and the /etc/motd file needs to have the legal message approved by the company's legal and corporate security departments warning users of the legal consequences of logging in to this system unauthorized.

To remove saved patches:
_____ swmodify –x patch_commit=true '*.*'

/etc/motd:
_____ edit /etc/motd and add the company's legal version of the warning

syslogd patch:
_____ download patch into /tmp: ftp://ftp.itrc.hp.com/superseded_patches/hp-ux_patches/s700_800/11.X/PHCO_21023
_____ cd /tmp; sh PHCO_21023
_____ swinstall -x autoreboot=true -x patch_match_target=true -s /tmp/PHCO_21023.depot
_____ edit /sbin/init.d/syslogd and change the line:

```
    /usr/sbin/syslogd -D &&
    to read
    /usr/sbin/syslogd -DN &&
```

CREATE IGNITE BOOT IMAGE/RECOVERY TAPE

This will create a bootable system recovery tape and can also be used to ignite other new systems to have the same configuration that was set up in this document if the hardware is supported with the same system configuration. This can also serve as the baseline for the system.

_____ /opt/ignite/bin/make_recovery -Ai

_____ YOU ARE DONE!

APPENDIX A

List of current security patches for HP-UX 11.00:

PHCO_21492 s700_800 11.0 Software Distributor (SD-UX) Cumulative Patch
PHCO_21534 s700_800 11.00 patch for shutdown(1M)
PHCO_21993 s700_800 11.00 auto_parms/set_parms
PHCO_22096 s700_800 11.00 cumulative newgrp(1) patch
PHCO_22365 s700_800 11.00 lpspool subsystem cumulative patch
PHCO_22665 s700_800 11.00 kermit(1) patch
PHCO_22686 s700_800 11.00 top(1) cumulative patch
PHCO_22923 s700_800 11.00 libc cumulative patch
PHCO_23088 s700_800 11.00 man(1) patch
PHCO_23117 s700_800 11.00 bdf(1M) cumulative patch
PHCO_23118 s700_800 11.00 df(1M) cumulative patch
PHKL_22589 s700_800 11.00 LOFS, select(), IDS/9000 and umount race fix
PHNE_16295 s700_800 11.00 vacation patch.
PHNE_17949 s700_800 11.00 Domain Management (DESMS B.01.12)
PHNE_18017 s700_800 11.00 Domain Management (DESMS-NS B.01.11)
PHNE_18546 s700_800 11.00 sendmail(1m) 8.9.3 patch
PHNE_20619 s700_800 11.00 Bind 4.9.7 components
PHNE_21731 s700_800 11.00 r-commands cumulative mega-patch
PHNE_21835 s700_800 11.00 inetd(1M) cumulative patch
PHNE_21936 s700_800 11.00 ftpd(1M) and ftp(1) patch
PHNE_22125 s700_800 11.00 ONC/NFS General Release/Performance Patch
PHNE_22397 s700_800 11.00 cumulative ARPA Transport patch
PHSS_16649 s700_800 11.00 Receiver Services October 1998 Patch
PHSS_17483 s700_800 11.00 MC/LockManager A.11.05 (English) Patch
PHSS_17484 s700_800 11.00 MC/LockManager A.11.05 (Japanese) Patch
PHSS_17496 s700_800 11.00 Predictive C.11.0[0,a-m] cumulative patch
PHSS_17581 s700_800 11.00 MC ServiceGuard 11.05 Cumulative Patch
PHSS_21046 s700_800 11.00 OV EMANATE14.2 Agent Consolidated Patch
PHSS_21326 s700_800 11.00 OV OB2.55 patch - DA packet
PHSS_21637 s700_800 11.00 OV OB2.55 patch - WindowsNT packet
PHSS_22341 s700_800 11.00 CDE Runtime NOV2000 Periodic Patch
PHSS_22424 s700_800 11.00 OV NNM6.1 Consolidated Patch 10/08/2000
PHSS_22678 s700_800 11.X Continental Clusters A.02.00
PHSS_22683 s700_800 11.X MC/ServiceGuard and SG-OPS Edition A.11.09
PHSS_22936 s700_800 11.00 AudioSubsystem Dec 2000 Periodic Patch
PHSS_23266 s700_800 11.00 Support Tool Manager A.21.00 A.21.05
PHSS_23269 s700_800 11.00 Support Tool Manager A.22.00 Patch
PHSS_23332 s700_800 11.00 Support Tool Manager Patch

REFERENCES:

Building a Bastion Host using HP-UX 11 by Kevin Steves
For format, the paper recommended at
http://ww.sans.org/y2k/practical/Jeff_Campione_GCUX.htm
The HP-UX documentation at docs.hp.com
The class materials from Track 6

Last Updated: September 21st, 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**