DISCLAIMER : This document is nothing more than the musings of the author as he attempts t

In this documentation, screen outputs will be presented in green. Where keyboard inputs are required, the prompt will be as #

ls -al

means you should type ls -al at the super user prompt.

This document assumes you have already set up Solaris. For instructions on installing Solaris, See http://www.wwwpages.com/solaris-lab/1404-is10u11113zfs.html

Mirror Drives

If you have two drives in the system, and the current boot drive is smaller or equal size to the other, you can mirror them with ZFS.

 # zpool attach rpool c0t0d0s0 c0t1d0s0

Our existing drive is c0t0d0s0 and we want to attach c0t1d0s0 to it. You may be prompted to use the -f if the new drive has already been in a pool.

While it is a fairy quick process, you can follow the progress of the resilver with

 # zpool status -v

Adding Users and Groups

Currently, our only user is 'root'. Logging in as root is a bad idea, and we will be disabling root logins shortly. Before we can do this, we need to create a group for users, and then add users. Below I am creating a group called 'users' and giving it a group id of 100. Then I am creating a user called 'me', assigning it a user id of 101, assigning it to group 100, setiing it's default shell to /bin/bash, and then setting a password for the user. You can repeat this process as needed, but do not assign two users the same user id.

 # groupadd -g 100 users
 # useradd -u 101 -g 100 -md /home/me -c "Its Me" -s /bin/bash me
 # passwd me

now we will set the password to not expire. You MUST do this for root. If the root password expires, you have to boot into single user mode to reset it, which is a pain! You can modify users accounts by changing the word root below to other usernames.

 # passwd -x -1 root

now change the 3 failed attempts locking the user account.

 # usermod -K lock_after_retries=no root

Power Management

Next we are going to disable power management. This is necessary for me, because my work related systems run 24/7 and can't afford the delay of being woken up from a Power Management induced sleep.

 # vi /etc/power.conf

Change the autopm line from default to disable

save the file, then restart the power service

 # svcadm restart power

Change Root's Home Directory and Shell

 # cd /
 # mkdir root
 # chmod 700 root
 # chown root:root root

Edit /etc/passwd and change the first line from

root:x:0:0:Super-User:/:/sbin/sh
to
root:x:0:0:Super-User:/root:/bin/bash

now go back to / and delete any hidden files (files starting with a .)

Make Root a Role

To perform this step, you can not have logged in as root. Log in as a normal user and then:

$ su -
 # usermod -K type=role root

verify the change

 # grep root /etc/user_attr

now set your user account up to be able access the root role

 # usermod -R root youruser (replace youruser with an actual username).

 # echo "" > /var/adm/wtmpx

Verify everything took:

 # grep root /etc/user_attr

root::::type=role;auths=solaris.*,solaris.grant;profiles=Web Console Management,All;lock_after_retries=no;clearance=admin_high;min_label=admin_low
youruser::::type=normal;lock_after_retries=no;roles=root

Configure the Basic Auditing and Reporting Tool

This tool allows the system administrator to monitor changes to critical system files.

 # groupadd -g 10100 bartadm
 # useradd -d /bartadm -g 10100 -m -s /bin/pfsh -u 10100 bartadm
 # passwd -N bartadm
 # chmod 750 /bartadm
 # cd /bartadm
 # rm *
 # rm .profile

Edit /**etc/security/prof_attr** and add the following line:

File Integrity:::File Integrity Management:

Edit /**etc/security/exec_attr** and add the following line:

File Integrity:solaris:cmd:::/usr/bin/bash:privs=file_dac_read,file_dac_search

Assign the profile to bartadm

 # usermod -P "File Integrity" bartadm

Verify the profile

 # grep "^bartadm" /etc/user_attr

should output

bartadm::::type=normal;profiles=File Integrity

Clean Up System

remove groups and accounts that are not needed

 # groupdel lp
 # groupdel uucp
 # groupdel nuucp
 # groupdel sysadmin

 # userdel lp
 # userdel -r uucp
 # userdel -r nuucp

change ownership of files owned by nouser or nogroup

 # find / -nouser -exec chown root {} ;
 # find / -nogroup -exec chgrp sys {} ;

 # chmod 755 /etc/lp
 # svcadm disable ipp-listener

Delete Unused Packages

We are going to delete some packages that we don't need. It is important to use Oracle provided packages where ever possible because they maintain them with their Critical Patch Upgrade process. If you remove the Oracle patch for Apache (for instance) and then install apache from another source, the CPU will not patch it. When attempting to install software, check the installation cd to see if the package is available there.

If you intend on using one of these products, don't remove the package. I'm removing the packages I don't need.

- Mozilla -
 # pkgrm SUNWmozapoc-adapter
 # pkgrm SUNWmozchat
 # pkgrm SUNWmozdom-inspector

 # pkgrm SUNWmozgm
 # pkgrm SUNWmozilla
 # pkgrm SUNWmozilla-devel

 # pkgrm SUNWmozjs-debugger
 # pkgrm SUNWmozmail
 # pkgrm SUNWmoznspr

 # pkgrm SUNWmoznspr
 # pkgrm SUNWmoznss
 # pkgrm SUNWmoznss-devel

 # pkgrm SUNWmozpsm

 # pkgrm SUNWmozspell
 # pkgrm SUNWthunderbird

 # pkgrm SUNWthunderbird-calendar
- Samba -
 # pkgrm SUNWsmbac
 # pkgrm SUNWsmbar
 # pkgrm SUNWsmbau
- Apache 2 -
 # pkgrm SUNWapch2d
 # pkgrm SUNWapch2r
 # pkgrm SUNWapch2u
- Apache 1 -
 # pkgrm SUNWapchd
 # pkgrm SUNWapchr
 # pkgrm SUNWapchu
- 1394 Drivers -
 # pkgrm SUNW1394
 # pkgrm SUNW1394h
 # pkgrm SUNWav1394

 # pkgrm SUNWfwdc
 # pkgrm SUNWfwdcd
 # pkgrm SUNWfwdcu

 # pkgrm SUNWscsa1394
- Gnome Instant Messanger -
 # pkgrm SUNWgnome-im-client
 # pkgrm SUNWgnome-im-client-devel
 # pkgrm SUNWgnome-im-client-root
- MySql -
 # pkgrm SUNWmysqlr
 # pkgrm SUNWmysqlt
 # pkgrm SUNWmysqlu
- SIP Express Router -
 # pkgrm SUNWserweb
 # pkgrm SUNWseru
 # pkgrm SUNWserr
- PostgreSQL V8.1 -
 # pkgrm SUNWpostgr
 # pkgrm SUNWpostgr-contrib
 # pkgrm SUNWpostgr-devel

 # pkgrm SUNWpostgr-docs
 # pkgrm SUNWpostgr-libs
 # pkgrm SUNWpostgr-pl

 # pkgrm SUNWpostgr-server
 # pkgrm SUNWpostgr-server-data
- PostgreSQL V8.2 -
 # pkgrm SUNWpostgr-82-client
 # pkgrm SUNWpostgr-82-contrib
 # pkgrm SUNWpostgr-82-devel

 # pkgrm SUNWpostgr-82-docs
 # pkgrm SUNWpostgr-82-jdbc
 # pkgrm SUNWpostgr-82-libs

 # pkgrm SUNWpostgr-82-pl
 # pkgrm SUNWpostgr-82-server
 # pkgrm SUNWpostgr-82-server-data-root

 # pkgrm SUNWpostgr-82-tcl

Configure Login Restrictions

edit /**etc**/**default**/**login** and modify lines to read

RETRIES=3
SLEEPTIME=4
SYSLOG_FAILED_LOGINS=-0
edit /**etc**/**security**/**policy.conf** and modify lines to read

LOCK_AFTER_RETRIES=YES
CRYPT_ALGORITHMS_DEPRECATE=__unix__
CRYPT_DEFAULT=6

Configure Password Complexity

edit /**etc**/**default**/**passwd** and modify lines to read

PASSLENGTH=14
MINLOWER=1
MINUPPER=1
MINDIGIT=1
MINSPECIAL=1
MAXREPEATS=3
HISTORY=5
MAXWEEKS=8
MINWEEKS=1
MINDIFF=4
DICTIONLIST=/usr/share/lib/dict/words
DICTIONDBDIR=/var/passwd
and make the dictionary database
 # mkpwdict

Lock Down Logs and Other Files

 # cd /var/sadm/patch
 # find . -name log -type f -exec chmod 640 {} ;

 # cd /var/sadm/pkg
 # find . -name "*log" -type f -exec chmod 640 {} ;

 # cd /var/adm
 # chmod 640 *

 # cd /var/log
 # chmod 640 *

 # cd /var/saf/zsmon
 # chmod 640 log

Change man page permissions

 # find /usr/share/man/ -type f -exec chmod 644 {} ;

edit /**etc/pam.conf** and comment any reference to "*pam_rhost_auth*"

<<end of document>>