# Administración de Sistemas

## Las funciones y la responsabilidad de un administrador

Alberto Hernández Gallardo

Universidad Europea

# Índice

- Funciones del administrador
- Definición del entorno
- Procesos periódicos
- Ficheros de logs
- Usuarios

## Funciones del administrador. Aprovisionamiento de cuentas

- El proceso de agregar y eliminar usuarios puede automatizarse, pero ciertas decisiones administrativas (dónde ubicar el directorio de inicio de un usuario, tipo de directorio, en qué máquinas crear la cuenta, etc.) deben realizarse antes de que se pueda agregar un nuevo usuario.
- Definición de roles y grupos de permisos
- Políticas de contraseñas
- Cuando un usuario ya no debe tener acceso al sistema, la cuenta del usuario debe estar deshabilitada. Todos los archivos propiedad de la cuenta se deben respaldar.

## Funciones del administrador.
## Configuración de hardware

- Las tareas de soporte de hardware pueden abarcar desde la simple tarea de agregar una impresora a la tarea más compleja de agregar una matriz de discos.
- Con la virtualización, la configuración del hardware puede ser más compleja. Los dispositivos pueden necesitar instalación en varias capas de la pila de virtualización.
- Gestión y definición de ventanas de actuación

# Funciones del administrador.
# Gestión de Backups

- La realización de copias de seguridad es quizás el trabajo más importante del administrador del sistema y son absolutamente necesarias.
- Las copias de seguridad se pueden automatizar, pero sigue siendo tarea del administrador del sistema asegurarse de que las copias de seguridad se ejecuten correctamente y de acuerdo con el cronograma.
- Definición de políticas de Backup
  - Frecuencia
  - Tipo
  - Contenido
  - Políticas de restauración

## Funciones del administrador.
## Instalación y actualización de software

- Definición de niveles de entornos (test, preproducción, producción)
- Una vez que el software está funcionando correctamente, los usuarios deben ser informados de su disponibilidad y ubicación.
- A medida que se lanzan parches y actualizaciones de seguridad, deben incorporarse sin problemas en los entornos.
- El software local y las secuencias de comandos administrativas se deben empaquetar y gestionar de forma adecuada y compatibles con los procedimientos nativos de actualización utilizados.
- A medida que este software evoluciona, las nuevas versiones se deben organizar en un repositorio de versiones.

## Funciones del administrador.
## Monitorización del sistema

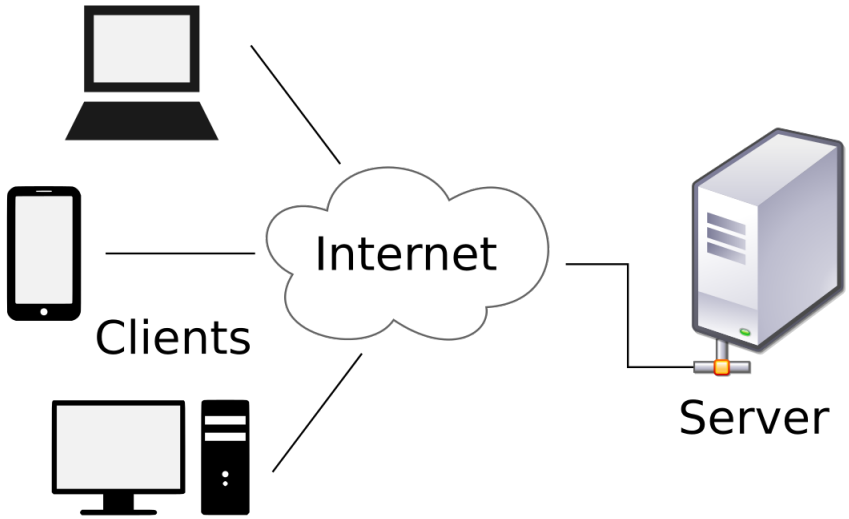
- Todos los sistemas requieren de una monitorización proactiva.
- Aspectos destacados en la monitorización:
  - Utilización de recursos (CPU, disco, red)
  - Fallos hardware
- La automatización de la monitorización pueden ayudar a los administradores de sistemas con esta tarea.
- Definición de los protocolos en caso de fallo o saturación.

## Funciones del administrador. Procedimientos y documentación

- El administrador del sistema debe implementar una política de seguridad y verificar periódicamente para asegurarse de que no se ha violado la seguridad del sistema.
- En los sistemas de baja seguridad, esta tarea puede incluir solo algunas comprobaciones básicas para el acceso no autorizado.
- En un sistema de alta seguridad, puede incluir una elaborada red de comprobaciones y programas de auditoría.
- Todos los procedimientos deben estar documentados, así como debe existir documentación técnica de toda la infraestructura.

# Definición del entorno

- Arquitectura física vs cloud computing
- Gestión de la virtualización
- Conectividad entre la arquitectura
- Conectividad con el usuario



# Definición del entorno.
# Alta disponibilidad

- Asegurar grado absoluto de continuidad
  - Acceso al sistema
  - Actualizaciones
  - Operaciones pesadas
- Downtime es usado para definir cuándo el sistema no está disponible
- Principales puntos críticos
  - Energía
  - Red
  - Procesamiento
  - Almacenamiento

# Definición del entorno.
# Alta disponibilidad

- Sistemas rebundantes
  - Son aquellos en los que se repiten datos o hardware de carácter crítico que se quiere asegurar ante los posibles fallos que puedan surgir por su uso continuado.
  - Solución a los problemas de protección y confiabilidad.
  - Este tipo de sistemas se encarga de realizar el mismo proceso en más de una estación, ya que si por algún motivo alguna dejara de funcionar o colapsara, inmediatamente otro tendría que ocupar su lugar y realizar las tareas del anterior.
  - Han sido usadas por la industria militar y aerospacial por muchos años para alcanzar una alta confiabilidad.

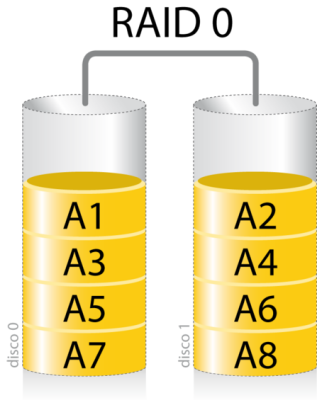
# Definición del entorno.
# Alta disponibilidad

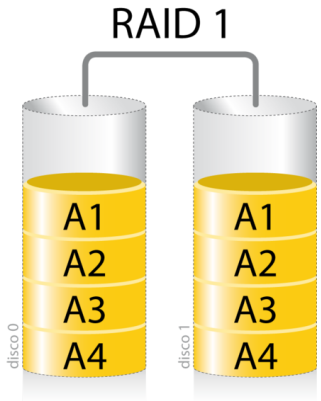
- RAID
  - Redundant Array of Independent Disks.
  - Sistema de almacenamiento que usa múltiples discos duros o SSD entre los que se distribuyen o replican los datos.
  - Dependiendo de su configuración (nivel) los beneficios de un RAID respecto a un único disco son uno o varios de los siguientes:
    - mayor integridad
    - mayor tolerancia a fallos
    - mayor rendimiento
    - mayor capacidad.
  - En sus implementaciones originales, su ventaja clave era la habilidad de combinar varios dispositivos de bajo coste y tecnología más antigua en un conjunto que ofrecía mayor capacidad, fiabilidad, velocidad o una combinación de éstas.

# Definición del entorno.
# Alta disponibilidad

- RAID
  - **RAID 0:** La información se divide entre todos los discos del sistema, es decir, no hay redundancia y por tanto no hay recuperación de datos. Se trata de un sistema con tiempos de acceso muy rápidos.

  - **RAID 1** o MDA (Mirrored Disk Array): Los discos de asocian por parejas y en cada uno de ellas se almacenará la misma información. Se trata de un disco primario, donde se leen y escriben los datos y un disco espejo que será una copia del disco primario.



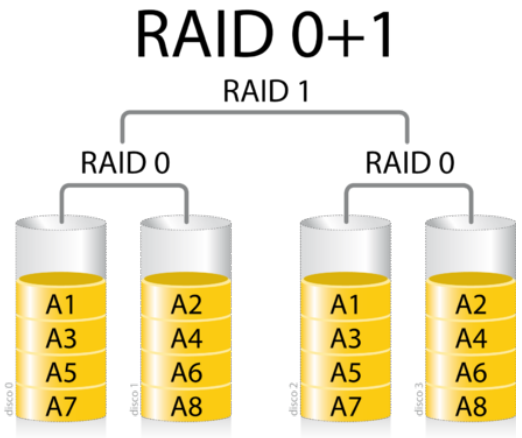



# Definición del entorno.
# Alta disponibilidad

- RAID
  - **RAID 3**: "striping con paridad dedicada", utiliza un disco de protección de información separado para almacenar información de control codificada. Esta información de control codificada o paridad proviene de los datos almacenados en los discos y permite la reconstrucción de la información en caso de falla. Se requieren mínimo tres discos y se utiliza la capacidad de un disco para la información de control.
  - **RAID 5**: Sistema de discos independientes con integración de códigos de error mediante paridad, en donde los datos y la paridad se guardan en los mismos discos, haciendo que se consiga aumentar la velocidad. Hay que tener en cuenta que la paridad nunca se guarda en los discos que contienen los datos que han generado dicha paridad. Este sistema requiere al menos tres discos duros.

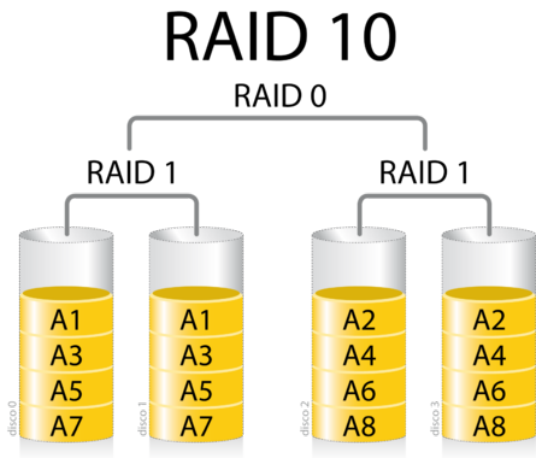
# Definición del entorno.
# Alta disponibilidad

- RAID
  - **RAID 0+1**: Primero se crean dos conjuntos RAID 0 (dividiendo los datos en discos) y luego, sobre los anteriores, se crea un conjunto RAID 1 (realizando un espejo de los anteriores). La ventaja de un RAID 0+1 es que cuando un disco duro falla, los datos perdidos pueden ser copiados del otro conjunto de nivel 0 para reconstruir el conjunto global



# Definición del entorno.
# Alta disponibilidad

- RAID
  - **RAID 1+0**: Primero se crean dos conjuntos RAID 1 y luego, sobre los anteriores, se crea un conjunto RAID 0. En cada división RAID 1+0, pueden fallar todos los discos salvo uno sin que se pierdan datos



# Definición del entorno.
# Alta disponibilidad

- Clústers
  - **Nodos**: Cada uno de los servidores que conforman la red.
  - **Sistema operativo**: Este debe de tener un entorno multiusuario, cuanto más fácil sea el manejo del sistema menores problemas tendremos. Comúnmente Solingest instala sus cluster con sistemas Microsoft Cluster Services (MSCS), pero es totalmente factible la instalación de un Cluster con un sistema Linux o Unix como podrían ser Rocks (Linux) o Solaris (Unix).
  - **Conexiones de Red**: Las conexiones utilizadas en este tipo de sistema pueden ser muy variadas, se pueden utilizar desde simples conexiones Ethernet con placas de red comunes o sistemas de alta velocidad como Fast Ethernet, Gigabit Ethernet, Myrinet, Infiniband, SCI, etc.

# Definición del entorno.
# Alta disponibilidad

- Clústers
  - **Middleware**: El middleware es el software que actúa entre el sistema operativo y las aplicaciones y que brinda al usuario la experiencia de estar utilizando una única super máquina. Este software provee una única interfaz de acceso al sistema, denominada SSI (Single System Image). Optimiza el sistema y provee herramientas de mantenimiento para procesos pesados como podrían ser migraciones, balanceo de carga, tolerancia de fallos, etc.

# Definición del entorno.
# Alta disponibilidad

- Clústers: Carácterísticas
  - Un clúster consta de dos o más nodos
  - Los nodos están conectados entre sí por un canal de comunicación funcional
  - Los clústers necesitan software especializado
    - Software a nivel de aplicación
    - Software a nivel de sistema
  - Todos los elementos del clúster trabajan para cumplir una funcionalidad conjunta

# Definición del entorno.
# Alta disponibilidad

- Clústers: Carácterísticas
  - Los clúster poseen una forma de acoplamiento
    - Fuerte: software cuyos elementos se interrelacionan mucho unos con otros, y hacen las funcionalidades del clúster de manera cooperativa.
    - Medio: software que no necesita un conocimiento tan exhaustivo de todos los recursos de otros nodos, pero que sigue usando el software de otros nodos para aplicaciones de muy bajo nivel.
    - Débil: los programas se dividen en diversos nodos y por tanto se necesitan pero que no están a un nivel tan bajo.
  - Mejora la disponibilidad
  - Mejora el rendimiento.

# Definición del entorno.
# Alta disponibilidad

- SAN, NAS  y FiberChannel
  - **SAN**: red concebida para conectar servidores, matrices (arrays) de discos y librerías de soporte. Una red SAN se distingue de otros modos de almacenamiento en red por el modo de acceso a bajo nivel. El tipo de tráfico en una SAN es muy similar al de los discos duros como ATA,SATA y SCSI. La mayoría de las SAN actuales usan el protocolo SCSI para acceder a los datos de la SAN, aunque no usen interfaces físicas SCSI.
  - **NAS**: Tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento de un servidor con ordenadores personales o servidores clientes a través de una red (normalmente TCP/IP), haciendo uso de un Sistema Operativo optimizado para dar acceso con los protocolos CIFS, NFS, FTP o TFTP.

# Definición del entorno.
# Alta disponibilidad

- SAN, NAS  y FiberChannel
  - **FiberChannel**: Tecnología de red Gigabit utilizada principalmente para redes de almacenamiento SAN y para la conexión de Cabinas de Discos DAS, capaz de funcionar sobre cables de fibra óptica y sobre cables de cobre, aunque en la práctica suele ser cableado de fibra óptica (multimodo o monomodo). Fiber Channel Protocol (FCP) es un protocolo de transporte para la transmisión de comandos SCSI sobre redes Fiber Channel

# Definición del entorno.
# Alta disponibilidad

- Balanceadores de carga
  - Dispositivo hardware o software que se pone al frente de un conjunto de servidores que atienden una aplicación y, tal como su nombre lo indica, asigna o balancea las solicitudes que llegan de los clientes a los servidores usando algún algoritmo.
    - Round-Robin: las peticiones son distribuidas entre los servidores de forma cíclica, independientemente de la carga del servidor
    - Weighted Round-Robin: Las peticiones se entregan dependiendo del peso que se le de a cada servidor.
    - LeastConnection: Cada petición es atendida por el servidor con menos conexiones activas en ese momento.
    - Weighted LeastConnection: Las peticiones se entregan dependiendo del peso y el número de conexiones que se tengan
    - IP-hash: Todas las peticiones de un usuario son atendidas por el mismo servidor.

# Definición del entorno.
# Alta disponibilidad

- Balanceadores de carga
  - **Primera generación**: Detectar el rendimiento del servidor vía "passive polling", lo que significa que el balanceador de carga mide el tiempo de respuesta de los servidores.
  - **Segunda generación**: El balanceador de carga continuamente realiza peticiones de datos de cada servidor en la granja de servidores para monitorizar sus condiciones y direccionar las peticiones de los clientes hacia el servidor que se encuentre más disponible y en mejor estado para responder a dichas peticiones. Los parámetros solicitados, dependen del producto utilizado. Normalmente se emplea la utilización de la CPU del servidor, el uso de memoria y el número de conexiones abiertas.

# Procesos periódicos

- Cron es el demonio del sistema con el que se programan acciones en base al tiempo. Las realiza cada hora, día, semana, mes y con cierto intervalo de días, desde segundo plano, siempre y cuando el sistema se encuentre en modo multiusuario.
- Cron lee el archivo de configuración llamado crontab que contiene la lista de comandos y tiempos en los que debe ser invocado.
- Los comandos son ejecutados por la shell.
- Existe un crontab por cada usuario.
- Los archivos cron.deny y cron.allow permiten definir qué usuarios tienen acceso para administrar archivos crontab

# Procesos periódicos

- El formato de crontab sigue la siguiente estructura:

```
*  *  *  *  * comando o programa a ejecutar
|  |  |  |  |
|  |  |  |  |----- día de la semana (0 - 6) (0-> Domingo)
|  |  |  |-------- Mes (1 - 12)
|  |  |----------- Día del mes (1 - 31)
|  |-------------- Hora (0 - 23)
|----------------- Minuto (0 - 59)
```

  - * -> Cualquier valor
  - Número entero -> Sólo para ese valor
  - Números separados por guiones -> Todo el rango
  - Números separados por guiones seguidos de barra ->Todo el rango con un salto específico
  - Números separados por comas ->Sólo esos valores

# Procesos periódicos

- Formato del comando:
  - $ crontab filename

  Remplaza el existente archivo crontab con un archivo definido por el usuario
  - $ crontab –e

  Editar el archivo crontab del usuario, cada linea nueva sera una nueva tarea de crontab
  - $ crontab -l

  Lista todas las tareas de crontab del usuario
  - $ crontab -r

  Borra el crontab perteneciente a usuario

  Siempre se puede añadir la opción –u para manejar el crontab de otro usuario

# Procesos periódicos

- Programar una sola ejecución:
  - Comando at
  - Parámetros:

    - HH[:]MM[am|pm] [Mes día]
    - Se puede añadir a la fecha/hora un número (seguido de minutes, hours, days, weeks)
    - También se pueden añadir valores relativos como now, midnight, today o tomorrow.

    - $ comando | at now + 3 minutes
    - $ at 12am tomorrow < script.sh

## Procesos periódicos

- Programar una sola ejecución:
  - Los archivos at.deny y at.allow permiten definir qué usuarios tienen acceso.
  - El comando atq muestra la lista de tareas pendientes a ejecutar.
  - Elcomando atqr permite eliminar una tarea

# Ficheros de logs

- Los daemons del sistema, el kernel y diversas utilidades y servicios emiten generan logs con todos los datos que registran.
- Estos datos tienen una vida útil limitada y deben resumirse, comprimirse, archivarse y, finalmente, desecharse.
- Es posible que los datos de acceso y auditoría deban gestionarse estrechamente de acuerdo con las políticas de seguridad.
- Históricamente, UNIX ha intentado utilizar un sistema integrado conocido como **syslog** ó **rsyslog (Ubuntu)** para agrupar todo en un solo lugar.

# Ficheros de logs

- Muchas aplicaciones generan sus propios archivos independientes de logs.
- En la mayoría de los casos, un evento de registro se captura como una sola línea de texto que incluye la hora y la fecha, el tipo y la gravedad del evento, y cualquier otro detalle relevante.
- Aunque cada distribución de Linux tiene su propia manera de nombrar y dividir los archivos de registro. En su mayor parte, los paquetes de Linux envían su información de registro a los archivos en el directorio /var/log.

# Ficheros de logs

- Ficheros de configuración:
  - /etc/syslog.conf -> configuración syslog
  - /etc/rsyslog.conf -> configuración rsyslog
  - /etc/syslog.d/* -> archivos adicionales de configuración syslog
  - /etc/rsyslog.d/* -> archivos adicionales de configuración rsyslog

  - /etc/logrotate.conf -> política de rotación
  - /etc/logrotate.d/* -> archivos adicionales de políticas de rotación

  - /var/log/* -> archivos de logs

# Ficheros de logs

- Configuración
  - El archivo /etc/syslog.conf controla el comportamiento de syslogd. Es un archivo de texto con un formato simple.
  - El formato básico es
    - selector <Tab> acción

    - facility.level
    - facility1,facility2.level
    - facility1.level1;facility2.level2
    - *.level
    - *.level;badfacility.none
    - facility.!level
    - facility.=level

# Ficheros de logs

| Facility code | Keyword | Description |
|---|---|---|
| 0 | kern | kernel messages |
| 1 | user | user-level messages |
| 2 | mail | mail system |
| 3 | daemon | system daemons |
| 4 | auth | security/authorization messages |
| 5 | syslog | messages generated internally by syslogd |
| 6 | lpr | line printer subsystem |
| 7 | news | network news subsystem |
| 8 | uucp | UUCP subsystem |
| 9 | cron | clock daemon |
| 10 | authpriv | security/authorization messages |
| 11 | ftp | FTP daemon |
| 12 | ntp | NTP subsystem |
| 13 | security | log audit |
| 14 | console | log alert |
| 15 | solaris-cron | scheduling daemon |
| 16-23 | local0...local7 | locally used facilities (local0-local7) |

# Ficheros de logs

| Leve.Code | Keyword | Description |
|---|---|---|
| 0 | emerg | System is unusable. |
| 1 | alert | Action must be taken immediately |
| 2 | crit | Critical conditions |
| 3 | err | Error conditions |
| 4 | warning | Warning conditions |
| 5 | notice | Normal but significant conditions |
| 6 | info | Informational messages |
| 7 | debug | Debug-level messages |

# Ficheros de logs

| Action | Description |
|---|---|
| *filename* | Agrega el mensaje al archivo local |
| @*hostname* | Reenvía el mensaje al hotname indicado |
| @*ipaddress* | Reenvía el mensaje a la ip indicada |
| \| *fifoname* | Escribe el mensaje en la tubería fifoname |
| *user1,user2,...* | Muestra por pantalla el mensaje a los usuarios indicados si están conectados |
| * | Muestra el mensaje por pantalla a todos los usuarios conectados |

# Ficheros de logs

- Logrotate implementa una variedad de políticas de administración de registros y es estándar en todas las distribuciones de Linux
- El archivo de configuración de logrotate consiste en una serie de especificaciones para grupos de archivos de registro que se administrarán.

# Ficheros de logs

| Opción | Significado |
|---|---|
| compress | Comprime todas las versiones anteriores a la actual |
| daily, weekly, monthly | Rota los archivos de log en el plazo indicado |
| delaycompress | Comprime todas las versiones excepto la actual y la más reciente anterior |
| endscript | Marca el final del prerotate o postrotate script |
| errors emailaddr | Envía por e-mail las notificaciones de tipo error |
| missingok | No muestra ningún fallo si el archivo no existe |
| notifempty | No realiza la rotación si el archivo está vacío |
| olddir dir | Especifica el directorio para los archivos antiguos |
| postrotate | Comienza el script que se ejecutará una vez rotado |
| prerotate | Comienza el script que se ejecutará antes de la rotación |
| rotate n | Incluye n versiones de rotación |
| sharedscripts | Ejecuta el script sólo una vez para el grupo completo |
| size logsize | Rota si el archivos tiene un tamaño superior al especificado |
| copytruncate | Copia los archivos y despues trunca el original |

# Ficheros de logs

```
# Global options
errors errors@book.admin.com
rotate 5
weekly
# Logfile rotation definitions and options
/var/log/messages {
        postrotate
                /bin/kill -HUP `cat /var/run/syslogd.pid`
        endscript
}
/var/log/samba/*.log {
        notifempty
        copytruncate
        sharedscripts
        postrotate
                /bin/kill -HUP `cat /var/lock/samba/*.pid`
        endscript
}
```

# Usuarios

- El archivo /etc/passwd es una lista de todos los usuarios reconocidos por el sistema.
- Se puede ampliar o reemplazar por un servicio de directorio, por lo que la autorización recae en sistemas independientes (P. Ej. LDAP)
- El sistema consulta /etc/passwd en el momento del inicio de sesión para determinar el UID y el directorio personal de un usuario, entre otras cosas.

# Usuarios

- Cada línea en el archivo representa un usuario y contiene siete campos separados por dos puntos:
  - Nombre de inicio de sesión
  - Marcador de posición de contraseña cifrado
  - Número de UID (ID de usuario)
  - Número predeterminado de IDG (ID de grupo)
  - Información "GECOS": nombre completo, oficina, extensión, teléfono residencial
  - Directorio personal
  - Iniciar sesión shell

# Usuarios

- El archivo /etc/shadow es un archivo de contraseñas ocultas solo es legible por el superusuario y sirve para mantener las contraseñas cifradas.

- También incluye información adicional de la cuenta que no se proporcionó en el formato original /etc/passwd.

## Usuarios

- Cada línea en el archivo representa una asignación de contraseña para un usuario:
  - Nombre de inicio de sesión
  - Contraseña encriptada
  - Fecha del último cambio de contraseña
  - Número mínimo de días entre cambios de contraseña
  - Número máximo de días entre cambios de contraseña
  - Número de días de antelación para advertir a los usuarios sobre la caducidad de la contraseña
  - Días después de la caducidad de la contraseña que la cuenta está deshabilitada
  - Fecha de vencimiento de la cuenta
  - Un campo reservado que actualmente está siempre vacío

# Usuarios

- El archivo /etc/group contiene los nombres de los grupos UNIX y una lista de los miembros de cada grupo.
- Cada línea representa un grupo y contiene cuatro campos:
  - Nombre del grupo
  - Contraseña cifrada o marcador de posición
  - Número de GID
  - Lista de miembros, separados por comas (sin espacios)

# Usuarios

## /etc/passwd

```
root:x:0:0:The System,,x6096,:/:/bin/sh
jl:!:100:0:Jim Lane,ECOT8-3,,:/staff/jl:/bin/sh
dotty:x:101:20::/home/dotty:/sbin/nologin
```

## /etc/shadow

```
millert : $md5$em5J8hL$a$iQ3pXe0sakdRaRFyy7Ppj. : 14469 : 0 : 180 : 14 : : :
```

## /etc/group

```
system:!:0:root,pconsole,esaadmin
staff:!:1:ipsec,esaadmin,trent,ben,garth,evi bin:!:2:root,bin
sys:!:3:root,bin,sys
adm:!:4:bin,adm
nobody:!:4294967294:nobody,lpd
```

# Usuarios.
# Centralización de cuentas

- Los usuarios necesitan la comodidad y seguridad de un solo nombre de usuario, UID y contraseña en todos los aplicativos de la organización.
- Los administradores necesitan un sistema centralizado que permita que los cambios (como las bajas de cuentas) se propaguen instantáneamente en todas partes.
- Dicha centralización se puede lograr de varias formas, la mayoría de las cuales (incluido el sistema de Active Directory de Microsoft) involucran a LDAP (Protocolo ligero de acceso a directorios), en cierta medida.

## Usuarios.
## Centralización de cuentas: LDAP

- LDAP es un repositorio generalizado similar a una base de datos que puede almacenar datos de administración de usuarios y otros tipos de datos.
- Utiliza un modelo jerárquico de cliente/servidor que admite múltiples servidores y múltiples clientes simultáneos.
- Una de las grandes ventajas de LDAP como repositorio de todo el sitio para los datos de inicio de sesión es que puede imponer UID y GID únicos en todos los sistemas.
- También funciona bien en Windows.
- El Directorio Activo de Microsoft usa LDAP y Kerberos y puede administrar muchos tipos de datos, incluida la información del usuario.

## Usuarios.
## Centralización de cuentas: SSO

- Los sistemas de inicio de sesión único (SSO) equilibran la comodidad del usuario con problemas de seguridad.
- La idea es que un usuario pueda iniciar sesión una vez y autenticarse en ese momento. El usuario obtiene credenciales de autenticación, que luego puede utilizarse para acceder a otras máquinas y aplicaciones.
- El usuario solo tiene que recordar una secuencia de inicio de sesión y contraseña en lugar de muchos.
- En caso de ataque, el impacto de una cuenta comprometida es mayor porque un inicio de sesión otorga a un atacante acceso a múltiples máquinas y aplicaciones.

## Usuarios.
## Centralización de cuentas: SSO

- El servidor de autenticación se convierte en un cuello de botella crítico. Si no funciona, todo el trabajo útil se detiene en toda la empresa.
- Aunque SSO es una idea simple, implica una gran complejidad de back-end porque las diversas aplicaciones y máquinas a las que un usuario podría querer acceder deben comprender el proceso de autenticación y las credenciales de SSO.
- Existen varios sistemas de SSO de código abierto:
  - JOSSO, un servidor SSO de código abierto escrito en Java
  - CAS, el Servicio Central de Autenticación, de Yale (también Java)
  - Likewise Open, una herramienta de integración que hace que Microsoft Active Directory se integre con los sistemas Linux

## Usuarios.
## Centralización de cuentas: Sistemas de gestión de identidad

- Combinan varios conceptos clave de UNIX en una GUI amigable
- Estos sistemas se han diseñado teniendo en cuenta los requisitos normativos de rendición de cuentas, seguimiento y auditoría.
- Hay muchos sistemas comerciales en este espacio:
  - Oracle Identity Management
  - Sun Identity Management Suite
  - 12 Courion
  - Avatier Identity Management Suite (AIMS)
  - BMC Identity Management Suite
  - Microsoft Azure Active Directory