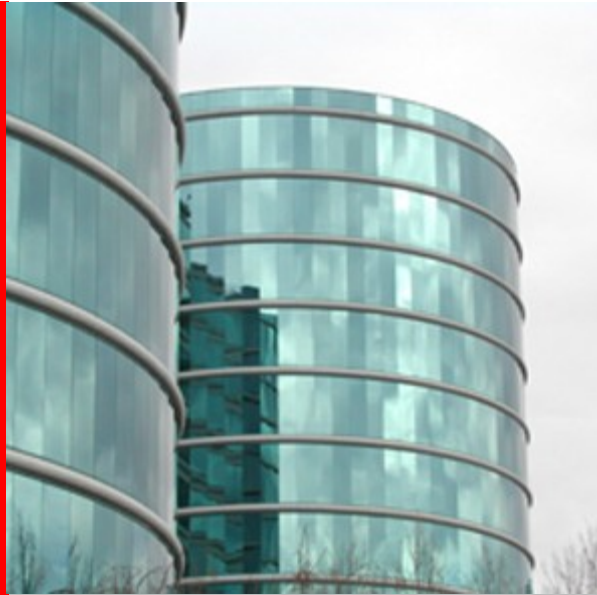


ORACLE®

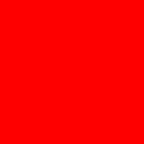


ORACLE[®]



Selected Solaris 11 Security Features: Theory and Practice

Brent Paulson
Solaris Security Engineering
Oracle Corporation



The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

IPFilter changes in S11

- Host Based Firewall
 - Simplified method of configuring IPFilter on a per-host basis
 - A new daemon, `svc.ipfd(1M)`, monitors changes to SMF services relating to the firewall configuration and updates the IPFilter configuration on-the-fly
 - A new per-service SMF property group named **firewall_config** stores the firewall policy configuration
 - Available for services like SSH, FTP, `in.rlogind`, etc.
 - These can be set using SMF commands or Visual Panels

IPFilter in Practice

- Host Based Firewall example
 - Block in.ftpd(1M) requests from a specific host:

```
$ svcadm enable ipfilter # default policy is none
```

```
$ svccfg -s ftp setprop firewall_config/policy = deny
```

```
$ svccfg -s ftp setprop firewall_config/apply_to =  
host:mothra.uk.oracle.com
```

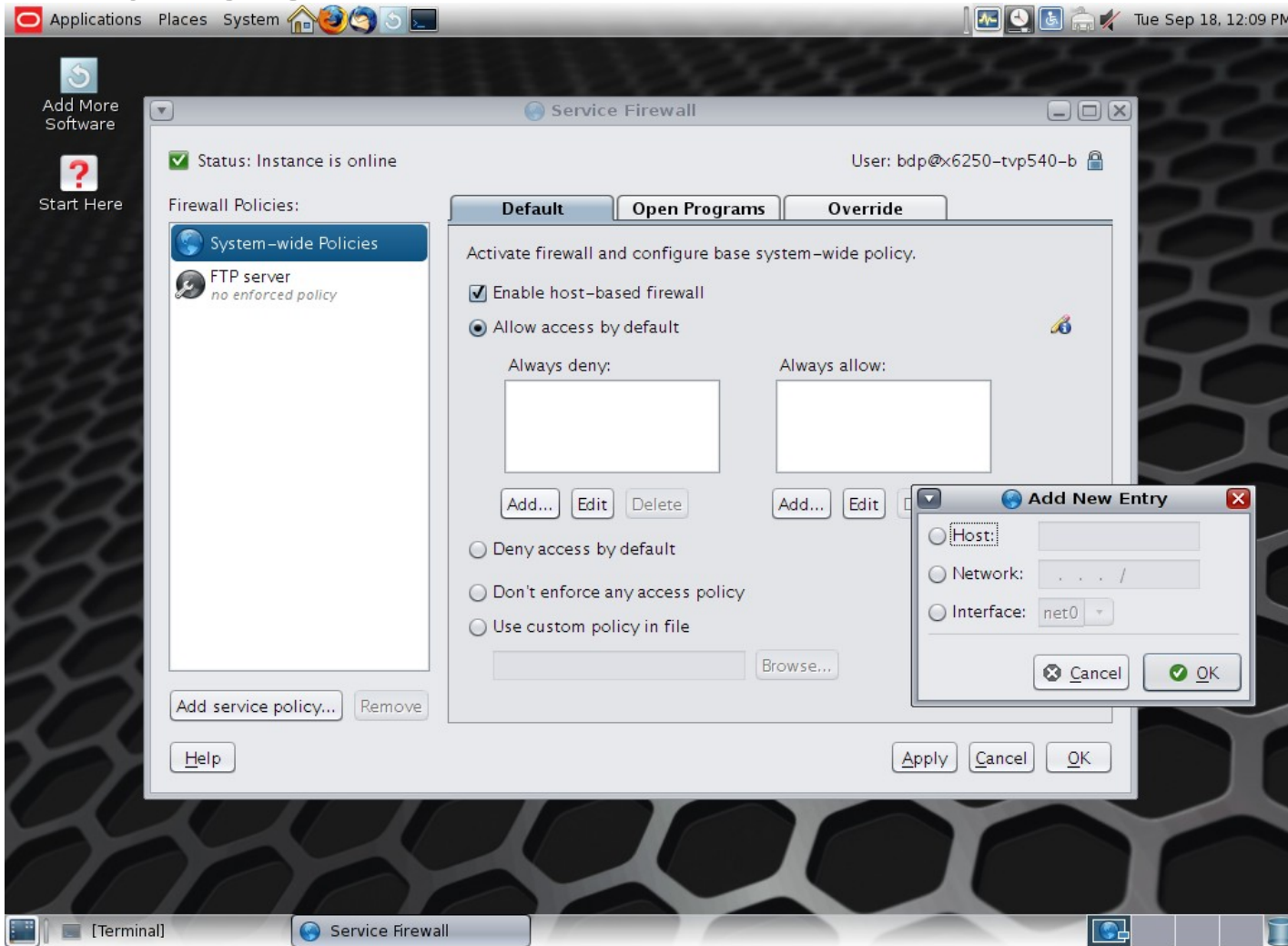
```
$ svcadm refresh ftp
```

```
dkp@mothra:~$ ftp remotehost
```

```
<nothing happens>
```

- More details in ipfilter(5) and svc.ipfd(1M)

IPFilter in Practice with Visual Panels



Audit changes in S11

- Solaris Auditing enabled by default
 - Reboot no longer required
 - Audit events in the 'lo' audit_class(4) are audited by default (logins, logouts, su(1M), etc.)
 - `$ auditrecord -c lo #` to see which events in the 'lo' class
- Audit configuration no longer in audit_control(4)
 - System-wide audit flags now set using '-setflags' to auditconfig(1M)
 - User audit flags set using '-K audit_flags=always:never' to usermod(1M) or rolemod(1M) (or useradd/roleadd)
 - Additional audit configuration done using auditconfig(1M)
 - audit_control(4) no longer exists

Audit changes in S11

- New **Audit Configuration** rights profile allows for all system-wide configuration using `auditconfig(1M)`
- A user or role with the `solaris.audit.assign` authorization can use `usermod(1M)` or `profiles(1)` to configure audit flags on a per-user or per-profile basis.
 - `audit_user(4)` and `audit_startup(4)` are now gone
- Per-user audit flags can be viewed using:

```
$ userattr audit_flags user  
lo,ad:no
```
- Auditing doesn't need to be enabled in the global zone to be enabled in non-global zones

Solaris Auditing in Practice

```
# usermod -P +"Audit Configuration" auditadm
auditadm:~$ auditconfig -setpolicy +perzone,zonename,argv
auditadm:~$ auditconfig -setflags lo,ua,as
# usermod -A +solaris.audit.assign -P +"User Security"
auditmgr
auditmgr:~$ usermod -K audit_flags=ex,ap:no dkp

dkp:~$ ssh remotehost /bin/date -u

# usermod -P +"Audit Review" auditusr
auditusr:~$ auditreduce -c ex -u dkp | praudit -x | xsltproc - |
lynx -stdin
```

Solaris Auditing in Practice

```
auditusr:~$ auditreduce -c ex -u dkp | praudit -x | xsltoproc - | lynx -stdin
```

```
Event: execve(2)
time: 2012-09-18 12:48:39.486 +01:00 vers: 2 mod: host: x6250-tvp540-b
PATH: /usr/bin/amd64/ksh
ATTRIBUTE mode: 100555 uid: root gid: bin fsid: 65538 nodeid: 33379
device: 18446744073709551615
EXEC_ARGS
arg: ksh
arg: -c
arg: /bin/date -u
SUBJECT audit-uid: dkp uid: dkp gid: staff ruid: dkp rgid: staff pid:
20625 sid: 3285340739 tid: 5629 202240 gojira.uk.oracle.com
RETURN errval: success retval: 0
Event: execve(2)
time: 2012-09-18 12:48:39.489 +01:00 vers: 2 mod: host: x6250-tvp540-b
PATH: /usr/bin/date
ATTRIBUTE mode: 100555 uid: root gid: bin fsid: 65538 nodeid: 17268
device: 18446744073709551615
EXEC_ARGS
arg: /bin/date
arg: -u
SUBJECT audit-uid: dkp uid: dkp gid: staff ruid: dkp rgid: staff pid:
20625 sid: 3285340739 tid: 5629 202240 gojira.uk.oracle.com
RETURN errval: success retval: 0
File: time: 2012-09-18 12:48:39.000 +01:00
```

Solaris Auditing in Practice

- Which users ran su(1M) in the past week?

```
auditusr:~$ auditreduce -m AUE_su -a $(date -d last-week +"%Y
%m%d" | praudit
```

- What were all of the commands a user ran while on the system?
 - First find their initial login audit record

```
auditusr:~$ auditreduce -c lo -u dkp | praudit
```

```
header,81,2,login – ssh,,x6250-tvp540-b,2012-09-18 13:07:34.755
+01:00
```

```
subject,dkp,dkp,staff,dkp,staff,20641,2689198737,6710 202240
gojira.uk.oracle.com
```

```
return,success,0
```

- Then identify their session-ID, identified in red above, and run:

```
auditusr:~$ auditreduce -s 2689198737 | praudit
```

SunSSH changes in S11

- New chroot(2) functionality using sshd **ChrootDirectory** keyword
- **ForceCommand** keyword – Forces execution of specified command; similar to 'command=...' in `$HOME/.ssh/authorized_keys`
 - Can be used to lock down an account by specifying a command like `gitshell`, `svnserve`, or `'rsync –server'`
- Support for conditional configuration using the sshd **Match** keyword
 - Limit features to specific users, groups, or hosts
 - Enforce granular feature access, e.g. `publickey` authentication only allowed for certain hosts or subnets

SunSSH in Practice

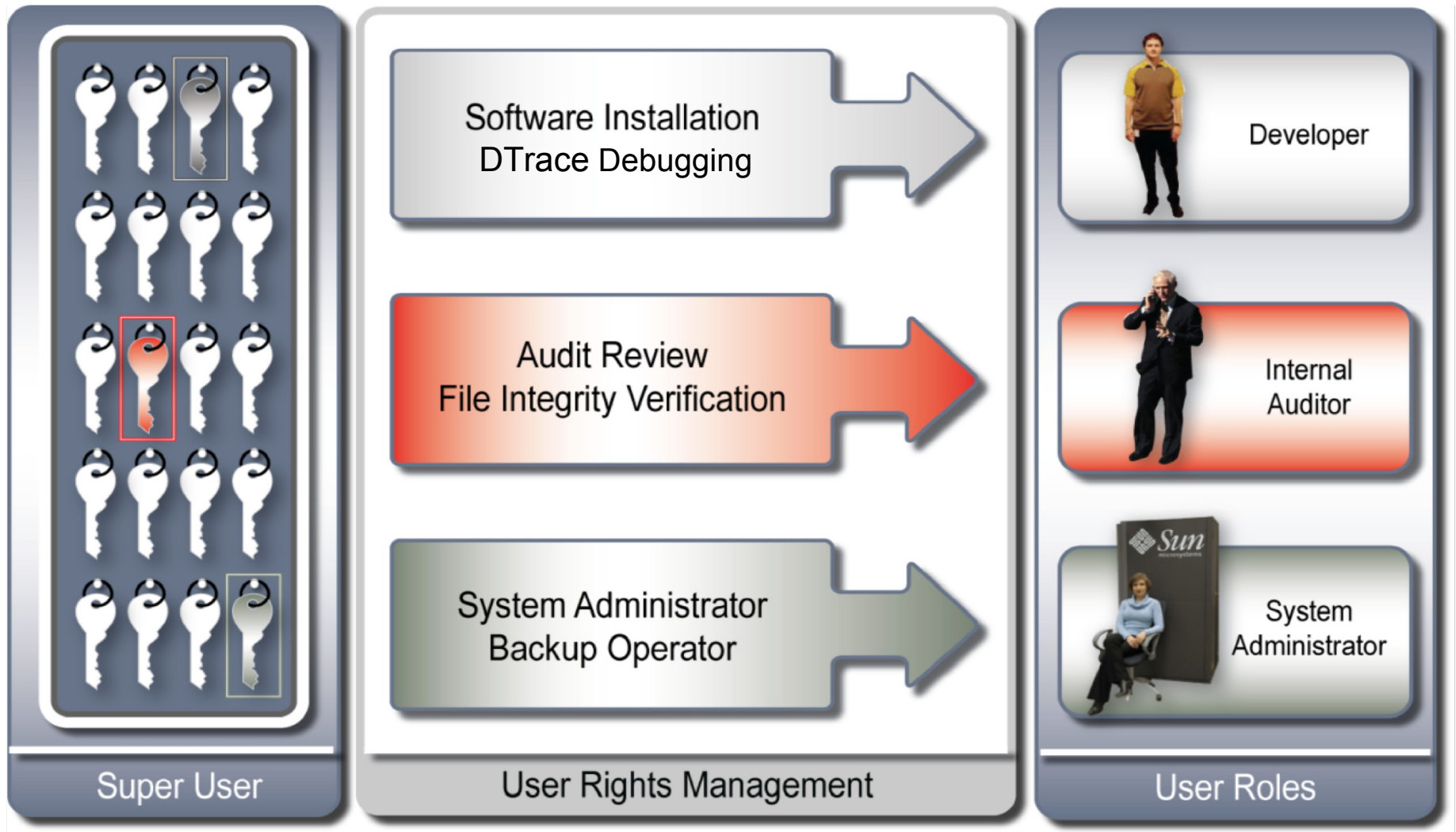
- Example:

```
$ cat /etc/ssh/sshd_config
Match User *,!root
    Banner /etc/banner
Match Host trusted.example.com
    PermitRootLogin yes
Subsystem sftp internal-sftp
Match Group sftp
    AllowTcpForwarding no
    X11Forwarding no
    ForceCommand internal-sftp
    ChrootDirectory %h
```

SunSSH changes in S11

- Ability to use the OpenSSL PKCS#11 engine for offloading cryptographic operations to the Cryptographic Framework using new **UseOpenSSLEngine** sshd and ssh keyword
 - Performance win especially for UltraSPARC T2 platforms
- Ability to use X.509 Certificates for authentication
 - Step-by-step commands in the sshd(1M) man page

Rights Management



RBAC changes in S11

- Root is a role by default:
 - LiveCD and Text Installer
 - Choice with AI Install
- Initial root password matches that of initial user but is expired and needs to be changed on first su(1M)
- Role authentication policy is configurable to require either user's or role's password
 - Uses the **roleauth** keyword to rolemod(1M) or roleadd(1M)

RBAC in Practice

- Create a role which will be used to manage the networking configuration on the system. Users will authenticate using their own password.

```
# roleadd -m -P "Network Management" -K  
roleauth=user netmgmt
```

- Assign this role to one or more users

```
# usermod -R +netmgmt dkp
```

```
dkp:~$ su - netmgmt
```

```
Password: <dkp's passwd>
```

```
netmgmt:~$ snoop -d net0
```

```
Using device net0 (promiscuous mode)
```

```
[...]
```

RBAC changes in S11

- New options to restrict access to files, networks, and applications
 - **Stop** rights profile stops processing authorizations and rights profiles
 - The simplest way to create a restricted shell
 - New basic privileges for locking down processes
 - **file_read** – read a file or directory
 - **file_write** – write to a file or directory
 - **net_access** – open a TCP, UDP, SDP, or SCTP endpoint
 - Privileges for setuid-to-root executables are specified in new **Forced Privileges** rights profile

RBAC in Practice

- Create a role which can only run the commands in the Audit Review rights profile.

```
# roleadd -m -P "Audit Review,Stop" -K  
roleauth=user auditor
```

- Assign this role to one or more users

```
# usermod -R +auditor dkp
```

```
dkp:~$ su – auditor
```

```
Password: <dkp's passwd>
```

```
auditor:~$ date
```

```
-ksh: date: cannot execute [Permission denied]
```

```
auditor:~$ auditreduce -c lo | praudit
```

```
[...]
```

RBAC changes in S11

- RBAC-enhanced Desktop
 - GNOME desktop automatically applies RBAC attributes for the user
 - New **Console User** rights profile
 - Automatically assigned to users logged in on /dev/console
 - Useful for workstation/laptop use cases
 - Power Management, WiFi/Network Configuration, suspend/resume, removable media management
 - Applications are invoked with granted privileges or role assumption dialogs

RBAC changes in S11

- LDAP support
 - Scope option added to RBAC and TX CLIs
 - -S ldap|files
 - Default for modifications is **files**
 - Default LDAP attributes are used
 - Client machine must be initialized with **admin** credential

- In Practice:

```
$ useradd -S ldap dkp
```

```
$ profiles -S ldap -p "Custom Profile" 'remove  
cmd=/usr/bin/cp; exit'
```

RBAC changes in S11

- New **User Management** rights profile allows users or roles to:
 - Create new user accounts with default attributes
 - Create new groups and manage existing groups
- **pfexec(1)** is now “in-kernel”
 - No longer a setuid program
- All standard shells (including bash, zsh, and tcsh) now available as profile shells
- A new process flag specifies that all execs are subject to RBAC policy
 - **ppriv(1)** shows: flags = PRIV_PFEEXEC
 - Transparent to programs, scripts, etc.

PAM: Pluggable Authentication Modules

- What is it?
 - A flexible, modular framework that provides a generic way to authenticate a user
 - PAM allows system administrators to choose any authentication service available on the system on a per-application basis
 - PAM lets you “plug in” new authentication services without changing the system entry services themselves like login, in.ftpd, and sshd.
 - Public, X/Open standard API used by nearly all UNIX or UNIX-like operating systems

PAM changes in S11

- New PAM module named **pam_tty_tickets(5)**
 - Provide credential caching a la sudo(1M)
 - After successful authentication a ticket is created in `/system/volatile/tty_tickets/<PAM_AUSER>/<PAM_USER>/<PAM_TTY>`
 - If a subsequent authentication attempt occurs within the configured timeout (default of 5 minutes) `pam_tty_tickets(5)` returns `PAM_SUCCESS`. If the timestamp on the ticket is older then the ticket is removed and the module returns `PAM_IGNORE`.

PAM changes in Practice

- Add these lines to /etc/pam.conf
su auth required pam_unix_cred.so.1
su auth sufficient pam_tty_tickets.so.1
su auth requisite pam_authok_get.so.1
su auth required pam_dhkeys.so.1
su auth required pam_unix_auth.so.1
dkp:~\$ su root -c /bin/date

Password:

Tuesday, September 18, 2012 01:53:38 PM BST

dkp:~\$ su root -c /bin/date

Tuesday, September 18, 2012 01:53:45 PM BST

New Virus Scan service in S11

- New SMF service
svc:/system/filesystem/vscan:icap, daemon
vscand(1M), and CLI vscanadm(1M)
- Leverages third-party scan engines like Symantec Antivirus Scan Engine, Trend Micro InterScan Web Security Suite, and McAfee Secure Internet Gateway
 - Can also be used with Clam AntiVirus (ClamAV)
- Also leverages ZFS and system attributes
- A virus scan is performed during open and close operations if the file hasn't been scanned before or if the file has been modified since last scanned

S11 Virus Scan in Practice

- Install a scan engine (Symantec or ClamAV or etc.)

- Enable the file system to allow virus scans

```
# zfs set vscan=on zpool/fs/mail
```

- Enable the vscan SMF service

```
# svcadm enable vscan
```

- Add a scan engine to the vscan service

```
# vscanadm add-engine -p host=<hostname with  
ICAP server> scan-engine-1
```

- Optionally configure types of files not to scan or limit size types with 'vscanadm set'.

S11 Virus Scan in Practice (cont'd)

- Attempts to open a file in /zpool/fs/mail will result in a scan first (if it hasn't already been scanned or changed since last scan) before allowing access

```
$ tail -1 /zpool/fs/mail/msg1
```

The End

```
$ cat /zpool/fs/mail/virus
```

```
cat: cannot open /zpool/fs/mail/virus: Permission denied
```

- The file has been quarantined (the av_quarantine attribute will be set) which means it can't be read, written, or renamed – only deleted.

```
$ cd /zpool/fs/mail/ ; ls -l v virus
```

```
-rw-r--r-- 1 root sys 4241 May 4 00:27 virus
```

```
{archive,nohidden,...,av_quarantined,...}
```

Zones changes in S11

- Immutable Zones – provide read-only system profiles for **solaris** non-global zones
 - The zone's configuration is preserved by implementing read-only root file systems for non-global zones
 - Additional restrictions are placed on the runtime environment
 - Unless performed as part of specific maintenance operations, modifications to system binaries or system configurations are blocked
 - The global zone can write to a non-global zone's file system for installation, image updates, and maintenance
 - Example:

```
# zonecfg -z ozone set file-mac-policy=fixed-configuration
```

ZFS changes in S11

- ZFS Encryption - `zfs_encrypt(1M)`
 - You can use existing storage pools as long as they are upgraded
 - ZFS encryption is inheritable to descendent file systems
 - Data is encrypted using AES (Advanced Encryption Standard) with key lengths of 128, 192, and 256 in the CCM and GCM operation modes.
 - ZFS encryption uses the Oracle Solaris Cryptographic Framework
 - ZFS encryption works with compression and deduplication
 - Example:

```
# zfs create -o encryption=on zpool/home/dkp  
Enter passphrase for 'zpool/home/dkp': xxxxxxxx  
Enter again: xxxxxxxx
```

ZFS Encryption in Practice

```
$ wget -o hamlet.txt  
http://www.gutenberg.org/dirs/etext98/2ws2610.txt  
# mkfile 64m /tmp/pool1_file  
# zpool create clear_pool /tmp/pool1_file  
# cp /tmp/hamlet.txt /clear_pool  
# grep -ic Hamlet /clear_pool/hamlet.txt  
113  
# zpool export clear_pool  
# strings /tmp/pool1_file | grep -ic Hamlet  
115
```

Two extra copies, one for the filename hamlet.txt as this is cleartext and one for metadata.

ZFS Encryption in Practice (cont'd)

- Now encrypt the filesystems in the pool

```
# mkfile 64m /tmp/pool2_file
```

```
# zpool create -O encryption=on encrypted_pool  
/tmp/pool2_file
```

```
Enter passphrase for 'encrypted_pool': xxxxxxxx
```

```
Enter again: xxxxxxxx
```

```
# cp /tmp/hamlet.txt /encrypted_pool
```

```
# grep -ic Hamlet /encrypted_pool/hamlet.txt
```

```
113
```

```
# zpool export encrypted_pool
```

```
# strings /tmp/pool2_file | grep -ic Hamlet
```

```
0
```


Q&A

Hardware and Software

ORACLE®

Engineered to Work Together

ORACLE®