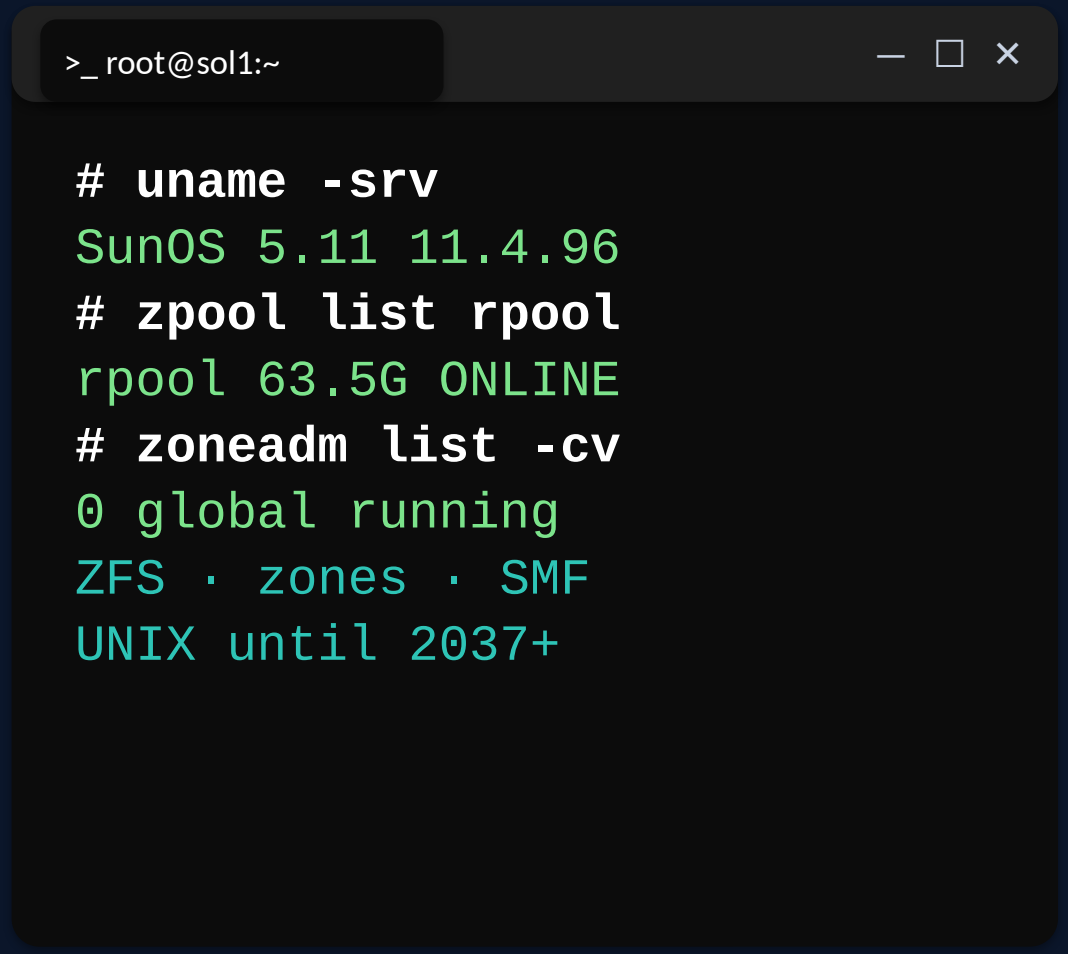


LESSON 7 OF 12

Oracle Solaris 11.4

ZFS · Zones · SMF · LDoms · OLVM

Users, RBAC, Compliance & Solaris Security

Full Course · Solaris 11.4 SRU96 · OVM (Nov 2026)

What You Will Learn in Lesson 7

- Users and groups: useradd, passwd, home directories on ZFS
- RBAC: authorizations, rights profiles, roles
- pfexec, profiles, roles, and sudo on Solaris
- Password policy and account lockout
- compliance: assess and report against benchmarks
- Security extensions: sxadm (ASLR, NXstack…), verified boot
- Auditing and file integrity (bart)

Users and Groups

```
root@sol1:~# groupadd -g 2001 webteam
root@sol1:~# useradd -m -u 2101 -g webteam -c 'Ali Ahmadi' -s /usr/bin/bash ali
root@sol1:~# passwd ali
root@sol1:~# zfs list | grep export/home        # each home is its own dataset
rpool/export/home/ali   35K  30.1G  35K  /export/home/ali
root@sol1:~# zfs set quota=5G rpool/export/home/ali
root@sol1:~# usermod -G webteam,staff ali ; id -a ali
root@sol1:~# passwd -s ali                      # password status
root@sol1:~# passwd -l ali ; passwd -u ali       # lock / unlock
root@sol1:~# userdel -r olduser
```

RBAC Building Blocks

Piece	Meaning / Example
Authorization	Permission for an action: solaris.smf.manage.apache
Privilege	Fine-grained kernel right: net_privaddr, file_dac_read
Rights profile	Bundle of commands, auths, privileges: 'Service Management'
Role	Special account with profiles; users assume it with su
Databases	/etc/security/prof_attr, exec_attr, auth_attr; /etc/user_attr
Principle	Least privilege: give profiles, not the root password

Rights Profiles and pfexec

```
root@sol1:~# getent prof_attr | grep -i 'Service Management'
root@sol1:~# profiles -p 'Network Management' info
root@sol1:~# usermod -P +'Service Management' ali     # add a profile to ali
root@sol1:~# usermod -A +solaris.smf.manage.apache ali
ali@sol1:~$ profiles
Service Management
Basic Solaris User
ali@sol1:~$ pfexec svcadm restart apache24     # allowed by the profile
ali@sol1:~$ pfbash                              # profile shell: no pfexec needed
ali@sol1:~$ ppriv $$                            # show process privileges
```

Roles and sudo

```
root@sol1:~# roleadd -m -P 'Network Management,Network Security' netadm
root@sol1:~# passwd netadm
root@sol1:~# usermod -R +netadm ali             # ali may assume netadm
ali@sol1:~$ roles
netadm
ali@sol1:~$ su - netadm                         # role password (or user's: roleauth)
netadm@sol1:~$ ipadm show-addr                  # role shell has the profiles
root@sol1:~# rolemod -K roleauth=user netadm    # authenticate with own password
# sudo also exists: visudo / /etc/sudoers.d — RBAC is the Solaris-native way
root@sol1:~# usermod -K type=role root          # root stays a role (default)
```

Password Policy and Lockout

File / Setting	Example
/etc/default/passwd	MINWEEKS=1 MAXWEEKS=13 PASSLENGTH=12 MINDIGIT=1 HISTORY=10
/etc/security/policy.conf	LOCK_AFTER_RETRIES=YES ; CRYPT_DEFAULT=6 (SHA-512)
/etc/default/login	RETRIES=3 ; CONSOLE=/dev/console (root logins)
usermod -K lock_after_retries=no	Exception for a service account
passwd -f user	Force change at next login
logins -p / logins -x	Find accounts without passwords, show details

compliance: Assess and Report

```
root@sol1:~# pkg install security/compliance
root@sol1:~# compliance list -p
Benchmarks:  pci-dss  solaris
Profiles for solaris:  Baseline  Recommended
root@sol1:~# compliance assess -b solaris -p Recommended -a recommended-nov
root@sol1:~# compliance report -a recommended-nov -f html -o /var/tmp/report.html
root@sol1:~# compliance report -a recommended-nov -s fail | head
root@sol1:~# compliance tailor -t mysite            # create a tailored profile
root@sol1:~# svccfg -s compliance-assess:default setprop ... # schedule assessments
```

Security Extensions and Verified Boot

```
root@sol1:~# sxadm status
EXTENSION  STATUS                    CONFIGURATION
aslr       enabled (tagged-files)    default (tagged-files)
nxstack    enabled (all)             default (all)
nxheap     enabled (tagged-files)    default (tagged-files)
root@sol1:~# sxadm enable -c model=all aslr      # stronger: all processes
# Verified boot: kernel modules checked against Oracle signatures
root@sol1:~# svccfg -s boot-config listprop config/verified_boot   # policy
# SPARC: set policy in ILOM / OBP; x86: UEFI Secure Boot
root@sol1:~# elfsign verify -e /usr/kernel/drv/amd64/vboxdrv
```

Auditing and File Integrity (bart)

```
root@sol1:~# auditconfig -getflags
root@sol1:~# auditconfig -setflags lo,ex,ua,as   # logins, exec, user/admin
root@sol1:~# audit -s ; auditconfig -getcond
root@sol1:~# auditreduce -c lo -a 20261120 | praudit -l | tail -3
# bart: baseline of system files, then compare later
root@sol1:~# bart create -R /etc > /var/tmp/etc.bart.0
root@sol1:~# vim /etc/motd
root@sol1:~# bart create -R /etc > /var/tmp/etc.bart.1
root@sol1:~# bart compare /var/tmp/etc.bart.0 /var/tmp/etc.bart.1
/motd:
  size  control:43  test:61
```

Summary and Homework

- useradd -m: each home is a ZFS dataset (quotas, snapshots)
- RBAC: authorizations + privileges → rights profiles → roles
- usermod -P / -A / -R; pfexec, pfbash, profiles, roles
- Password policy: /etc/default/passwd, policy.conf
- compliance assess / report; sxadm; verified boot
- Auditing with auditconfig/praudit; bart create / compare
- Homework: give ali 'Service Management', run a Recommended compliance report

Thank You! 🙏

Free videos & PDFs: www.MyWebUniversity.com

Slides for this lesson: MyWebUniversity.com/presentations

YouTube: @MyWebUniversity · @MyWebUniversity-Dari

Wahidullah Lutfy — Founder and Director of IT of MyWebUniversity, and CS teacher

Book: The Direct Path to Linux Ubuntu (Amazon · Barnes & Noble)

Learn it, then pass it on.