ANEXO TEMA 5: MONITORIZACIÓN Y FICHEROS DE CONFIGURACIÓN

0. OBJETIVO DEL DOCUMENTO

En este documento encontraras información sobre máquinas Windows y Linux y pretende alcanzar dos objetivos:

- Recoger información para controlar el funcionamiento de un sistema a través de su estado actual y del estudio de los ficheros de log.

- Identificar los ficheros de configuración de los distintos servicios instalados en la máquina, de tal forma que podamos copiarlos para volver a configurar el servicio rápidamente en caso de perdida de la máquina.

1. WINDOWS

Herramientas:

- Configuración del sistema
- Monitor del sistema
- Visor de eventos
- Archivos de log
- Consolas administrativas

1.1 MONITORIZACIÓN

UTILIZANDO:

Gestor de programas instalados en el equipo

Administrador de tareas **taskmgr.exe**

Aplicaciones

Procesos

Seleccionar las columnas de salida

Mostrar procesos de todos los usuarios.

Servicios

Rendimiento

Funciones de red

Usuarios

Visor de eventos **eventvwr.msc**

Aplicación

Seguridad

Sistema

Monitor de recursos

Monitor de rendimiento

Administración de servicios

Administración de usuarios, grupos, unidades organizativas,..

Directivas de grupo (GPO)

Gestor de cuotas y administración de discos y particiones

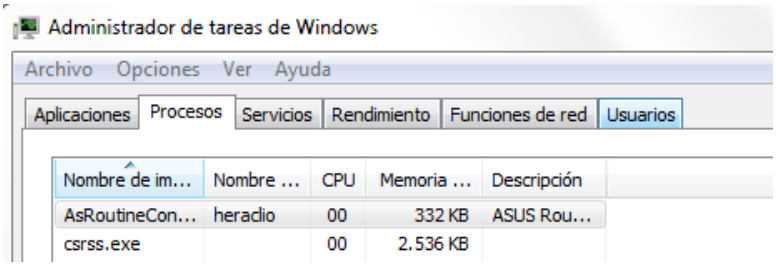
Administración de dispositivos – hardware – drivers

Log del sistema – Registro de actividad

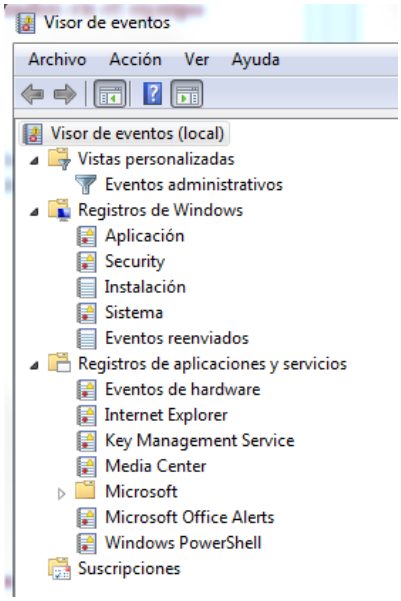
Copias de seguridad de ficheros de configuración

1.1.1 ENTORNO GRÁFICO

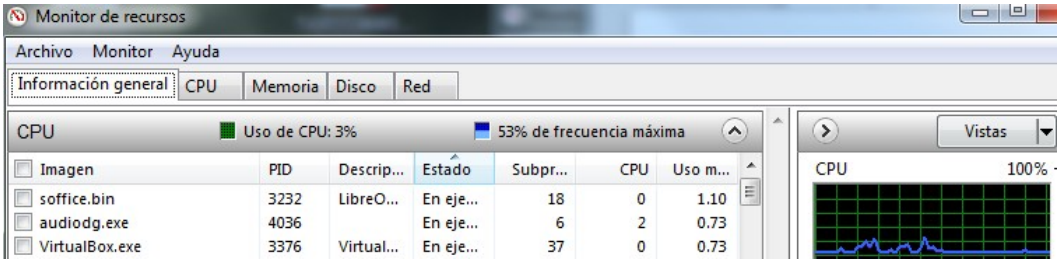
Monitor del sistema:



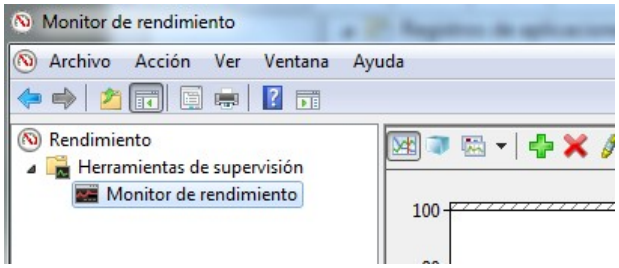
Visor de eventos:



Monitor de recursos:



Monitor de rendimiento:



Consolas administrativas:

AdRmsAdmin.msc	Active Directory Rights Management Services
Adsiedit.msc	ADSI Edit
Azman.msc	Authorization Manager
Certmgr.msc	Certmgr (Certificates)
Certtmpl.msc	Certificates Template Console
CluAdmin.msc	Failover Cluster Management
Comexp.msc	Component Services
Compmgmt.msc	Computer Management
Devmgmt.msc	Device Manager
Dfsmgmt.msc	DFS Management
Dhcpmgmt.msc	DHCP Manager
Diskmgmt.msc	Disk Management
Dnsmgmt.msc	DNS Manager
Domain.msc	Active Directory Domains And Trusts
Dsa.msc	Active Directory Users And Computers
Dssite.msc	Active Directory Sites And Services
Eventvwr.msc	Event Viewer
Fsmgmt.msc	Shared Folders
Fsrm.msc	File Server Resource Manager
Fxsadmin.msc	Microsoft Fax Service Manager
Gpedit.msc	Local Group Policy Editor
Lusrmgr.msc	Local Users And Groups
Napclcfg.msc	NAP Client Configuration
Nfsmgmt.msc	Services For Network File System
Nps.msc	Network Policy Server
Ocsp.msc	Online Responder
Perfmon.msc	Reliability And Performance Monitor
Pkiview.msc	Enterprise PKI
Printmanagement.msc	Print Management
Remoteprograms.msc	TS RemoteApp Management
Rsop.msc	Resultant Set of Policy
Secpol.msc	Local Security Policy
ServerManager.msc	Server Manager
StorageMgmt.msc	Share And Storage Management
Services.msc	Services
StorExpl.msc	Storage Explorer
Tapimgmt.msc	Telephony
Taskschd.msc	Task Scheduler
Tmp.msc	Trusted Platform Module (TPM) Management
Tsadmin.msc	Terminal Services Management
Tsconfig.msc	Terminal Services Configuration
Tsgateway.msc	TS Gateway Manager
Tsmmc.msc	Remote Desktops
Uddi.msc	UDDI Services Console
Wbadmin.msc	Windows Server Backup
Wdsmgmt.msc	Windows Deployment Services
Winsmgmt.msc	WINS Manager
WmiMgmt.msc	WMI Control

¿Que **procesos** se están ejecutando en el equipo? ¿Quien? ¿Por que?

PROCESO	EJECUTADO POR / ALMACENADO EN	UTILIDAD
winlogon.exe	SYSTEM	Valida la identidad del usuario en el sistema. Esencial.
Dwm.exe	Usuario en curso \windows\system32\	Para cambiar el comportamiento o manipular otros programas. Responsable de los efectos gráficos. Firmado por Microsoft.
Proceso inactivo del sistema	SYSTEM	Lo la CPU hace cuando no hace nada.
Hkcmd.exe	Usuario en curso \windows\system32\	Permite la configuración y diagnostico de dispositivos INTEL
Svchost.exe	Varios usuarios \windows\system32\ \windows\syswow64\	Utilizado por algunos servicios para comunicarse a través de la red
...		

¿**Servicios** que se ejecutan en mi ordenador cuando lo arranco? ¿Por que?

¿**Quien se ha conectado** hoy a mi ordenador? ¿quien ha iniciado sesión? ¿Cuando?

¿Quien **ha intentado conectarse hoy a mi ordenador y no ha podido**? ¿Con que cuenta? ¿Cuando?

Errores en el visor de eventos ¿Por que?

¿Interesado en la auditoria del login a windows? ¿Necesitas tener un control de los accesos de inicio de sesión en windows?

Auditoría de inicio de sesión en Windows.

Configuración para el registro de eventos de inicio de sesión:

1. Abrimos el **Panel de Control**
2. Clic en **Herramientas administrativas**
3. Clic en **Directiva de seguridad local**
4. Al abrirse la nueva ventana desplegamos la opción de **Directivas locales** y **Directiva de auditoría.**
5. Doble clic en **Auditar eventos de inicio de sesión**
6. Marcamos las casillas de **correcto** y **erróneo**
7. **Aceptar.**

Visualizar todos los eventos auditados de inicio de sesión que se van registrando en el sistema:

1. Abrimos el **Panel de Control**
2. Clic en **Herramientas administrativas**
3. Clic en **Visor de eventos**
4. Al abrirse la nueva ventana, seleccionamos **Seguridad** del menú.
5. El resultado son todos los registros separados por líneas.

Virus que parecen procesos

filtro: Auditoría de seguridad, inicio de sesión.

Ejemplo de auditoría de los usuarios del sistema:

¿Qué información aparece en el visor de eventos?

Objetivo1: **control / auditoría del acceso de los usuarios al sistema**
Objetivo2: **control /auditoría del acceso de los usuarios a cualquier recurso**

AUDITORÍA DE SEGURIDAD AVANZADA

LOGON/LOGOFF

Id de inicio de sesión
Id del evento
- 4624: Inicio de sesión correcta de una cuenta
- 4648: Intento de inicio de sesión con credenciales explícitas
- 4625: Acceso fallido de una cuenta
- 4647: Cierre de sesión iniciado por el usuario
- 4634: Se cerró la sesión en una cuenta

Auditar Logon

Auditar Logoff

Guía paso a paso de la directiva de seguridad avanzada

Planear la auditoría de acceso a archivos

Aplicar o modificar la configuración de directiva de auditoría de un archivo o una carpeta local

1.1.2 LÍNEA DE COMANDOS

SERVICIO	COMANDO	UTILIDAD
	hostname	muestra el nombre del equipo
	winver	muestra la versión del sistema operativo
	getmac	muestra la dirección física (MAC)
	ipconfig ipconfig /all	muestra la configuración de red
	ipconfig /release ipconfig /renew	borra y solicita ip dinámica (DHCP)
	route print	muestra la tabla de rutas
	ping	prueba de conectividad
	diskpart • **list disk** • **select disk** ○ **list partition**	configuración y gestión de discos y particiones
	nslookup	prueba del DNS
	netstat	conexiones establecidas en el sistema
	tracert	ruta hasta el destino
	arp arp -a	gestión de la tabla arp
	netsh	configuración de la red
	ssh	conexión remota segura
	ftp	transferencia de ficheros
	scp	transferencia de ficheros segura
	shutdown /r shutdown /s	apagar el equipo

PowerShell

PowerShell es un shell de línea de comandos y un lenguaje de scripting basado en tareas integrado en .NET. PowerShell ayuda a los administradores de sistemas y a los usuarios avanzados a automatizar rápidamente las tareas que administran sistemas operativos (**Linux, macOS y Windows**) y procesos.

Los comandos de PowerShell permiten administrar los equipos desde la línea de comandos. Los proveedores de PowerShell permiten obtener acceso a almacenes de datos, como el Registro y el almacén de certificados, con la misma simplicidad con que se obtiene acceso al sistema de archivos. **PowerShell incluye un analizador de expresiones muy completo y un lenguaje de scripting totalmente desarrollado.**

ACTIVE DIRECTORY

11 herramientas esenciales para administrar Active Directory

net session

```
C:\Users\Administrador>net session

Equipo                  Usuario              Tipo cliente    Abre tiempo inact.
-------------------------------------------------------------------------------
\\192.168.10.2          ambrosio                                1 00:01:07

\\192.168.10.3          Heraclio                                3 00:02:50

\\192.168.2.100         meli                                    1 01:36:26

\\192.168.3.100         eduardo                                 3 00:22:48

\\192.168.5.100         amor                                    1 00:18:23

Se ha completado el comando correctamente.
```

quser

```
C:\Users\Administrador>quser
 NOMBRE USUARIO        NOMBRE SESIóN      ID. ESTADO  TIEMPO IN. TIEMPO SESIóN
>administrador         rdp-tcp#0           2  Activo          .  09/12/2014 9:52
```

netstat

```
C:\Users\Administrador>netstat

Conexiones activas

  Proto  Dirección local        Dirección remota       Estado
  TCP    127.0.0.1:389          dc1:49160              ESTABLISHED
  TCP    127.0.0.1:389          dc1:49162              ESTABLISHED
  TCP    127.0.0.1:389          dc1:53932              ESTABLISHED
  TCP    127.0.0.1:49160        dc1:ldap               ESTABLISHED
  TCP    127.0.0.1:49162        dc1:ldap               ESTABLISHED
  TCP    127.0.0.1:53932        dc1:ldap               ESTABLISHED
  TCP    192.168.20.101:389     dc1:53919              ESTABLISHED
  TCP    192.168.20.101:389     dc1:53929              ESTABLISHED
  TCP    192.168.20.101:389     dc1:53948              ESTABLISHED
  TCP    192.168.20.101:445     is31w7pr:64283         ESTABLISHED
  TCP    192.168.20.101:445     is32w7pr:63010         ESTABLISHED
  TCP    192.168.20.101:445     is22w7pr:52441         ESTABLISHED
  TCP    192.168.20.101:445     departamento-2:4013    ESTABLISHED
  TCP    192.168.20.101:445     departamento-3:49808   ESTABLISHED
  TCP    192.168.20.101:3389    departamento-3:50470   ESTABLISHED
  TCP    192.168.20.101:53919   dc1:ldap               ESTABLISHED
  TCP    192.168.20.101:53929   dc1:ldap               ESTABLISHED
  TCP    192.168.20.101:53948   dc1:ldap               ESTABLISHED
  TCP    192.168.20.101:58814   dc2:epmap              SYN_SENT
  TCP    192.168.20.101:58815   dc2:epmap              SYN_SENT
  TCP    [::1]:49157            dc1:50957              ESTABLISHED
  TCP    [::1]:49157            dc1:53212              ESTABLISHED
  TCP    [::1]:49157            dc1:53498              ESTABLISHED
  TCP    [::1]:49157            dc1:53512              ESTABLISHED
  TCP    [::1]:50957            dc1:49157              ESTABLISHED
  TCP    [::1]:53212            dc1:49157              ESTABLISHED
  TCP    [::1]:53498            dc1:49157              ESTABLISHED
  TCP    [::1]:53512            dc1:49157              ESTABLISHED
```

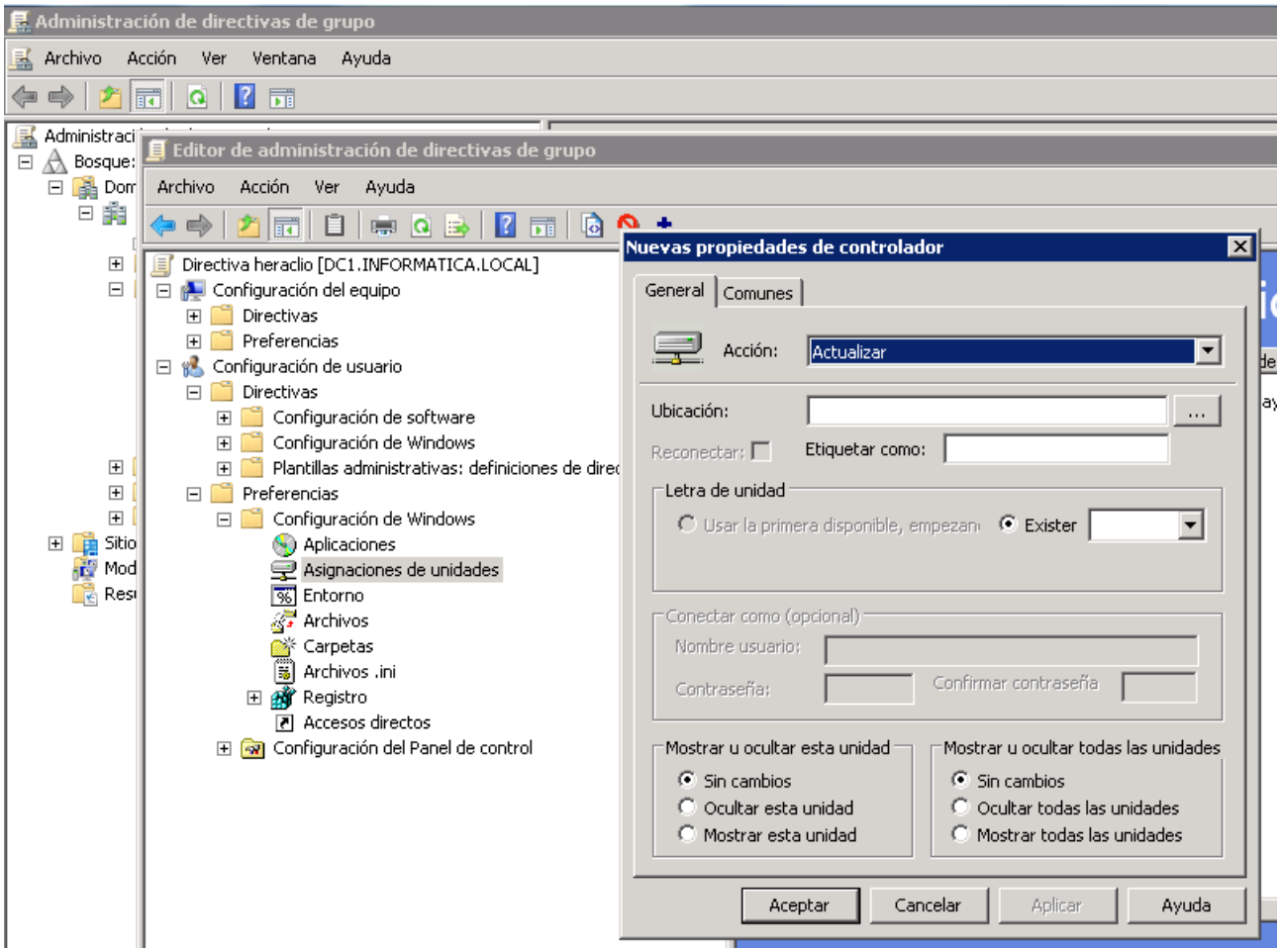
1.2 FICHEROS DE CONFIGURACIÓN

1.2.1 GPO - DIRECTIVAS DE GRUPO

- Asignar scripts de inicio del equipo
- Asignar scripts de apagado del equipo
- Asignar scripts de inicio de sesión del usuario
- Asignar scripts de cierre de sesión del usuario

Asignar script de inicio de sesión del usuario

Conectar una unidad de red mediante GPO

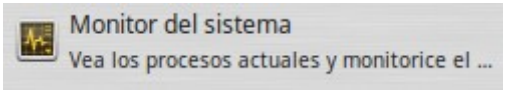


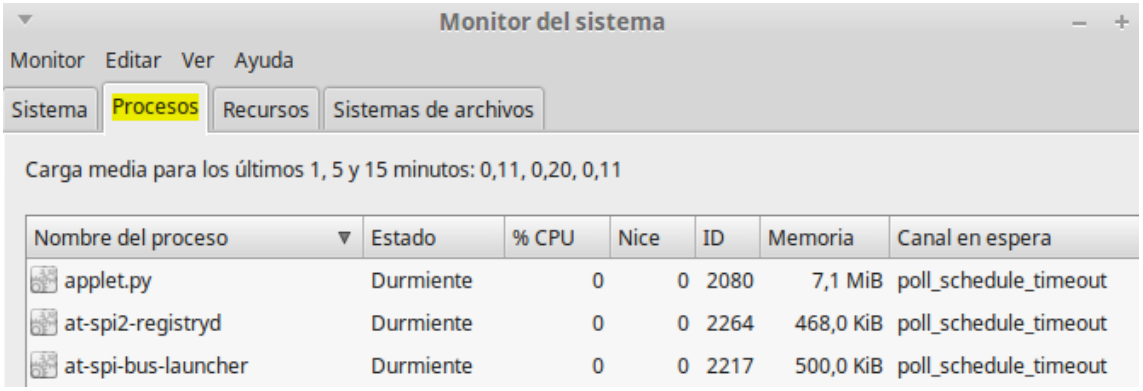
2. LINUX – UBUNTU SERVER

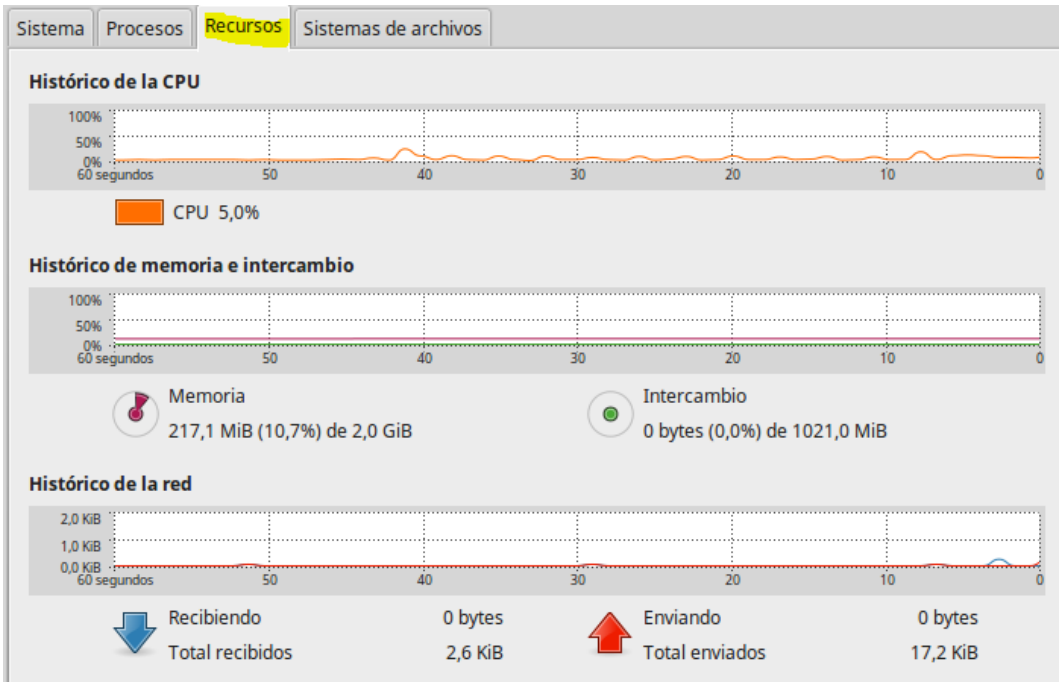
2.1 MONITORIZACIÓN

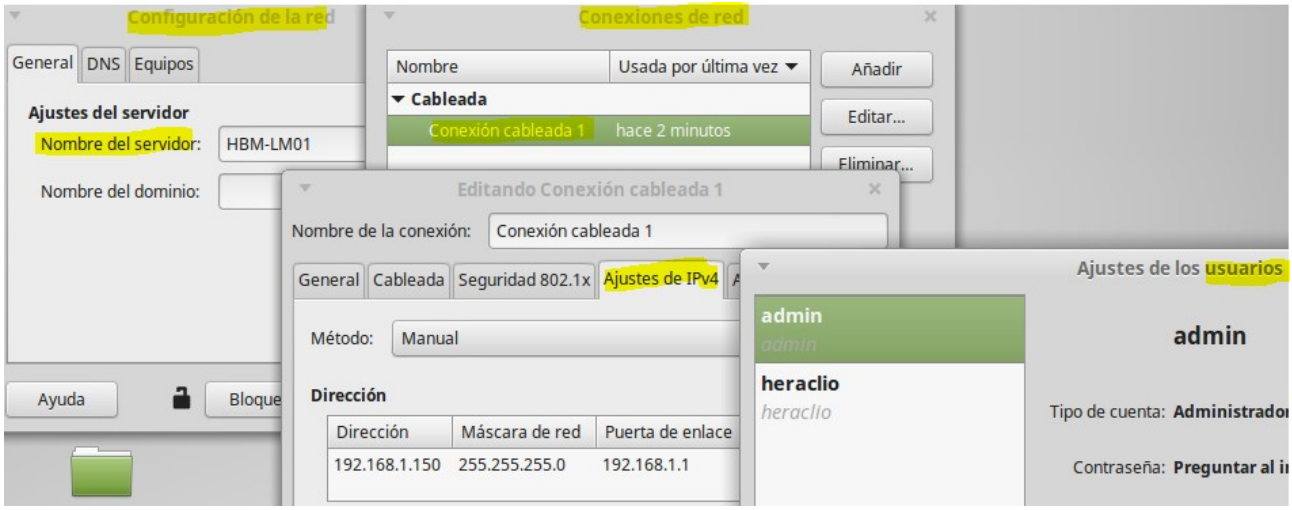
2.1.1 ENTORNO GRÁFICO

Disponible en los clientes linux y en los servidores donde tengamos instalado el entorno gráfico.






Sistema
Procesos
Recursos
Sistemas de archivos
Histórico de la CPU
100%
50%
0%
60 segundos
50
40
30
20
10
0
CPU 5,0%
Histórico de memoria e intercambio
Memoria
217,1 MiB (10,7%) de 2,0 GiB
Intercambio
0 bytes (0,0%) de 1021,0 MiB
Histórico de la red
2,0 KiB
1,0 KiB
0,0 KiB
Recibiendo
0 bytes
Total recibidos
2,6 KiB
Enviando
0 bytes
Total enviados
17,2 KiB


Configuración de la red
General
DNS
Equipos
Ajustes del servidor
Nombre del servidor:
HBM-LM01
Nombre del dominio:
Ayuda
Conexiones de red
Nombre
Usada por última vez
Cableada
Conexión cableada 1
hace 2 minutos
Añadir
Editar...
Eliminar...
Editando Conexión cableada 1
Nombre de la conexión:
Conexión cableada 1
General
Cableada
Seguridad 802.1x
Ajustes de IPv4
Método:
Manual
Dirección
Dirección
Máscara de red
Puerta de enlace
192.168.1.150
255.255.255.0
192.168.1.1
Ajustes de los usuarios
admin
admin
heraclio
heraclio
admin
Tipo de cuenta:
Contraseña:

2.1.1 LÍNEA DE COMANDOS

Comandos

SERVICIO	COMANDO	UTILIDAD
	hostname	muestra el nombre del equipo
	uname -a	muestra la versión del sistema operativo
	ifconfig -a ip a **ip link show nombredeinterface**	muestra la configuración de red
	route	muestra la tabla de rutas
	cat /proc/sys/net/ipv4/ip_forward	muestra si está habilitado (1) o deshabilitado (0) el servicio de enrutamiento
	cat /etc/resolv.conf	muestra la dirección IP del servidor DNS asignado al equipo
	ping	prueba de conectividad
	nslookup **nameserver**	prueba del DNS
	ps -ef	muestra el estado de los procesos activos en el sisema
	kill	para terminar un proceso
	reboot	para reiniciar o apagar el equipo
	start stop restart status …	para gestionar un servicio
	apt-get	para gestionar paquetes
	netstat	conexiones establecidas en el sistema
	traceroute	ruta hasta el destino
	arp arp -a	gestión de la tabla arp
	ssh	conexión remota segura
	ftp	transferencia de ficheros
	scp	transferencia de ficheros segura
	df -h	utilización del disco
	mount	monta sistemas de ficheros
	fdisk -l **lsblk -a lsblk -fn lsblk -fm**	gestiona la tabla de particiones
	pstree	muestra la estructura de directorios

SERVICIO	COMANDO	UTILIDAD
	top	
	find / -name	Buscador de ficheros
	service ufw status **service ufw enable** **service ufw disable** **ps -ef|grep ufw**	Gestión del servicio UFW - Firewall
	reboot **halt -p** **sutdown -h**	Reiniciar / parar la máquina
	sudo **sudo su** **exit**	Cambiar de ususuario
	dhclient -r **dhclient**	Borrar / renovar asignación ip DHCP

Linux Shell Scripting Tutorial

2.1.2 FICHEROS DE LOG

Almacenados en el directorio **/var/log**

/var/log/	Archivos de log
syslog	Información general del funcionamiento del sistema
auth-log	Control de acceso: acceso o intentos de acceso
dmesg	Mensajes del arranque del Sistema Operativo. Problemas harware
dpkg.log	Registro de instalaciones y desinstalaciones dpkg
/apt/term.log	Log del comando apt
unattended-upgrades	Registro de actualizaciones automáticas

2.2 FICHEROS DE CONFIGURACIÓN

Ficheros y directorios de configuración

SERVICIO	FICHERO	DESCRIPCIÓN
NOMBRE	**/etc/hostname**	Contiene el nombre del equipo
DISTRIBUCIÓN	**/etc/version**	Versión de la distribución
LOCALHOST	**/etc/hosts**	Contiene la resolución de nombres para localhost
RED	**/etc/network/interfaces**	Contiene la configuración de red del equipo
ROUTER	**/proc/sys/net/ipv4/ip_forward**	Contiene un 1 cuando está habilitado el servicio de enrutamiento y un 0 cuando está deshabilitado
	/etc/sysctl.conf	Variables de configuración del kernel Fichero de configuración que se ejecuta en el arranque del equipo. Lo utilizamos para activar el servicio de enrutamiento.
DNS	**/etc/resolv.conf**	Contiene la dirección IP de los servidores DNS utilizados por el equipo
NAT	**/etc/rc.local**	Fichero de configuración que se ejecuta en el arranque del equipo. Configuración personal del proceso de arranque. Lo utilizamos para habilitar NAT cuando no tenemos cortafuegos de red.
cuentas locales	**/etc/passwd**	Contiene las cuentas locales del equipo
	/etc/shadow	Contiene las contraseñas
grupos locales	**/etc/group**	Contiene los grupos definidos en el equipo
root	**/etc/sudoers**	Lista de usuarios con privilegios especiales de root y los comandos que pueden ejecutar

SERVICIO	FICHERO	DESCRIPCIÓN
Variables de entorno	**/etc/profile**	Variables de entorno globales a todos los usuarios
particiones y sistema de archivos	**/etc/fstab**	Lista de sistemas de archivos montados automáticamente en el arranque del sistema
	/etc/mtab	Lista de sistemas de archivos montados actualmente
SMB	**/etc/samba/smb.conf**	Fichero de configuración de samba

3. RECUPERACIÓN DE UN EQUIPO CON PROBLEMAS

3.1 EJEMPLO DE PROCEDIMIENTO DE REPARACIÓN DE UN EQUIPO CON PROBLEMAS DE SOFTWARE (MALWARE):

Cuando un equipo estropeado con problemas de software entra en el taller, se comprueba su problema y se llega a una conclusión para solucionarlo.

1. Se procede a ver el sistema nada más iniciar el equipo y ver posibles problemas (ventanas emergentes, programas trampa, más de 1 antivirus, etc.)
2. Una vez analizados los problemas se pasa a bajar los 3 programas de limpieza: **ADWCleaner**, **Combofix** y **Malwabyte Antimalware**.
3. Antes de iniciar los programas de limpieza en Ejecutar pondremos msconfig y miraremos las opciones de inicio del sistema. Una vez visto se procederá a deshabilitar los programas/aplicaciones que ralenticen el equipo o que no necesiten iniciarse al encender el equipo.
4. Iniciaremos el primer programa: ADWCleaner. Este programa busca por todo el sistema carpetas, ficheros, extensiones en navegadores..., los lista y elimina todos los seleccionados. Cuando acaba este programa reinicia el equipo y después de iniciar nos saltara un fichero con todo lo que ha borrado.
5. El siguiente a iniciar es el Combofix, este programa busca más malware pero de forma más profunda, al igual que el ADW nos sacara un fichero con todo lo que ha borrado. Aparte este programa te da la opción de hacer una copia de seguridad antes de iniciar el borrado de los archivos que él considera peligrosos.
6. Una vez pasado el Combofix el siguiente en iniciar es el Malwarebyte, este programa es como un antivirus, algo más rápido y más eficaz. Al acabar de analizar el equipo borrara lo que encuentre y reinicia el equipo.
7. Por último se pasa el antivirus de equipo para ver si queda algo, se revisan las extensiones de los navegadores y si queda algún programa que los 3 limpiadores no hayan podido quitar. Después de verificar estos cambios se desinstalan los programas de limpieza y se pasa el CCleaner para borrar archivos basura.
8. En el supuesto caso que el grado de infección sea muy alto se llamara al cliente para pedirle el consentimiento de salvar datos y reinstalar el sistema operativo.

Si el ordenador posee el virus de la policía, el proceso cambia:

1. Se ejecutará Mini Windows XP con la herramienta de CD Hiren'sBoot. Se buscará en el sistema, dentro de la carpeta %AppData% los archivos Skype.dat y otros archivos renombrados como Skype. (extensión) y se eliminarán.
2. El ordenador conseguirá arrancar en cuanto estos archivos hayan sido eliminados. Desde ahí, se podrá realizar el proceso normal para la eliminación de malware.

3.2 EJEMPLO DE PROCEDIMIENTO DE REPARACIÓN DE UN EQUIPO CON PROBLEMAS DE HARDWARE

Si el ordenador posee un problema de hardware, se testearían los componentes.

1. Testeo de disco duro con las herramientas de “Hard Disk Tools” del Hiren’sBoot.
2. Testeo de memoria con las herramientas de “Memory Tools” del Hiren’sBoot, normalmente la herramienta “MemTest”.
3. Testeo de fuente de alimentación con el tester físico de fuentes.

Herramientas:

- Configuración del sistema
- Monitor del sistema
- Visor de eventos
- Archivos de log
- Consolas administrativas