Administration Tasks

ADMINUX®

Security Administration

- Scan for "Trojan Horse" violations
- Scan for "Backdoor" violations
- Intrusion Detection - Run checksums on all system directories to determine if any changes have been made
- Scan for unsecured directories and files
- Scan for user accounts with no password
- Look for any new Operating System errors that may have been logged
- Monitor for suspicious failed "login" attempts
- Monitor for suspicious failed "su" attempts
- Log all ".rhosts" files
- Scan root's PATH variable for security problems
- Monitor system owned world writeable files
- Monitor user owned writeable files
- Identify rogue (misplaced) devices
- Log deletion of system owned files
- Log deletion of user owned files
- Monitor changes to access (owner, group or permissions) on secured files
- Scan for potential problems in /etc/passwd file, such as:
  - no matching entry in NIS
  - group ID not in /etc/group
  - invalid home directory
  - duplicate logins
  - duplicate UIDs
  - root entry missing
  - root entry is not the first entry
  - unexpected value for shell
  - shell is Set UID
  - shell is Set GID
- Kill idle users
- Any new orphan files?
- Monitor for the removal of the sticky bit on directories
- Audit security and suggest improvement changes
- Transfer all data between AdminUXs as encrypted and certified
- Monitor TCP/IP ports for change in status
- Can root log in on non-console devices?
- Does PAM have any breathtaking configurations?
- Create a daily security diary

Network Administration

- Poll devices on network and determine if any network hosts are down
- Poll the network to determine if any network interfaces are down
- Determine if collision rates are abnormal on all network interfaces
- Determine if packet error rates are abnormal on all network interfaces
- Poll URL to determine if the web page exists
- Poll URL to determine if the web page has changed
- Alert if an inactive TCP/IP port becomes active
- Alert if an active TCP/IP port becomes inactive
- Audit for ports that should not be active
- Distribute matrix changes to a workgroup of AdminUXs

Performance Administration

- Log benchmarks
- Run sar reports for yesterday's data
- Analyze buffer performance
- Analyze cpu performance
- Analyze disk performance
- Analyze memory performance
- Look for any new Operating System errors that may have been logged
- Was there an unauthorized date/time change?
- Was the last boot expected?
- Determine if the system needs to be shutdown.
- Determine if collision rates are abnormal on all network interfaces.
- Determine if packet error rates are abnormal on all network interfaces

Administration Tasks ADMINUX®

Process Administration

- Monitor for failed daemons
- Restart any stopped daemon, if permitted
- Monitor for orphan processes
- Kill orphan processes, if permitted
- Monitor for runaway processes

Filesystem Administration

- Monitor if all filesystems are mounted
- Monitor if there is adequate filesystems space
- Monitor if there is adequate swap space
- Model free blocks and forecast if the resource will be exhausted in 90/60/30 days

File Administration

- Restore any missing critical file, device or symbolic link
- Archive/trim defined system logs
- Remove defined garbage files
- Does /dev use more space than expected?
- Any new large mailboxes?
- Any new orphan files?
- Reassign orphan files' ownership to a valid user
- Error check /etc/gettydefs
- Error check /etc/inittab
- Error check /etc/passwd
- Locate and log large files
- Monitor the growth of large files
- Locate and log huge directories

Backup Administration

- Did the Autobackup Administrator complete?
- Has the Autobackup Status been checked recently?
- Is tonight's tape(s) inserted?
- Did the Autobackup run the normal length of time?
- Is the Autobackup Administrator enabled?
- If applicable, create the volume group configuration backup files
- Synchronize AdminUX's logs onto other hosts (Logs are available if this machine goes down)
- Synchronize application logs/files onto other hosts for backup

User Administration

- Enable/Disable a login
- Kill idle users
- Monitor user application logs for a defined event
- Look for user posted events to alarm
- Randomly select a new message-of-the-day
- Change file names in users' home directories if file name contains meta characters
- Enforce certain time of day login rule
- Assign a menu command to the login
- Assign a time zone to the login if needed
- If applicable, display a login greeting
- If applicable, display any birthdays for today
- If applicable, celebrate the login's birthday
- Prevent a user from logging in from more than one device
- Allow a user to run a super user command

Printer Administration

- Monitor if the print scheduler is running
- Monitor if all printers are enabled
- Monitor if all print destinations are accepting requests
- Monitor if there is a default print destination
- Restart lp spooling system's sequence number each year

Administration Tasks

ADMINUX®

Keep A Record

- Create a daily security diary
- If applicable, create the volume group configuration backup files
- Create a table of all files on the local filesystems (FILES.tab)
- Create a table of everything known about the print spooling system (LPPERMS.tab)
- Maintain 24 hour status logs to diagnose system problems (STATUS00.log - STATUS23.log)
- Log kernel system log errors (ERRPT.log)
- Log deleted system owned files (MISSING.log)
- Log response time benchmark (RESPONSE.log)
- Log active users (USERS.log) and terminals (TERMS.log)
- Log removed garbage files (CLEANUP.log).
- Log current disk space (DISK.log).
- Log current directory space (DU.log).
- Log current space for users' home directory (DUUSR.log).
- Log orphan files (FORPHANS.log)
- Log large files (LRGFILES.log)
- Log huge directories (HUGEDIR.log)
- Log security concerns (SECURITY.log)
- Log failed login attempts (FAILEDLGIN.log)
- Log failed "su" attempts (FAILEDSU.log)
- Log all "su" attempts (SU.log)
- Log all system boots and shutdowns (BOOT.log,SHUTDOWN.log)
- Log a history of all repairs made by AdminUX (REPAIRS.log)
- Log all ".rhosts" files (RHOSTS.log)
- Log all SGID files (SGID.log)
- Log all sticky bit files (STICKYBIT.log)
- Log all SUID files (SUID.log)
- Log system uptime (UPTIME.log)
- Log all files that are writeable by users (USERSWRITE.log)
- Log all world writeable files (WORLDWRITE.log)
- Log system configuration settings (SYSTEM.log)
- Log resource data (DB.log)

Alarm Administration

- Send notifications if an alarm is set
- Send alarm to Tivoli
- Send alarm to OpenView
- Send alarms to other machines

Boot Administration

- Make certain that the console is linked correctly
- If applicable, do an fsck on all filesystems
- Re-create /tmp and /usr/tmp if missing
- Remove lock and obsolete control files
- Ask for a new date/time if unreasonable
- Restore any missing files, devices and symbolic links
- Re-create any missing lost+found directories
- Re-create utmp file if missing