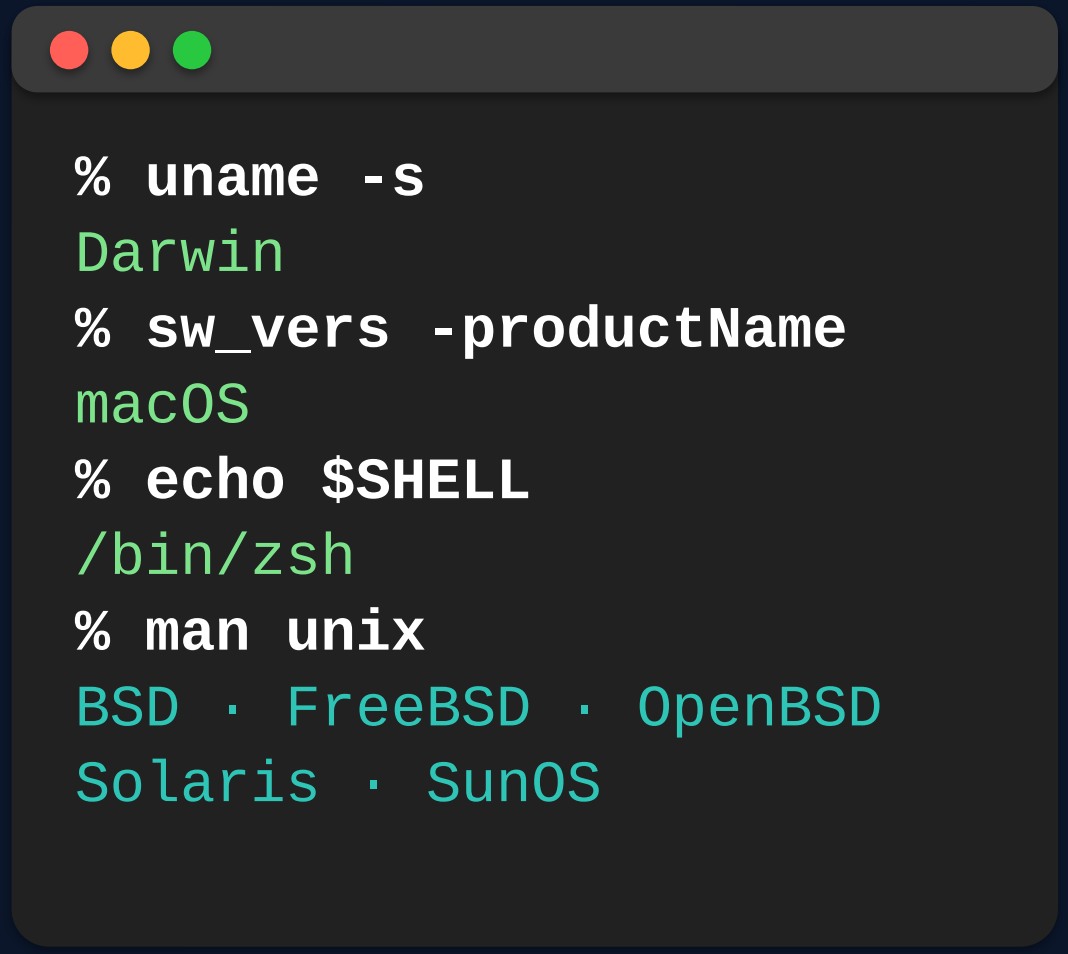


LESSON 8 OF 12

macOS UNIX

Darwin & BSD

Account Management: Users, Groups, sudo & Directory Services

Full Course · macOS 27 Golden Gate

What You Will Learn in Lesson 8

- Account types: administrator, standard, sharing only, guest, root
- Users & Groups in System Settings
- Directory Services: where macOS really keeps accounts
- dscl, sysadminctl and dseditgroup from Terminal
- sudo, /etc/sudoers.d and Touch ID for sudo
- Secure Tokens, volume owners and FileVault
- Accounts on FreeBSD, OpenBSD and Solaris

macOS Account Types

Type	Can do	Use it for
Administrator	Install software, change settings, use sudo	You — but not for daily browsing on shared Macs
Standard	Use apps, change own settings	Daily work, students, family
Sharing Only	Connect to shared files; no login at the Mac	File server access
Guest	Temporary login; files erased at logout	Visitors (off by default)
root	Everything; disabled by default	Use sudo instead

Users & Groups in System Settings

- System Settings → Users & Groups → Add User (admin password required)
- Choose Standard or Administrator; set name, account name, password
- Click ⓘ on a user: change type, reset password, Advanced Options
- Advanced Options: UID, group, account name, login shell, home folder
- Add Group: create groups and tick their members
- Login options: automatic login off, Guest User off

Directory Services: Where Accounts Live

```
% id
uid=501(wahid) gid=20(staff) groups=20(staff),80(admin),12(everyone),...

% dscl . -list /Users UniqueID | awk '$2 >= 500'   # real people
wahid      501
% dscl . -list /Users | head -3                    # system accounts start with _
_amavisd  _analyticsd  _appleevents
% dscl . -read /Users/wahid NFSHomeDirectory UserShell RealName

% sudo ls /var/db/dslocal/nodes/Default/users | head   # one .plist per user
```

/etc/passwd exists but macOS does not use it for normal logins.

Create, Change and Delete Users: sysadminctl

```
% sudo sysadminctl -addUser student1 -fullName "Student One" -password -
   (type the new password when asked)
% sudo sysadminctl -addUser labadmin -fullName "Lab Admin" -password - -admin

% sudo sysadminctl -resetPasswordFor student1 -newPassword -
% sudo dscl . -create /Users/student1 UserShell /bin/bash   # change shell
% sysadminctl -secureTokenStatus student1

% sudo sysadminctl -deleteUser student1 -keepHome     # keep files
% sudo sysadminctl -deleteUser student1 -secure       # erase home
```

Groups: dseditgroup

```
% dscl . -list /Groups | grep -v '^_' | head
admin  everyone  staff  wheel ...

% sudo dseditgroup -o create -r "Lab Students" labstudents
% sudo dseditgroup -o edit -a student1 -t user labstudents
% dseditgroup -o checkmember -m student1 labstudents
yes student1 is a member of labstudents

% sudo dseditgroup -o edit -a student1 -t user admin    # make admin
% sudo dseditgroup -o edit -d student1 -t user admin    # remove admin
% groups student1;  id student1
```

sudo: Borrowing Root's Power Safely

```
% sudo -l                              # what may I run?
% sudo -k                              # forget my cached password now
% sudo cat /etc/sudoers | grep -v '^#' | grep -v '^$'
root    ALL = (ALL) ALL
%admin  ALL = (ALL) ALL
#includedir /private/etc/sudoers.d

# Let labstudents restart Apache only — always edit with visudo:
% sudo visudo -f /etc/sudoers.d/labstudents
%labstudents ALL = (root) /usr/sbin/apachectl restart
```

Touch ID for sudo and Account Auditing

```
# Touch ID for sudo (survives macOS updates):
% sudo cp /etc/pam.d/sudo_local.template /etc/pam.d/sudo_local
% sudo vim /etc/pam.d/sudo_local      # remove the # before:
auth       sufficient     pam_tid.so

# Who is here, and who was here?
% who;  w                             # logged-in users
% last | head                         # recent logins and reboots
% dscl . -read /Groups/admin GroupMembership   # who is an admin?
```

Secure Tokens, Volume Owners and FileVault

- Secure Token: lets an account unlock FileVault and create other token users
- The first admin created in Setup Assistant gets a Secure Token
- Apple silicon: Volume Owners may change startup security and install updates
- Check: sysadminctl -secureTokenStatus <user>
- Check: diskutil apfs listUsers /
- Create users from a token-holding admin, or they may not unlock the disk

Home Folders and Account Hygiene

- Home folder: /Users/<shortname> with Desktop, Documents, Library …
- Default permissions keep other users out (drwxr-x---+)
- /Users/Shared: a folder every user can use
- Disable, don't delete, while you investigate: sudo pwpolicy -u <user> -disableuser
- Remove admin rights you no longer need
- Enterprise Macs: accounts and password rules come from MDM

Accounts on Other UNIX Systems

Task	FreeBSD	OpenBSD	Solaris 11.4
Add user	adduser or pw useradd -n bob -m	adduser or useradd -m bob	useradd -m bob
Set password	passwd bob	passwd bob	passwd bob
Admin group	pw groupmod wheel -m bob	usermod -G wheel bob	RBAC profiles / roles
Root tool	sudo (pkg) or su	doas (/etc/doas.conf)	su - (root is a role), pfexec, sudo
Account files	/etc/master.passwd (vipw)	/etc/master.passwd (vipw)	/etc/passwd, /etc/shadow

Lab: A Classroom of Users

```
% sudo dseditgroup -o create -r "Lab Students" labstudents
% for n in 1 2 3; do
>   sudo sysadminctl -addUser student$n -fullName "Student $n" -password "Temp#Pass$n"
>   sudo dseditgroup -o edit -a student$n -t user labstudents
> done
% dscl . -read /Groups/labstudents GroupMembership
% dscl . -list /Users UniqueID | awk '$2 >= 500'
% sysadminctl -secureTokenStatus student1
% sudo sysadminctl -deleteUser student3 -secure
```

Lab only: never put real passwords in a script.

Summary & Homework

- Admin, Standard, Sharing Only, Guest; root is disabled — use sudo
- Accounts live in Directory Services: dscl . -list / -read
- sysadminctl creates, resets, deletes; dseditgroup manages groups
- visudo + /etc/sudoers.d for least-privilege rules; Touch ID via sudo_local
- Homework: do the lab; give labstudents one safe sudo command
- Next: Lesson 9 — Processes, Services & launchd

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.