SOLARIS OS Kullanıcı YÖNETİMİ

Hazırlayan: Asiye Yigit

Agustos 2011

Kullanıcı Yönetimi – Kullanıcı Hesapları

- “user name”
- “password”
- “user’s home directory”
- “user’s login shell”
- “user’s initialization files”

Kullanıcı Yönetimi – Kullanıcı Hesapları

- “login name”
- “user identification number”
- “group identification number”
- “comment”
- “home directory”
- “user’s login shell”
- “password aging”

Kullanıcı Yönetimi – Şifre Yaşlandırma

- Min change
- Max change
- Max inactive
- Expiration date
- warning

Kullanıcı Yönetimi – Kullanıcı ve Grup Bilgilerinin Depolanması

- /etc/passwd
- /etc/shadow
- /etc/group

Kullanıcı Yönetimi – Komut Satırından Kullanıcı Yönetimi

- “useradd”
- “usermod”
- “userdel”
- “groupadd”
- Groupmod”
- “groupdel”

Kullanıcı Yönetimi – Komut Satırından Kullanıcı Yönetimi

- “useradd [-u uid] [-g gid] [-G gid [,gid,...]] [-d dir] [-m] [-s shell] [-c comment] loginname”

“useradd –u 100 –g other –d /export/home/newuser1 –m –s /bin/ksh –c “Regular User Account” newuser1”

  - “-u uid”
  - “-g group”
  - “-G group”
  - “-d dir”
  - “-m”
  - “-s shell”
  - “-c comment”
  - “-o”
  - “-e expire”

Kullanıcı Yönetimi – Komut Satırından Kullanıcı Yönetimi

- “usermod [-u uid [-o]] [-g group] [-G group [, group ...]] [–d dir] [-m] [-s shell] [-c comment] [-l newlogname] [-f inactive] [-e expire] login”

“usermod –d /export/home/guest1 –m –l guest1 newuser1”

- “-l newlogname”
- “-m”

Kullanıcı Yönetimi – Komut Satırından Kullanıcı Yönetimi

- “userdel [-r] login”

“userdel guest1”

  - “-r”

Kullanıcı Yönetimi – Komut Satırından Group Yönetimi

- “groupadd [-g gid [-o]]”

“groupadd –g 301 class1”

  - “-g gid”
  - “-o”

Kullanıcı Yönetimi – Komut Satırından Group Yönetimi

- “groupmod [-g gid [-o]] [-n name] groupname”

“groupmod –g 400 class”

  - “-g gid”
  - “-o”
  - “-n name”

Kullanıcı Yönetimi – Komut Satırından Group Yönetimi

- “groupdel groupname”

“groupdel class1”

  - “-g gid”
  - “-o”
  - “-n name”

Kullanıcı Yönetimi – Task

- Sistem üzerinde kendi kullanıcınızı oluşturunuz
- /etc/passwd, /etc/shadow, /etc/group dosyalarının inceleyiniz, her bir girişi yorumlayınız.
- Kendi kullanıcınız için şifre yaşlandırmasını konfigüre ediniz ve çalıştığını gözlemleyiniz.

Kullanıcı Yönetimi – Başlangıç Dosyaları

- “system-wide initialization files”
  - /etc/profile
  - /etc/.login
- “user’s environment”
  - $HOME/.profile
  - $HOME/.kshrc
  - $HOME/.cshrc
- Shell Pathname
  - /bin/sh
  - /bin/ksh
  - /bin/csh

Kullanıcı Yönetimi – Başlangıç Dosyaları

- “SHELL Variables”
  - “Environment Variables”
  - “Local Variables”
- “SHELL Variables”
  - LOGNAME
  - HOME
  - SHELL
  - PATH
  - MAIL
  - TERM
  - LPDEST
  - PWD
  - PS1
  - prompt

Kullanıcı Yönetimi – Başlangıç Dosyaları

- VARIABLE=value;export VARIABLE
- setenv variable value

Kullanıcı Yönetimi – Task

- “ksh” kullanacak şekilde kullanıcınızı oluşturunuz.
- Başlangıç dosyanızda EDITOR, PATH, ENV değişkenlerinizi set ediniz.
- Login sonrası tanımladığınız değişken içeriklerini görüntüleyiniz

Kullanıcı Yönetimi – Task

- Edit /etc/skel/local.profile so that it sets the PATH variable to the same paths as used by the root user. Set the EDITOR, LPDEST, EXINIT, and ENV variables to appropriate values.
- Use admintool to create a new user called user9 who uses the Korn shell. Log in as the new user and verify all the variables you set in local.profile are set correctly in the user's environment.
- Create a .kshrc file for the new user that includes two aliases and sets the primary prompt to echo the current working directory. Log out and log in again as the same user to verify .kshrc works. Log out and log in again as root.
- Use useradd to create a new user called user10 that uses the Korn shell. Log in as this user and record the list of initialization files in your home directory. Copy the appropriate file to .profile. Test the login to verify the same list of variables is set as with the first user you created. Log out and log in as root when finished.

Kullanıcı Yönetimi – Sorular

- Yeni konuya geçmeden önce aşağıda olan soruları cevaplayabildiğinizden emin olun:
  - Describe the format of the files /etc/passwd and /etc/shadow for securing login access
  - Describe the format of the /etc/group file for maintaining shared and restricted access to files and directories
  - Add, modify, and delete user accounts on the local system with the commands useradd, usermod, and userdel
  - Add, modify, and delete group accounts for the local system with the commands groupadd, groupmod, and groupdel
  - Define the two different types of shell initialization files
  - Describe the shell startup activities during login for the three main Solaris Operating Environment shells
  - List the shell initialization files used to set up a user's work environment at login
  - Describe the purpose of the /etc/skel directory
  - Modify initialization files to customize a user's work environment

Sistem Güvenliği

- “pwconv”
- “/var/adm/loginlog”
- “/var/adm/utmpx”
- “who”
- “finger –m username”
- “last”
- “last user9”
- “last reboot”
- “rusers –l”
- “su [-] [username]”
- “whoami”

Sistem Güvenliği

- “Effective User ID” ve “Effective Group ID”
- “sysadmin group”
- “/etc/deafult/su”
  - CONSOLE
  - SULOG
- “/etc/default/login”
  - CONSOLE
  - UMASK
- “/etc/default/passwd”
  - MAXWEEKS
  - MINWEEKS
  - PASSLENGTH
- “CONSOLE variable”
- “SULOG variable”
- “/var/adm/sulog”

Sistem Güvenliği - Task

- Create the file /var/adm/loginlog. Use the command line login to make five failed login attempts. List the contents of /var/adm/loginlog. Use finger to display information for user9 on your system and your partner's system.
- Use last to identify when the first root login session on your system occurred and how long the session lasted. Use last to learn when your system last booted. Use rusers to list users logged in on all systems on your network, and just on your partner's system.
- Use su to change your user identity from root to user9, both with and without the dash (-) option. Record differences. Use whoami and who am i to list effective and real user identity during your su sessions. Locate the su log declared in /etc/default/su and identify which user initiated your su attempts.
- As root, attempt a telnet session to your partner's system.Record error messages. Change the CONSOLE variable on your partner's system to allow root logins from any terminal. Attempt the telnet session again.