

Tarefas UD03

Bloque 01

Administración de sistemas operativos

*Unidade Didáctica 01:
Información do sistema*

Nome: Ruben

Apellidos: Rey Feal

Data:



Índice

Tarefa 1. Estrutura de directorios.....	.1
1.1. MS Windows1
1.2. POSIX2
Tarefa 2. Sistemas de ficheiros.....	.4
Tarefa 3. Busca de rastros e información.....	.6
3.1. MS Windows6
3.2. GNU/Linux14
Tarefa 4. Sistemas de ficheiros virtuais.....	.23
4.1. MS Windows23
4.1.1. <i>Instalación servidor SMB/CIFS</i>23
4.1.2. <i>Configuración SMB/CIFS para un cliente GNU/Linux</i>24
4.1.3. <i>Configuración SMB/CIFS para un cliente Windows</i>25
4.2. GNU/Linux26
4.2.1. <i>Instalación servidor SMB/CIFS</i>26
4.2.2. <i>Configuración SMB/CIFS para un cliente GNU/Linux</i>27
4.2.3. <i>Configuración SMB/CIFS para un cliente Windows</i>28
Tarefa 5. Siglas.....	.29

Tarefa 1. Estrutura de directorios

1.1. MS Windows

En canto a estrutura de directorios dos sistemas Windows, cubrir a seguinte táboa cos directorios máis destacados, indicando a súa ruta/*path* habitual e o seu contido e/ou función. Engadir as filas que se vexan necesarias. Non quedarse só cos directorios do raíz, é dicir, tamén indicar por exemplo subdirectorios destacados de C:\Windows\...

Nome dir.	Path	Función/Contido
Raíz do disco	C:\	Contén os directorios principais do sistema operativo e outros arquivos do usuario ou programas instalados.
Windows	C:\Windows	Directorio do sistema operativo Windows; contén os arquivos principais para o funcionamento do sistema.
System32	C:\Windows\System32	Arquivos executables e DLLs críticos para o funcionamento do sistema operativo.
SysWOW64	C:\Windows\SysWOW64	Versión de 32 bits dos arquivos do sistema en sistemas operativos de 64 bits; necesario para compatibilidade con aplicacións máis antigas.
WinSxS	C:\Windows\WinSxS	Almacena múltiples versións de arquivos DLL para asegurar compatibilidade e estabilidade do sistema.
Temp	C:\Windows\Temp	Arquivos temporais creados polo sistema operativo ou programas, que poden ser borrados de forma segura en moitos casos.
Program Files	C:\Program Files	Directorio para programas instalados de 64 bits.
Program Files (x86)	C:\Program Files (x86)	Directorio para programas instalados de 32 bits en sistemas operativos de 64 bits.
Users	C:\Users	Directorio que contén os perfís de usuario.
Desktop	C:\Users\<usuario>\Desktop	Escritorio do usuario; contén accesos directos e arquivos visibles no escritorio.
Documents	C:\Users\<usuario>\Documents	Carpeta de documentos do usuario; usada para almacenar arquivos persoais.
Downloads	C:\Users\<usuario>\Downloads	Descargas realizadas polo usuario desde o navegador ou outras aplicacións.
AppData	C:\Users\<usuario>\AppData	Arquivos e configuracións específicas das aplicacións. Divídese en tres subdirectorios: Local, LocalLow e Roaming.
Local	C:\Users\<usuario>\AppData\Local	Datos específicos do dispositivo; típicos de aplicacións que non precisan sincronizarse entre dispositivos.

Nome dir.	Path	Función/Contido
Roaming	C:\Users\<usuario>\AppData\Roaming	Datos que se sincronizan en distintos dispositivos (en redes corporativas ou coa conta de Microsoft).
LocalLow	C:\Users\<usuario>\AppData\LocalLow	Usado por aplicacións que precisan menos privilexios ou son de seguridade reducida (ex.: navegadores en modo restrinxido).
System Volume Information	C:\System Volume Information	Arquivos do sistema, como puntos de restauración, bases de datos de indexación, e outros datos críticos do disco.
Pagefile.sys	C:\pagefile.sys	Arquivo de memoria virtual usado para xestionar a memoria cando a RAM está chea.
Hiberfil.sys	C:\hiberfil.sys	Arquivo usado para almacenar o estado do sistema cando se activa o modo de hibernación.
Recycle Bin	C:\\$Recycle.Bin	Contén arquivos e carpetas eliminadas polo usuario, pero aínda recuperables dende a papeleira de reciclaxe.
Drivers	C:\Windows\System32\drivers	Controladores de hardware necesarios para o funcionamento de dispositivos conectados ao sistema.

1.2. POSIX

En canto a estrutura de directorios dos sistemas POSIX, cubrir a seguinte táboa cos directorios máis destacados, indicando a súa ruta/*path* habitual e o seu contido e/ou función. Engadir as filas que se vexan necesarias. Non quedarse só cos directorios do raíz, é dicir, tamén indicar por exemplo subdirectorios destacados de /var/... ou de /usr/...

Nome dir.	Path	Función/Contido
raíz	/	Directorio raíz que contén todos os demais directorios do sistema.
bin	/bin	Comandos e programas básicos do sistema accesibles a todos os usuarios, como <code>ls</code> , <code>cp</code> , <code>mv</code> , entre outros.
sbin	/sbin	Comandos e programas para administración do sistema, normalmente só accesibles ao superusuario.
etc	/etc	Arquivos de configuración do sistema e servizos, como <code>passwd</code> , <code>hosts</code> , <code>ssh</code> , entre outros.
home	/home	Directorio que contén os subdirectorios dos usuarios do sistema, con arquivos e

Nome dir.	Path	Función/Contido
		configuracións persoais.
root	/root	Directorio persoal do superusuario (root).
var	/var	Arquivos que cambian frecuentemente no sistema, como logs, datos de aplicacións, colas de impresión, entre outros.
usr	/usr	Programas, bibliotecas e datos de usuario que non son críticos para o arranque do sistema.
opt	/opt	Directorio para instalación de software adicional de terceiros.
tmp	/tmp	Arquivos temporais do sistema ou aplicacións; normalmente eliminados tras un reinicio.
dev	/dev	Dispositivos de hardware representados como arquivos especiais, como discos (/dev/sda), terminais, ou interfaces de rede.
proc	/proc	Sistema de arquivos virtual que proporciona información sobre procesos en execución e o estado do sistema.
sys	/sys	Sistema de arquivos virtual para interactuar co hardware e os controladores.
boot	/boot	Arquivos necesarios para o arranque do sistema, como o kernel e o cargador de arranque (grub).
lib	/lib	Bibliotecas compartidas necesarias para os programas no directorio /bin e /sbin.
mnt	/mnt	Punto de montaxe temporal para sistemas de arquivos ou dispositivos externos.
media	/media	Punto de montaxe automático para dispositivos externos como discos USB ou CD-ROM.
srv	/srv	Datos específicos dun servizo, como servidores web ou FTP.

Tarefa 2. Sistemas de ficheiros

Existen diferentes tipos de sistemas de ficheiros, con diferentes técnicas de implementación, tamaños de bloque, características de seguridade, etc.

Investiga e cubre a seguinte táboa relativa aos tipos de sistemas de ficheiros:

Tipo sistema de ficheiros	Características	Exemplos
Transaccionais	Garantizan consistencia e recuperación en fallos mediante transaccións ACID.	NTFS (transaccións), ZFS
Distribuídos	Xestionan ficheiros en múltiples máquinas, con redundancia, escalabilidade e alta dispoñibilidade.	HDFS, Ceph, GlusterFS
Cifrados	Ofrecen cifrado para protexer datos contra accesos non autorizados, garantindo seguridade.	EFS, ext4 (con dm-crypt/LUKS)
Virtuais	Non almacenan datos, actúan como interfaces para acceder a recursos ou sistemas (abstracción).	procfs, sysfs, tmpfs, FUSE

Contestar ás seguintes cuestións:

1. En Windows é preciso que o ficheiro teña extensión para que sexa recoñecido polas aplicacións que o manexa? E en GNU/Linux?

Windows necesita extensiones para identificar programas; GNU/Linux no, ya que reconoce archivos por permisos o contenido.

2. Importa o que o nome do ficheiro esta en maiúsculas ou minúsculas?

Windows no distingue entre ellas; GNU/Linux sí, siendo `archivo.txt` y `ARCHIVO.TXT` diferentes.

3. Cal é o límite de caracteres para un ficheiro en Windows? E en GNU/Linux?

Windows y GNU/Linux permiten nombres de hasta 255 caracteres, pero GNU/Linux admite rutas de hasta 4096 bytes.

4. Son o mesmo os atributos que os permisos dun ficheiro ou directorio? Se non son o mesmo, indica un exemplo claro onde se manexen e distingan cada concepto en Windows e a continuación en GNU/Linux.

Atributos definen propiedades (solo lectura, oculto), mientras que los permisos controlan acceso (lectura, escritura, ejecución).

5. Que é un i-nodo? Indica un comando en GNU/Linux no que se vexa o i-nodo de ficheiros e directorios.

Es una estructura que almacena metadatos del archivo (permisos, tamaño); se visualiza con `ls -li`.

6. Que diferencia un enlace duro dun enlace simbólico/*soft*? Indica como se crearían en GNU/Linux?

El enlace duro comparte el i-nodo original; el simbólico solo apunta al nombre del archivo.

7. Que son SELinux e AppArmor, e que aportan aos sistemas GNU/Linux?

Ambos restringen acceso en GNU/Linux; SELinux es más complejo y granular, AppArmor usa perfiles más simples basados en rutas.

Tarefa 3. Busca de rastros e información

3.1. MS Windows

Usando o comando findstr, trata de resolver os seguintes enunciados traballando sobre os ficheiros

C:\Windows\Logs\CBS\CBS.log e C:\Windows\Logs\DISM\dism.log:

1. Consulta a axuda sobre o comando findstr:

```
C:\Program Files (x86)\VMware\VMware Player\bin>help findstr
Busca cadenas en los archivos.

FINDSTR [/B] [/E] [/L] [/R] [/S] [/I] [/X] [/V] [/N] [/M] [/O] [/P]
        [/F:archivo] [/C:cadena] [/G:archivo] [/D:lista_directorios]
        [/A:atrib_color] [/OFF[LINE]] cadenas [[unidad:][ruta]archivo[ ...]]

/B      Hace coincidir los modelos si están al principio de la línea.
/E      Hace coincidir los modelos si están al final de la línea.
/L      Literalmente usa cadenas de búsqueda.
/R      Usa cadenas de búsqueda como expresiones regulares.
/S      Busca archivos que coinciden en el directorio actual y en todos
        los subdirectorios.
/I      Especifica que la búsqueda no distingue mayúsculas de minúsculas.
/X      Imprime líneas que coinciden con exactitud.
/V      Solo imprime líneas que no contienen una correspondencia.
/N      Imprime el número de la línea antes de la línea que coincide.
/M      Solo imprime el nombre de archivo si el archivo contiene una
        correspondencia.
/O      Imprime un carácter de desplazamiento antes de las líneas que
        coinciden.
/P      Omite archivos con caracteres que no son imprimibles
/OFF[LINE] No omite archivos con el atributo "sin conexión" establecido.
/A:atr  Especifica atributos de color con dos dígitos hexadecimales.
        Consulte "color /?"
/F:archivo Lee la lista de archivos desde el archivo especificado
        (/ significa consola).
/C:cadena Usa una cadena especificada como una búsqueda de cadena
        literal.
/G:archivo Toma la búsqueda de archivos desde el archivo especificado
        (/ significa consola).
/D:dir   Busca un signo de punto y coma de la lista delimitada de
        directorios
cadenas  Texto que se va a buscar.
[unidad:][ruta]archivo
        Especifica el archivo o archivos que se van a buscar.

Usa espacios para separar múltiples cadenas de búsqueda a no ser que
el argumento lleve un prefijo con /C. Por ejemplo, 'FINDSTR "qué tal" x.y'
busca "qué" o "tal" en el archivo x.y. 'FINDSTR /C:"qué tal" x.y' busca
"qué tal" en el archivo x.y.

Expresión regular de referencia rápida:
.      Comodín: cualquier carácter
*      Repetir: cero o más ocurrencias de un carácter previo o de clase
^      Posición de línea: comienzo de la línea
$      Posición de línea: fin de línea
[clase] Clase de carácter: cualquier carácter en la serie
[^clase] Clase inversa: cualquier carácter que no esté en la serie
[x-y]   Intervalo: cualquier carácter que esté dentro del intervalo
        especificado
\x      Escape: uso literal de un metacarácter x
\<xyz   Posición de palabra: principio de palabra
xyz\>   Posición de palabra: fin de palabra
```

Para obtener una información más completa sobre expresiones regulares de FINDSTR referirse al Comando de referencia Command en línea.

C:\Program Files (x86)\VMware\VMware Player\bin>

2. Busca no ficheiro CBS.log as liñas que teñan a palabra windows ou microsoft:

```
Command Prompt for vctl
s-LanguageFeatures-Basic-fr-be-Package~31bf3856ad364e35~amd64~~10.0.19041.1, applicable state: Installed
2024-11-27 12:40:42, Info CBS Appl: Evaluating package applicability for package Microsoft-Windows-
s-LanguageFeatures-Basic-fil-ph-Package~31bf3856ad364e35~amd64~~10.0.19041.1, applicable state: Installed
2024-11-27 12:40:42, Info CBS Appl: Evaluating package applicability for package Microsoft-Windows-
s-LanguageFeatures-Basic-fi-fi-Package~31bf3856ad364e35~amd64~~10.0.19041.1, applicable state: Installed
2024-11-27 12:40:42, Info CBS Appl: Evaluating package applicability for package Microsoft-Windows-
s-LanguageFeatures-Basic-fa-ir-Package~31bf3856ad364e35~amd64~~10.0.19041.1, applicable state: Installed
2024-11-27 12:40:42, Info CBS Appl: Evaluating package applicability for package Microsoft-Windows-
s-LanguageFeatures-Basic-eu-es-Package~31bf3856ad364e35~amd64~~10.0.19041.1, applicable state: Installed
2024-11-27 12:40:42, Info CBS Appl: Evaluating package applicability for package Microsoft-Windows-
s-LanguageFeatures-Basic-et-ee-Package~31bf3856ad364e35~amd64~~10.0.19041.1, applicable state: Installed
2024-11-27 12:40:42, Info CBS Appl: Evaluating package applicability for package Microsoft-Windows-
s-LanguageFeatures-Basic-es-us-Package~31bf3856ad364e35~amd64~~10.0.19041.1, applicable state: Installed
2024-11-27 12:40:42, Info CBS Appl: Evaluating package applicability for package Microsoft-Windows-
s-LanguageFeatures-Basic-es-mx-Package~31bf3856ad364e35~amd64~~10.0.19041.1, applicable state: Installed
2024-11-27 12:40:42, Info CBS Appl: Evaluating package applicability for package Microsoft-Windows-
s-LanguageFeatures-Basic-en-us-Package~31bf3856ad364e35~amd64~~10.0.19041.1, applicable state: Installed
2024-11-27 12:40:42, Info CBS Appl: Evaluating package applicability for package Microsoft-Windows-
s-LanguageFeatures-Basic-en-in-Package~31bf3856ad364e35~amd64~~10.0.19041.1, applicable state: Installed
2024-11-27 12:40:42, Info CBS Appl: Evaluating package applicability for package Microsoft-Windows-
s-LanguageFeatures-Basic-en-gb-Package~31bf3856ad364e35~amd64~~10.0.19041.1, applicable state: Installed
2024-11-27 12:40:42, Info CBS Appl: Evaluating package applicability for package Microsoft-Windows-
s-LanguageFeatures-Basic-en-ca-Package~31bf3856ad364e35~amd64~~10.0.19041.1, applicable state: Installed
2024-11-27 12:40:42, Info CBS Appl: Evaluating package applicability for package Microsoft-Windows-
s-LanguageFeatures-Basic-en-au-Package~31bf3856ad364e35~amd64~~10.0.19041.1, applicable state: Installed
2024-11-27 12:40:42, Info CBS Appl: Evaluating package applicability for package Microsoft-Windows-
s-LanguageFeatures-Basic-el-gr-Package~31bf3856ad364e35~amd64~~10.0.19041.1, applicable state: Installed
2024-11-27 12:40:42, Info CBS Appl: Evaluating package applicability for package Microsoft-Windows-
s-LanguageFeatures-Basic-de-de-Package~31bf3856ad364e35~amd64~~10.0.19041.1, applicable state: Installed
2024-11-27 12:40:42, Info CBS Appl: Evaluating package applicability for package Microsoft-Windows-
s-LanguageFeatures-Basic-de-ch-Package~31bf3856ad364e35~amd64~~10.0.19041.1, applicable state: Installed
2024-11-27 12:40:42, Info CBS Appl: Evaluating package applicability for package Microsoft-Windows-
s-LanguageFeatures-Basic-da-dk-Package~31bf3856ad364e35~amd64~~10.0.19041.1, applicable state: Installed
2024-11-27 12:40:42, Info CBS Appl: Evaluating package applicability for package Microsoft-Windows-
s-LanguageFeatures-Basic-cy-gb-Package~31bf3856ad364e35~amd64~~10.0.19041.1, applicable state: Installed
2024-11-27 12:40:42, Info CBS Appl: Evaluating package applicability for package Microsoft-Windows-
s-LanguageFeatures-Basic-cs-cz-Package~31bf3856ad364e35~amd64~~10.0.19041.1, applicable state: Installed
2024-11-27 12:40:42, Info CBS Appl: Evaluating package applicability for package Microsoft-Windows-
s-LanguageFeatures-Basic-ca-es-Package~31bf3856ad364e35~amd64~~10.0.19041.1, applicable state: Installed
2024-11-27 12:40:42, Info CBS Appl: Evaluating package applicability for package Microsoft-Windows-
s-LanguageFeatures-Basic-bs-latn-ba-Package~31bf3856ad364e35~amd64~~10.0.19041.1, applicable state: Installed
2024-11-27 12:40:42, Info CBS Appl: Evaluating package applicability for package Microsoft-Windows-
s-LanguageFeatures-Basic-bn-in-Package~31bf3856ad364e35~amd64~~10.0.19041.1, applicable state: Installed
2024-11-27 12:40:42, Info CBS Appl: Evaluating package applicability for package Microsoft-Windows-
s-LanguageFeatures-Basic-bn-bd-Package~31bf3856ad364e35~amd64~~10.0.19041.1, applicable state: Installed
2024-11-27 12:40:42, Info CBS Appl: Evaluating package applicability for package Microsoft-Windows-
s-LanguageFeatures-Basic-bg-bg-Package~31bf3856ad364e35~amd64~~10.0.19041.1, applicable state: Installed
2024-11-27 12:40:42, Info CBS Appl: Evaluating package applicability for package Microsoft-Windows-
s-LanguageFeatures-Basic-be-by-Package~31bf3856ad364e35~amd64~~10.0.19041.1, applicable state: Installed
2024-11-27 12:40:42, Info CBS Appl: Evaluating package applicability for package Microsoft-Windows-
s-LanguageFeatures-Basic-ba-ru-Package~31bf3856ad364e35~amd64~~10.0.19041.1, applicable state: Installed
2024-11-27 12:40:42, Info CBS Appl: Evaluating package applicability for package Microsoft-Windows-
s-LanguageFeatures-Basic-az-latn-az-Package~31bf3856ad364e35~amd64~~10.0.19041.1, applicable state: Installed
2024-11-27 12:40:42, Info CBS Appl: Evaluating package applicability for package Microsoft-Windows-
s-LanguageFeatures-Basic-as-in-Package~31bf3856ad364e35~amd64~~10.0.19041.1, applicable state: Installed
2024-11-27 12:40:42, Info CBS Appl: Evaluating package applicability for package Microsoft-Windows-
s-LanguageFeatures-Basic-ar-sa-Package~31bf3856ad364e35~amd64~~10.0.19041.1, applicable state: Installed
2024-11-27 12:40:42, Info CBS Appl: Evaluating package applicability for package Microsoft-Windows-
s-LanguageFeatures-Basic-af-za-Package~31bf3856ad364e35~amd64~~10.0.19041.1, applicable state: Installed
2024-11-27 12:42:42, Info CBS Deleting the contents of directory: \\?\C:\Windows\CbsTemp
2024-11-27 12:42:42, Info CBS Deletion of: \\?\C:\Windows\CbsTemp successful

C:\Program Files (x86)\VMware\VMware Player\bin>findstr /I "windows microsoft" C:\Windows\Logs\CBS\CBS.log
```

3. Busca no ficheiro `CBD.log` as liñas que rematen en `Installed` e amosando o número de liña:

```
C:\Program Files (x86)\VMware\VMware Player\bin>findstr /E "Installed" C:\Windows\Logs\CBS\CBS.log
```


4. Busca no ficheiro `dism.log` que comece coa fecha de hoxe e conteña a palabra `failed` (recorda que se pode encadear varios comandos `findstr` coa tubería/*pipe*: |):

```
C:\> Command Prompt for vctl

lToPublic(hr:0x80070057)
2024-06-22 17:02:47, Info          DISM  API: PID=2372 TID=5776 Lookup in table by path failed for: DummyPat
h-2BA51B78-C7F7-4910-B99D-BB7345357CDC - CTransactionalImageTable::LookupImagePath
2024-06-22 17:02:47, Info          DISM  API: PID=2372 TID=5776 Lookup in table by path failed for: DRIVE_C
- CTransactionalImageTable::LookupImagePath
2024-06-22 17:02:47, Info          DISM  DISM Provider Store: PID=2372 TID=5872 Failed to get and initialize
the PE Provider. Continuing by assuming that it is not a WinPE image. - CDISMProviderStore::Final_OnConnect
2024-06-22 17:02:47, Warning       DISM  DISM Provider Store: PID=2372 TID=5872 Failed to load the provider:
C:\Windows\system32\Dism\SiloedPackageProvider.dll. - CDISMProviderStore::Internal_GetProvider(hr:0x8007007e)
2024-06-22 17:02:47, Warning       DISM  DISM Provider Store: PID=2372 TID=5872 Failed to load the provider:
C:\Windows\system32\Dism\MetaDeployProvider.dll. - CDISMProviderStore::Internal_GetProvider(hr:0x8007007e)
2024-06-22 17:02:48, Warning       DISM  DISM Provider Store: PID=5896 TID=5928 Failed to load the provider:
C:\Windows\TEMP\5E7A57CF-048A-47A8-ACF4-A505D0E7775E\PEProvider.dll. - CDISMProviderStore::Internal_GetProvider(hr:0
x8007007e)
2024-06-22 17:02:48, Info          DISM  DISM Provider Store: PID=5896 TID=5928 Failed to get and initialize
the PE Provider. Continuing by assuming that it is not a WinPE image. - CDISMProviderStore::Final_OnConnect
2024-06-22 17:11:31, Info          DISM  API: PID=9880 TID=8020 Lookup in table by path failed for: DummyPat
h-2BA51B78-C7F7-4910-B99D-BB7345357CDC - CTransactionalImageTable::LookupImagePath
2024-06-22 17:11:31, Info          DISM  API: PID=9880 TID=8020 Lookup in table by path failed for: DRIVE_C
- CTransactionalImageTable::LookupImagePath
2024-06-22 17:11:31, Warning       DISM  DISM Provider Store: PID=7976 TID=8948 Failed to load the provider:
C:\Users\ADMINI~1\AppData\Local\Temp\D9EF6AAB-1E87-476C-9CAC-9D13977FBB12\PEProvider.dll. - CDISMProviderStore::Inte
rnal_GetProvider(hr:0x8007007e)
2024-06-22 17:11:31, Info          DISM  DISM Provider Store: PID=7976 TID=8948 Failed to get and initialize
the PE Provider. Continuing by assuming that it is not a WinPE image. - CDISMProviderStore::Final_OnConnect
2024-06-22 17:16:26, Info          DISM  API: PID=9604 TID=9624 Lookup in table by path failed for: DummyPat
h-2BA51B78-C7F7-4910-B99D-BB7345357CDC - CTransactionalImageTable::LookupImagePath
2024-06-22 17:16:26, Info          DISM  API: PID=9604 TID=9624 Lookup in table by path failed for: DRIVE_C
- CTransactionalImageTable::LookupImagePath
2024-06-22 17:16:27, Warning       DISM  DISM Provider Store: PID=8932 TID=9156 Failed to load the provider:
C:\Users\ADMINI~1\AppData\Local\Temp\A64E99EC-8980-4A1F-BDDC-234D34E8C918\PEProvider.dll. - CDISMProviderStore::Inte
rnal_GetProvider(hr:0x8007007e)
2024-06-22 17:16:27, Info          DISM  DISM Provider Store: PID=8932 TID=9156 Failed to get and initialize
the PE Provider. Continuing by assuming that it is not a WinPE image. - CDISMProviderStore::Final_OnConnect
2024-09-06 13:09:43, Info          DISM  API: PID=5328 TID=7824 Lookup in table by path failed for: DummyPat
h-2BA51B78-C7F7-4910-B99D-BB7345357CDC - CTransactionalImageTable::LookupImagePath
2024-09-06 13:09:43, Info          DISM  API: PID=5328 TID=7824 Lookup in table by path failed for: DRIVE_C
- CTransactionalImageTable::LookupImagePath
2024-09-06 13:09:43, Info          DISM  DISM Provider Store: PID=5328 TID=10048 Failed to get and initializ
e the PE Provider. Continuing by assuming that it is not a WinPE image. - CDISMProviderStore::Final_OnConnect
2024-09-06 13:09:43, Warning       DISM  DISM Provider Store: PID=5328 TID=10048 Failed to load the provider
: C:\Windows\system32\Dism\SiloedPackageProvider.dll. - CDISMProviderStore::Internal_GetProvider(hr:0x8007007e)
2024-09-06 13:09:43, Warning       DISM  DISM Provider Store: PID=5328 TID=10048 Failed to load the provider
: C:\Windows\system32\Dism\MetaDeployProvider.dll. - CDISMProviderStore::Internal_GetProvider(hr:0x8007007e)
2024-09-06 13:09:44, Warning       DISM  DISM Provider Store: PID=2948 TID=4360 Failed to load the provider:
C:\Users\joselv\AppData\Local\Temp\A6CA8EB4-B600-4F92-95DD-BCE9461C5724\PEProvider.dll. - CDISMProviderStore::Intern
al_GetProvider(hr:0x8007007e)
2024-09-06 13:09:44, Info          DISM  DISM Provider Store: PID=2948 TID=4360 Failed to get and initialize
the PE Provider. Continuing by assuming that it is not a WinPE image. - CDISMProviderStore::Final_OnConnect
2024-09-06 13:09:44, Error        EnumeratePathEx: FindFirstFile failed for [\\?\C:\$WINDOWS.~Q\*]; G
LE = 0x3[gle=0x00000003]
2024-09-06 13:09:44, Error        EnumeratePathEx: FindFirstFile failed for [\\?\C:\$INPLACE.~TR\*];
GLE = 0x3[gle=0x00000003]
2024-09-06 13:09:44, Error        EnumeratePathEx: FindFirstFile failed for [\\?\C:\$Windows.~LS\*];
GLE = 0x3[gle=0x00000003]
2024-09-06 13:09:44, Error        EnumeratePathEx: FindFirstFile failed for [\\?\C:\ESD\Windows\*]; G
LE = 0x3[gle=0x00000003]
2024-09-06 13:09:44, Error        EnumeratePathEx: FindFirstFile failed for [\\?\C:\$Windows.~WS\*];
GLE = 0x3[gle=0x00000003]
2024-09-06 13:09:44, Error        EnumeratePathEx: FindFirstFile failed for [\\?\C:\ESD\Download\*];
GLE = 0x3[gle=0x00000003]

C:\Program Files (x86)\VMware\VMware Player\bin>findstr /i "%date: failed" C:\Windows\Logs\DISM\dism.log
```

5. Busca a palabra Error en todos os ficheiros con extensión .log do directorio C:\Windows\Logs\:

```
Command Prompt for vctl
C:\Windows\Logs\WinREAgent\setupact.log:2024-06-22 17:11:31, Info [WinREUpdateInstaller.exe]
Exit WinReGetConfig return value: 1, last error: 0x0
C:\Windows\Logs\WinREAgent\setupact.log:2024-06-22 17:11:31, Error 0x80004005 in WinREAgent::E
xecutor::ScheduleExecution (base\diagnosis\srt\winreagent\dll\executor.cpp:252): WinRE is not available[gle=0x0000000
2]
C:\Windows\Logs\WinREAgent\setupact.log:2024-06-22 17:11:31, Error 0x80004005 in WinREAgent::W
inREServicingManager::Schedule (base\diagnosis\srt\winreagent\dll\winreservicingmanager.cpp:436): Failed to schedule
execution[gle=0x0000007a]
C:\Windows\Logs\WinREAgent\setupact.log:2024-06-22 17:11:31, Error 0x80004005 in wmain (base\d
iagnosis\srt\winreagent\tools\winreupdateinstaller\main.cpp:71): [WinREUpdInst] Failed to schedule WinRE image servic
ing operation[gle=0x0000007a]
C:\Windows\Logs\WinREAgent\setupact.log:2024-06-22 17:16:27, Info [WinREUpdateInstaller.exe]
Exit WinReGetConfig return value: 1, last error: 0x0
C:\Windows\Logs\WinREAgent\setupact.log:2024-06-22 17:16:27, Error 0x80004005 in WinREAgent::E
xecutor::ScheduleExecution (base\diagnosis\srt\winreagent\dll\executor.cpp:252): WinRE is not available[gle=0x0000000
2]
C:\Windows\Logs\WinREAgent\setupact.log:2024-06-22 17:16:27, Error 0x80004005 in WinREAgent::W
inREServicingManager::Schedule (base\diagnosis\srt\winreagent\dll\winreservicingmanager.cpp:436): Failed to schedule
execution[gle=0x0000007a]
C:\Windows\Logs\WinREAgent\setupact.log:2024-06-22 17:16:27, Error 0x80004005 in wmain (base\d
iagnosis\srt\winreagent\tools\winreupdateinstaller\main.cpp:71): [WinREUpdInst] Failed to schedule WinRE image servic
ing operation[gle=0x0000007a]
C:\Windows\Logs\WinREAgent\setuperr.log:2024-06-01 12:48:02, Error 0x80070003 in PbrDeleteD
irectory (base\reset\util\src\filesystem.cpp:2948): Failed to delete directory [\\?\C:\$WinREAgent\Scratch][gle=0x000
00003]
C:\Windows\Logs\WinREAgent\setuperr.log:2024-06-01 12:48:02, Error 0x80070003 in PushButtonRes
et::Directory::Delete (base\reset\util\src\filesystem.cpp:2981): Failed to recursively delete [C:\$WinREAgent\Scratch
][gle=0x00000003]
C:\Windows\Logs\WinREAgent\setuperr.log:2024-06-01 12:48:02, Error 0x80070003 in WinREAgent::W
inREServicingManager::GetInstalledWinREVersion (base\diagnosis\srt\winreagent\dll\winreservicingmanager.cpp:178): Fai
led to get image info[gle=0x0000007a]
C:\Windows\Logs\WinREAgent\setuperr.log:2024-06-01 12:51:14, Error 0x80004005 in WinREAgent::E
xecutor::ScheduleExecution (base\diagnosis\srt\winreagent\dll\executor.cpp:252): WinRE is not available[gle=0x0000000
2]
C:\Windows\Logs\WinREAgent\setuperr.log:2024-06-01 12:51:14, Error 0x80004005 in WinREAgent::W
inREServicingManager::Schedule (base\diagnosis\srt\winreagent\dll\winreservicingmanager.cpp:436): Failed to schedule
execution[gle=0x0000007a]
C:\Windows\Logs\WinREAgent\setuperr.log:2024-06-01 12:51:14, Error 0x80004005 in wmain (base\d
iagnosis\srt\winreagent\tools\winreupdateinstaller\main.cpp:71): [WinREUpdInst] Failed to schedule WinRE image servic
ing operation[gle=0x0000007a]
C:\Windows\Logs\WinREAgent\setuperr.log:2024-06-01 12:51:43, Error 0x80070003 in WinREAgent::W
inREServicingManager::GetInstalledWinREVersion (base\diagnosis\srt\winreagent\dll\winreservicingmanager.cpp:178): Fai
led to get image info[gle=0x0000007a]
C:\Windows\Logs\WinREAgent\setuperr.log:2024-06-22 17:11:31, Error 0x80004005 in WinREAgent::E
xecutor::ScheduleExecution (base\diagnosis\srt\winreagent\dll\executor.cpp:252): WinRE is not available[gle=0x0000000
2]
C:\Windows\Logs\WinREAgent\setuperr.log:2024-06-22 17:11:31, Error 0x80004005 in WinREAgent::W
inREServicingManager::Schedule (base\diagnosis\srt\winreagent\dll\winreservicingmanager.cpp:436): Failed to schedule
execution[gle=0x0000007a]
C:\Windows\Logs\WinREAgent\setuperr.log:2024-06-22 17:11:31, Error 0x80004005 in wmain (base\d
iagnosis\srt\winreagent\tools\winreupdateinstaller\main.cpp:71): [WinREUpdInst] Failed to schedule WinRE image servic
ing operation[gle=0x0000007a]
C:\Windows\Logs\WinREAgent\setuperr.log:2024-06-22 17:16:27, Error 0x80004005 in WinREAgent::E
xecutor::ScheduleExecution (base\diagnosis\srt\winreagent\dll\executor.cpp:252): WinRE is not available[gle=0x0000000
2]
C:\Windows\Logs\WinREAgent\setuperr.log:2024-06-22 17:16:27, Error 0x80004005 in WinREAgent::W
inREServicingManager::Schedule (base\diagnosis\srt\winreagent\dll\winreservicingmanager.cpp:436): Failed to schedule
execution[gle=0x0000007a]
C:\Windows\Logs\WinREAgent\setuperr.log:2024-06-22 17:16:27, Error 0x80004005 in wmain (base\d
iagnosis\srt\winreagent\tools\winreupdateinstaller\main.cpp:71): [WinREUpdInst] Failed to schedule WinRE image servic
ing operation[gle=0x0000007a]
C:\>findstr /S /I "Error" C:\Windows\Logs\*.log
```


6. Repite a busca anterior pero limitando a liñas con data de hoxe e garadando o resultado nun ficheiro chamado erros-de-hoxe.txt:

```
findstr /s /i "%date% Error" C:\Windows\Logs\*.log > C:\Windows\Logs\erros-de-hoxe.txt
```

```
C:\Windows\Logs\DISM\dism.log:2024-10-15 08:38:00, Error EnumeratePathEx: FindFirstFile failed for [\\
?C:\$INPLACE.~TR\*]; GLE = 0x3[gle=0x00000003]
C:\Windows\Logs\DISM\dism.log:2024-10-15 08:38:00, Error EnumeratePathEx: FindFirstFile failed for [\\
?C:\$WINDOWS.~LS\*]; GLE = 0x3[gle=0x00000003]
C:\Windows\Logs\DISM\dism.log:2024-10-15 08:38:00, Error EnumeratePathEx: FindFirstFile failed for [\\
?C:\$ESD\Windows\*]; GLE = 0x3[gle=0x00000003]
C:\Windows\Logs\DISM\dism.log:2024-10-15 08:38:00, Error EnumeratePathEx: FindFirstFile failed for [\\
?C:\$WINDOWS.~WS\*]; GLE = 0x3[gle=0x00000003]
C:\Windows\Logs\DISM\dism.log:2024-10-15 08:38:00, Error EnumeratePathEx: FindFirstFile failed for [\\
?C:\$ESD\Download\*]; GLE = 0x3[gle=0x00000003]
C:\Windows\Logs\DISM\dism.log:2024-10-16 14:40:34, Error EnumeratePathEx: FindFirstFile failed for [\\
?C:\$WINDOWS.~Q\*]; GLE = 0x3[gle=0x00000003]
C:\Windows\Logs\DISM\dism.log:2024-10-16 14:40:34, Error EnumeratePathEx: FindFirstFile failed for [\\
?C:\$INPLACE.~TR\*]; GLE = 0x3[gle=0x00000003]
C:\Windows\Logs\DISM\dism.log:2024-10-16 14:40:34, Error EnumeratePathEx: FindFirstFile failed for [\\
?C:\$WINDOWS.~LS\*]; GLE = 0x3[gle=0x00000003]
C:\Windows\Logs\DISM\dism.log:2024-10-16 14:40:34, Error EnumeratePathEx: FindFirstFile failed for [\\
?C:\$ESD\Windows\*]; GLE = 0x3[gle=0x00000003]
C:\Windows\Logs\DISM\dism.log:2024-10-16 14:40:34, Error EnumeratePathEx: FindFirstFile failed for [\\
?C:\$WINDOWS.~WS\*]; GLE = 0x3[gle=0x00000003]
C:\Windows\Logs\DISM\dism.log:2024-10-16 14:40:34, Error EnumeratePathEx: FindFirstFile failed for [\\
?C:\$ESD\Download\*]; GLE = 0x3[gle=0x00000003]
C:\Windows\Logs\DISM\dism.log:2024-10-17 12:07:09, Error EnumeratePathEx: FindFirstFile failed for [\\
?C:\$WINDOWS.~Q\*]; GLE = 0x3[gle=0x00000003]
C:\Windows\Logs\DISM\dism.log:2024-10-17 12:07:09, Error EnumeratePathEx: FindFirstFile failed for [\\
?C:\$INPLACE.~TR\*]; GLE = 0x3[gle=0x00000003]
C:\Windows\Logs\DISM\dism.log:2024-10-17 12:07:09, Error EnumeratePathEx: FindFirstFile failed for [\\
?C:\$WINDOWS.~LS\*]; GLE = 0x3[gle=0x00000003]
C:\Windows\Logs\DISM\dism.log:2024-10-17 12:07:09, Error EnumeratePathEx: FindFirstFile failed for [\\
?C:\$ESD\Windows\*]; GLE = 0x3[gle=0x00000003]
C:\Windows\Logs\DISM\dism.log:2024-10-17 12:07:09, Error EnumeratePathEx: FindFirstFile failed for [\\
?C:\$WINDOWS.~WS\*]; GLE = 0x3[gle=0x00000003]
C:\Windows\Logs\DISM\dism.log:2024-10-17 12:07:09, Error EnumeratePathEx: FindFirstFile failed for [\\
?C:\$ESD\Download\*]; GLE = 0x3[gle=0x00000003]
C:\Windows\Logs\DISM\dism.log:2024-11-28 12:35:04, Error EnumeratePathEx: FindFirstFile failed for [\\
?C:\$WINDOWS.~Q\*]; GLE = 0x3[gle=0x00000003]
C:\Windows\Logs\DISM\dism.log:2024-11-28 12:35:04, Error EnumeratePathEx: FindFirstFile failed for [\\
?C:\$INPLACE.~TR\*]; GLE = 0x3[gle=0x00000003]
C:\Windows\Logs\DISM\dism.log:2024-11-28 12:35:04, Error EnumeratePathEx: FindFirstFile failed for [\\
?C:\$WINDOWS.~LS\*]; GLE = 0x3[gle=0x00000003]
C:\Windows\Logs\DISM\dism.log:2024-11-28 12:35:04, Error EnumeratePathEx: FindFirstFile failed for [\\
?C:\$ESD\Windows\*]; GLE = 0x3[gle=0x00000003]
C:\Windows\Logs\DISM\dism.log:2024-11-28 12:35:04, Error EnumeratePathEx: FindFirstFile failed for [\\
?C:\$WINDOWS.~WS\*]; GLE = 0x3[gle=0x00000003]
C:\Windows\Logs\DISM\dism.log:2024-11-28 12:35:04, Error EnumeratePathEx: FindFirstFile failed for [\\
?C:\$ESD\Download\*]; GLE = 0x3[gle=0x00000003]
C:\Windows\Logs\DISM\dism.log:2024-12-05 11:58:02, Error EnumeratePathEx: FindFirstFile failed for [\\
?C:\$WINDOWS.~Q\*]; GLE = 0x3[gle=0x00000003]
C:\Windows\Logs\DISM\dism.log:2024-12-05 11:58:02, Error EnumeratePathEx: FindFirstFile failed for [\\
?C:\$INPLACE.~TR\*]; GLE = 0x3[gle=0x00000003]
C:\Windows\Logs\DISM\dism.log:2024-12-05 11:58:02, Error EnumeratePathEx: FindFirstFile failed for [\\
?C:\$WINDOWS.~LS\*]; GLE = 0x3[gle=0x00000003]
C:\Windows\Logs\DISM\dism.log:2024-12-05 11:58:02, Error EnumeratePathEx: FindFirstFile failed for [\\
?C:\$ESD\Windows\*]; GLE = 0x3[gle=0x00000003]
C:\Windows\Logs\DISM\dism.log:2024-12-05 11:58:02, Error EnumeratePathEx: FindFirstFile failed for [\\
?C:\$WINDOWS.~WS\*]; GLE = 0x3[gle=0x00000003]
C:\Windows\Logs\DISM\dism.log:2024-12-05 11:58:02, Error EnumeratePathEx: FindFirstFile failed for [\\
?C:\$ESD\Download\*]; GLE = 0x3[gle=0x00000003]
PS C:\Users\Administrador> type C:\Windows\Logs\erros-de-hoxe.txt
```

Agora, emprgando o comando Get-Eventlog, trata de resolver os seguintes enunciados:

7. Obter a lista de rexistros de eventos dispoñibles en la equipo local:

```
Get-Eventlog -List
```

```
PS C:\Users\Administrador> Get-Eventlog -List
```

Max(K)	Retain	OverflowAction	Entries	Log
512	7	OverwriteOlder	9	Active Directory Web Services
20.480	0	OverwriteAsNeeded	1.172	Application
15.168	0	OverwriteAsNeeded	17	DFS Replication
512	0	OverwriteAsNeeded	84	Directory Service
102.400	0	OverwriteAsNeeded	30	DNS Server
20.480	0	OverwriteAsNeeded	0	HardwareEvents
512	7	OverwriteOlder	0	Internet Explorer
20.480	0	OverwriteAsNeeded	0	Key Management Service
131.072	0	OverwriteAsNeeded	18.422	Security
20.480	0	OverwriteAsNeeded	2.114	System
15.360	0	OverwriteAsNeeded	290	Windows PowerShell

8. Obter o rexistro de sistema:

Get-Eventlog -Logname System

```
PS C:\Users\Administrador> Get-EventLog -Logname System
```

Index	Time	EntryType	Source	InstanceID	Message
2667	dic. 05 12:22	Information	Service Control M...	1073748860	El servicio Servicio de implementación de AppX (AppX...
2666	dic. 05 12:22	Information	Service Control M...	1073748860	El servicio Microsoft Edge Update Service (edgeupdat...
2665	dic. 05 12:21	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2664	dic. 05 12:21	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2663	dic. 05 12:19	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2662	dic. 05 12:19	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2661	dic. 05 12:18	Information	Service Control M...	1073748860	El servicio Servicio de Windows Update Medic entró e...
2660	dic. 05 12:18	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2659	dic. 05 12:18	Warning	Microsoft-Windows...	1014	No se encontró la descripción del id. de evento '101...
2658	dic. 05 12:18	Warning	Microsoft-Windows...	1014	No se encontró la descripción del id. de evento '101...
2657	dic. 05 12:18	Information	Service Control M...	1073748860	El servicio Aplicación auxiliar de NetBIOS sobre TCP...
2656	dic. 05 12:18	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2655	dic. 05 12:17	Information	Service Control M...	1073748860	El servicio Optimización de distribución entró en es...
2654	dic. 05 12:17	Information	Service Control M...	1073748860	El servicio Servicio de Windows Update Medic entró e...
2653	dic. 05 12:17	Information	Service Control M...	1073748860	El servicio Aplicación auxiliar de NetBIOS sobre TCP...
2652	dic. 05 12:17	Information	Service Control M...	1073748866	Se envió un control "detener" correctamente al servi...
2651	dic. 05 12:17	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2650	dic. 05 12:17	Information	Service Control M...	1073748860	El servicio Servicio de configuración de red entró e...
2649	dic. 05 12:17	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2648	dic. 05 12:17	Information	Service Control M...	1073748860	El servicio Servicio FrameServer de la Cámara de Win...
2647	dic. 05 12:17	Information	Service Control M...	1073748860	El servicio Monitor del servidor de marco de la Cáma...
2646	dic. 05 12:16	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2645	dic. 05 12:16	Information	Service Control M...	1073748860	El servicio Servicio FrameServer de la Cámara de Win...
2644	dic. 05 12:16	Information	Service Control M...	1073748860	El servicio Monitor del servidor de marco de la Cáma...
2643	dic. 05 12:16	Information	Microsoft-Windows...	566	No se encontró la descripción del id. de evento '566...
2642	dic. 05 12:16	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2641	dic. 05 12:14	Information	Service Control M...	1073748860	El servicio Servicio de inspección de red de Antivir...
2640	dic. 05 12:14	Information	Microsoft-Windows...	6	Filtro de sistema de archivos 'WdFilter' (10.0, 2072...
2639	dic. 05 12:14	Information	Service Control M...	1073748860	El servicio Servicio Antivirus de Microsoft Defender...
2638	dic. 05 12:14	Information	Service Control M...	1073748860	El servicio Servicio Antivirus de Microsoft Defender...
2637	dic. 05 12:14	Information	Service Control M...	1073748860	El servicio Servicio Antivirus de Microsoft Defender...
2636	dic. 05 12:14	Information	Microsoft-Windows...	1	Filtro de sistema de archivos 'WdFilter' (Versión 10...
2635	dic. 05 12:14	Information	Service Control M...	1073748860	El servicio Servicio Antivirus de Microsoft Defender...
2634	dic. 05 12:14	Information	Service Control M...	1073748860	El servicio Servicio de inspección de red de Antivir...
2633	dic. 05 12:14	Information	Service Control M...	1073748860	El servicio Servicio de inspección de red de Antivir...
2632	dic. 05 12:14	Information	Service Control M...	1073748860	El servicio Servicio de configuración de red entró e...
2631	dic. 05 12:14	Information	Service Control M...	1073748860	El servicio Servicio de inspección de red de Antivir...
2630	dic. 05 12:13	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2629	dic. 05 12:13	Information	Microsoft-Windows...	16	No se encontró la descripción del id. de evento '16'...
2628	dic. 05 12:13	Information	Service Control M...	1073748860	El servicio Servicio de implementación de AppX (AppX...
2627	dic. 05 12:12	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2626	dic. 05 12:11	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2625	dic. 05 12:11	Information	Microsoft-Windows...	566	No se encontró la descripción del id. de evento '566...
2624	dic. 05 12:11	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2623	dic. 05 12:09	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2622	dic. 05 12:09	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2621	dic. 05 12:07	Information	Service Control M...	1073748860	El servicio Optimización de distribución entró en es...
2620	dic. 05 12:07	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2619	dic. 05 12:07	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2618	dic. 05 12:05	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2617	dic. 05 12:05	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2616	dic. 05 12:03	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2615	dic. 05 12:03	Information	Service Control M...	1073748860	El servicio Servicio de implementación de AppX (AppX...

9. Repite a consulta anterior pero soamente amosando as 10 entradas máis recentes do rexistro do sistema:

Get-Eventlog -Logname System -Newest 10

```
PS C:\Users\Administrador> Get-EventLog -Logname System -Newest 10
```

Index	Time	EntryType	Source	InstanceID	Message
2671	dic. 05 12:23	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2670	dic. 05 12:23	Information	Service Control M...	1073748860	El servicio Servicio de licencia de cliente (ClipSVC...
2669	dic. 05 12:23	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2668	dic. 05 12:22	Information	Service Control M...	1073748860	El servicio Optimización de distribución entró en es...
2667	dic. 05 12:22	Information	Service Control M...	1073748860	El servicio Servicio de implementación de AppX (AppX...
2666	dic. 05 12:22	Information	Service Control M...	1073748860	El servicio Microsoft Edge Update Service (edgeupdat...
2665	dic. 05 12:21	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2664	dic. 05 12:21	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2663	dic. 05 12:19	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2662	dic. 05 12:19	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...

10. Obter o rexistro do sistema dun día en concreto, por exemplo, do mércores da semana anterior (se non houbera rexistros dese día, escoller outro):

```
Get-Eventlog -Logname System -After "2024-11-27 00:00:00" -Before "2024-11-28 00:00:00"
```

```
PS C:\Users\Administrador> Get-Eventlog -Logname System -After "2024-11-27 00:00:00" -Before "2024-11-28 00:00:00"
```

Index	Time	EntryType	Source	InstanceID	Message
2412	nov. 27 14:33	Information	Service Control M...	1073748860	El servicio Windows Update entró en estado "en ejecu...
2410	nov. 27 14:33	Information	Service Control M...	1073748860	El servicio Servicio de licencia de cliente (ClipSVC...
2409	nov. 27 14:33	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2408	nov. 27 14:33	Information	Service Control M...	1073748860	El servicio Aplicación auxiliar de NetBIOS sobre TCP...
2407	nov. 27 14:33	Information	Service Control M...	1073748860	El servicio Aplicación auxiliar de NetBIOS sobre TCP...
2406	nov. 27 14:33	Information	Service Control M...	1073748866	Se envió un control "detener" correctamente al servi...
2405	nov. 27 14:33	Information	Service Control M...	1073748860	El servicio Servicio de implementación de AppX (AppX...
2404	nov. 27 14:33	Information	Service Control M...	1073748860	El servicio Monitor del servidor de marco de la Cáma...
2403	nov. 27 14:33	Information	Service Control M...	1073748860	El servicio Servicio FrameServer de la Cámara de Win...
2402	nov. 27 14:33	Information	Microsoft-Windows...	566	No se encontró la descripción del id. de evento '566...
2401	nov. 27 14:30	Information	Service Control M...	1073748860	El servicio Ayudante para el inicio de sesión de cue...
2400	nov. 27 14:29	Information	Service Control M...	1073748860	El servicio Servicio de licencia de cliente (ClipSVC...
2399	nov. 27 14:24	Information	Service Control M...	1073748860	El servicio Servicio de licencia de cliente (ClipSVC...
2398	nov. 27 14:24	Information	Service Control M...	1073748860	El servicio Ayudante para el inicio de sesión de cue...
2397	nov. 27 14:17	Information	Service Control M...	1073748860	El servicio Servicio de implementación de AppX (AppX...
2396	nov. 27 14:15	Information	Service Control M...	1073748860	El servicio Ayudante para el inicio de sesión de cue...
2395	nov. 27 14:14	Information	Service Control M...	1073748860	El servicio Servicio de licencia de cliente (ClipSVC...
2394	nov. 27 14:14	Information	Service Control M...	1073748860	El servicio Servicio de transferencia inteligente en...
2393	nov. 27 14:14	Information	Service Control M...	1073748864	El tipo de inicio del servicio Servicio de transfere...
2392	nov. 27 14:12	Information	Service Control M...	1073748860	El servicio Servicio de implementación de AppX (AppX...
2391	nov. 27 14:12	Information	Service Control M...	1073748860	El servicio Servicio de transferencia inteligente en...
2390	nov. 27 14:12	Information	Service Control M...	1073748864	El tipo de inicio del servicio Servicio de transfere...
2389	nov. 27 14:10	Information	Service Control M...	1073748860	El servicio Servicio Informe de errores de Windows e...
2388	nov. 27 14:08	Information	Service Control M...	1073748860	El servicio Servicio Informe de errores de Windows e...
2387	nov. 27 14:03	Information	Service Control M...	1073748860	El servicio Servicio Informe de errores de Windows e...
2386	nov. 27 14:02	Information	Service Control M...	1073748860	El servicio Windows Update entró en estado "detenido".
2385	nov. 27 14:01	Information	Service Control M...	1073748860	El servicio Servicio de licencia de cliente (ClipSVC...
2384	nov. 27 14:01	Information	Service Control M...	1073748860	El servicio Ayudante para el inicio de sesión de cue...
2383	nov. 27 14:01	Information	Service Control M...	1073748860	El servicio Servicio Informe de errores de Windows e...
2382	nov. 27 14:00	Information	Service Control M...	1073748860	El servicio Ayudante para el inicio de sesión de cue...
2381	nov. 27 13:59	Information	LsaSrv	6148	El PDC completó una operación de examen de confianza...
2380	nov. 27 13:59	Information	Service Control M...	1073748860	El servicio Servicio de licencia de cliente (ClipSVC...
2379	nov. 27 13:57	Information	Service Control M...	1073748860	El servicio Servicio de configuración de red entró e...
2378	nov. 27 13:54	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2377	nov. 27 13:54	Information	Microsoft-Windows...	566	No se encontró la descripción del id. de evento '566...
2376	nov. 27 13:54	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2375	nov. 27 13:54	Information	Service Control M...	1073748860	El servicio Servicio de licencia de cliente (ClipSVC...
2374	nov. 27 13:54	Information	Service Control M...	1073748860	El servicio Ayudante para el inicio de sesión de cue...
2373	nov. 27 13:52	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2372	nov. 27 13:52	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2371	nov. 27 13:51	Information	Service Control M...	1073748860	El servicio Ayudante para el inicio de sesión de cue...
2370	nov. 27 13:50	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2369	nov. 27 13:50	Information	Service Control M...	1073748860	El servicio Servicio de licencia de cliente (ClipSVC...
2368	nov. 27 13:50	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2367	nov. 27 13:48	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2366	nov. 27 13:48	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2365	nov. 27 13:46	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2364	nov. 27 13:46	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2363	nov. 27 13:44	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2362	nov. 27 13:44	Information	Service Control M...	1073748860	El servicio Servicio Informe de errores de Windows e...
2361	nov. 27 13:44	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...
2360	nov. 27 13:43	Information	Service Control M...	1073748860	El servicio Servicio de Windows Update Medic entró e...
2359	nov. 27 13:42	Information	Service Control M...	1073748860	El servicio Protección de software entró en estado "...

11. Obter as 20 entradas máis recente do rexistro de sistema de tipo erro:

```
Get-Eventlog -Logname System -EntryType Error -Newest 20
```

12. Repite o a consulta anterior pero na que o tipo sexa de aviso:

```
Get-Eventlog -Logname System -EntryType Warning -Newest 20
```

```
PS C:\Users\Administrador> Get-Eventlog -Logname System -EntryType Error -Newest 20
```

Index	Time	EntryType	Source	InstanceID	Message
2012	oct. 15 08:37	Error	NETLOGON	5774	Error en el registro dinámico del registro DNS '_ker...
2011	oct. 15 08:37	Error	NETLOGON	5774	Error en el registro dinámico del registro DNS '_ker...
2010	oct. 15 08:37	Error	NETLOGON	5774	Error en el registro dinámico del registro DNS '_lda...
2009	oct. 15 08:37	Error	NETLOGON	5774	Error en el registro dinámico del registro DNS '_lda...
2008	oct. 15 08:37	Error	NETLOGON	5774	Error en el registro dinámico del registro DNS '_ker...
2007	oct. 15 08:37	Error	NETLOGON	5774	Error en el registro dinámico del registro DNS '_ker...
2006	oct. 15 08:37	Error	NETLOGON	5774	Error en el registro dinámico del registro DNS 'eac0...
2005	oct. 15 08:37	Error	NETLOGON	5774	Error en el registro dinámico del registro DNS '_lda...
2004	oct. 15 08:37	Error	NETLOGON	5774	Error en el registro dinámico del registro DNS '_lda...
2003	oct. 15 08:37	Error	NETLOGON	5774	Error en el registro dinámico del registro DNS '_lda...
2002	oct. 15 08:37	Error	NETLOGON	5774	Error en el registro dinámico del registro DNS '_lda...
2001	oct. 15 08:37	Error	NETLOGON	5774	Error en el registro dinámico del registro DNS '_lda...
2000	oct. 15 08:37	Error	NETLOGON	5774	Error en el registro dinámico del registro DNS '_lda...
1834	oct. 09 13:36	Error	RemoteAccess	20063	El Administrador de conexiones de acceso remoto no s...
1833	oct. 09 13:36	Error	RemoteAccess	20063	El Administrador de conexiones de acceso remoto no s...
1705	oct. 01 09:39	Error	NETLOGON	5775	Error en la eliminación dinámica del registro DNS 'F...
1704	oct. 01 09:39	Error	NETLOGON	5775	Error en la eliminación dinámica del registro DNS 'g...
1703	oct. 01 09:39	Error	NETLOGON	5775	Error en la eliminación dinámica del registro DNS 'r...
1702	oct. 01 09:39	Error	NETLOGON	5775	Error en la eliminación dinámica del registro DNS 'D...
1701	oct. 01 09:39	Error	NETLOGON	5774	Error en el registro dinámico del registro DNS '_lda...

13. Obter todas ls entradas do rexistro de sistema relacionadas co disco:

```
Get-Eventlog -Logname System | Where-Object ( $_.Message -like "disk*" )
```

```
PS C:\Users\Administrador> Get-Eventlog -Logname System | Where-Object ( $_.Message -like "*disk*" )
```

14. Obter as últimas 100 entradas do rexistro do sistema que conteñan na mensaxe a palabra update:

```
Get-Eventlog -Logname System -Newest 100 | Where-Object ( $_.Message -like "*update*" )
```

```
PS C:\Users\Administrador> Get-Eventlog -Logname System -Newest 100 | Where-Object ( $_.Message -like "*update*" )
PS C:\Users\Administrador> |
```

15. Obter as últimas 10 entradas do rexistro de Aplicacións cuxa fonte sexa "Desktop Window Manager"

```
Get-Eventlog -Logname Application -Source "Desktop Window Manager" -Newest 10
```

```
PS C:\Users\Administrador> Get-Eventlog -Logname Application -Source "Desktop Window Manager" -Newest 10
```

Index	Time	EntryType	Source	InstanceID	Message
195	sep. 19 02:21	Information	Desktop Window Ma...	1073750851	El Administrador de ventanas de escritorio registró ...
149	sep. 19 01:54	Information	Desktop Window Ma...	1073750851	El Administrador de ventanas de escritorio registró ...

```
PS C:\Users\Administrador> |
```

16. Pega unha captura de pantalla do BPA do Windows Server que teñas instalado:

3.2. GNU/Linux

Emprega os comandos necesarios en GNU/Linux para obter a información que se solicita:

1. Consulta a axuda sobre o comando de grep e egrep:


```
GREP(1)                                User Commands                                GREP(1)

NAME
    grep, egrep, fgrep, rgrep - print lines that match patterns

SYNOPSIS
    grep [OPTION...] PATTERNS [FILE...]
    grep [OPTION...] -e PATTERNS ... [FILE...]
    grep [OPTION...] -f PATTERN_FILE ... [FILE...]

DESCRIPTION
    grep searches for PATTERNS in each FILE. PATTERNS is one or more patterns
    separated by newline characters, and grep prints each line that matches a
    pattern. Typically PATTERNS should be quoted when grep is used in a shell
    command.

    A FILE of "-" stands for standard input. If no FILE is given, recursive
    searches examine the working directory, and nonrecursive searches read
    standard input.

    Debian also includes the variant programs egrep, fgrep and rgrep. These
    programs are the same as grep -E, grep -F, and grep -r, respectively. These
    variants are deprecated upstream, but Debian provides for backward
    compatibility. For portability reasons, it is recommended to avoid the
    variant programs, and use grep with the related option instead.

OPTIONS
    Generic Program Information
        --help Output a usage message and exit.

        -V, --version
            Output the version number of grep and exit.

    Pattern Syntax
        -E, --extended-regexp
            Interpret PATTERNS as extended regular expressions (EREs, see below).

Manual page grep(1) line 1 (press h for help or q to quit)
```

2. Busca no ficheiro syslog as liñas que teñan a palabra linux sen ter en conta maiúsculas nin minúsculas:

```
eu@rubenrf:~$ grep -i "linux" /var/log/syslog
eu@rubenrf:~$
```

3. Busca no ficheiro syslog as liñas que teñan a palabra linux ou gnu sen ter en conta maiúsculas nin minúsculas e amosando o número de liña:

```
eu@rubenrf:~$ grep -i -n -E "linux|gnu" /var/log/syslog
```

4. Busca no ficheiro syslog as liñas que rematen en co UID do teu usuario amosando o número de liña:

```
eu@rubenrf:~$ grep -n "1000$" /var/log/syslog
eu@rubenrf:~$
```

5. Busca no ficheiro authlog que comece coa fecha de hoxe e conteña do usuario co que te autenticaches:

```
eu@rubenrf:~$ grep "^2024-12-09.*root" /var/log/auth.log
2024-12-09T09:15:01.348461+01:00 rubenrf CRON[10106]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2024-12-09T09:15:01.362692+01:00 rubenrf CRON[10106]: pam_unix(cron:session): session closed for user root
2024-12-09T09:17:01.378735+01:00 rubenrf CRON[10145]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2024-12-09T09:17:01.382645+01:00 rubenrf CRON[10145]: pam_unix(cron:session): session closed for user root
eu@rubenrf:~$
```

6. Busca a palabra error en todos os ficheiros que teñan como parte do nome “log” do directorio /var/log/:

```

eu@rubenrf:~$ grep -i "error" /var/log/*log
grep: /var/log/boot.log: Permiso denegado
/var/log/bootstrap.log:2024-08-27 15:37:06 URL:http://ftpmaster.internal/ubuntu/pool/main/libg/libgpg-error/libgpg-error0_1.47-3build2_amd64.deb [69990/69990] -> "/build/chroot//var/cache/apt/archives/partial/libgpg-error0_1.47-3build2_amd64.deb" [1]
/var/log/bootstrap.log:Selecting previously unselected package libgpg-error0:amd64.
/var/log/bootstrap.log:Preparing to unpack ../libgpg-error0_1.47-3build2_amd64.deb ...
/var/log/bootstrap.log:Unpacking libgpg-error0:amd64 (1.47-3build2) ...
/var/log/bootstrap.log:Setting up libgpg-error0:amd64 (1.47-3build2) ...
/var/log/syslog:2024-12-05T08:31:00.716721+01:00 rubenrf org.freedesktop.FileManager1[7204]: MESA: error: ZINK: failed to choose pdev
/var/log/syslog:2024-12-05T13:05:35.078483+01:00 rubenrf org.freedesktop.FileManager1[7204]: MESA: error: ZINK: failed to choose pdev
/var/log/syslog:2024-12-05T13:05:36.393613+01:00 rubenrf org.gnome.ArchiveManager1[7365]: MESA: error: ZINK: failed to choose pdev
/var/log/syslog:2024-12-05T13:05:36.707840+01:00 rubenrf org.gnome.ArchiveManager1[7365]: MESA: error: ZINK: failed to choose pdev
/var/log/syslog:2024-12-05T13:07:43.636083+01:00 rubenrf tracker-miner-fs-3[7461]: (tracker-extract-3:7461): GLib-GIO-WARNING **: 13:07:43.635: Error creating IO channel for /proc/self/mountinfo: Parámetro incorrecto (g-io-error-quark, 13)
/var/log/syslog:2024-12-05T13:07:58.775046+01:00 rubenrf tracker-miner-fs-3[7480]: (tracker-extract-3:7480): GLib-GIO-WARNING **: 13:07:58.772: Error creating IO channel for /proc/self/mountinfo: Parámetro incorrecto (g-io-error-quark, 13)
/var/log/syslog:2024-12-05T13:47:01.702415+01:00 rubenrf update-notifier.desktop[8978]: WARNING:root:Error loading .desktop file /usr/share/ubuntu/applications/texdoctk.desktop: constructor returned NULL
/var/log/syslog:2024-12-09T09:14:59.390085+01:00 rubenrf tracker-miner-fs-3[10098]: (tracker-extract-3:10098): GLib-GIO-WARNING **: 09:14:59.389: Error creating IO channel for /proc/self/mountinfo: Parámetro incorrecto (g-io-error-quark, 13)
grep: /var/log/vboxadd-install.log: Permiso denegado
grep: /var/log/vboxadd-uninstall.log: Permiso denegado
eu@rubenrf:~$

```

7. Repite a busca anterior pero limitando a liñas con data de hoxe e garadando o resultado nun ficheiro chamado erros-de-hoxe.txt:


```
eu@rubenrf:~$ grep -i "error" /var/log/*log > erros-de-hoxe.txt
```

8. Amosa as mensaxes durante o inicio do SO:

```
next_to_watch      <0>
jiffies            <100ccd6c0>
next_to_watch.status <0>
[13725.353619] 08:13:31.157151 timesync vgsvcTimeSyncWorker: Radical host time change:
328 763 478 000 000ns (HostNow=1 733 732 011 157 000 000 ns HostLast=1 733 403 247 679
000 000 ns)
[13725.538647] audit: type=1400 audit(1733732011.344:178): apparmor="DENIED" operation=
"capable" class="cap" profile="/usr/lib/snapd/snap-confine" pid=9670 comm="snap-confine"
" capability=12 capname="net_admin"
[13725.560264] audit: type=1400 audit(1733732011.365:179): apparmor="DENIED" operation=
"open" class="file" profile="snap-update-ns.firmware-updater" name="/proc/9699/maps" pi
d=9699 comm="5" requested_mask="r" denied_mask="r" fsuid=1000 ouid=0
[13726.221862] audit: type=1400 audit(1733732012.027:180): apparmor="DENIED" operation=
"open" class="file" profile="snap.firmware-updater.firmware-notifier" name="/proc/sys/v
m/max_map_count" pid=9670 comm="firmware-notifi" requested_mask="r" denied_mask="r" fsu
id=1000 ouid=0
[13726.231520] e1000 0000:00:03.0 enp0s3: Detected Tx Unit Hang
Tx Queue          <0>
TDH                <0>
TDT                <1>
next_to_use        <1>
next_to_clean      <0>
buffer_info[next_to_clean]
time_stamp         <100ccc780>
next_to_watch      <0>
jiffies            <100ccdec0>
next_to_watch.status <0>
[13726.831289] audit: type=1400 audit(1733732012.637:181): apparmor="DENIED" operation=
"capable" class="cap" profile="/usr/sbin/cupsd" pid=9924 comm="cupsd" capability=12 ca
pname="net_admin"
[13727.575681] e1000 0000:00:03.0 enp0s3: NETDEV WATCHDOG: CPU: 0: transmit queue 0 tim
ed out 5434 ms
[13727.575745] e1000 0000:00:03.0 enp0s3: Reset adapter
[13729.686046] e1000: enp0s3 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: RX
[13735.354131] 08:13:41.165459 timesync vgsvcTimeSyncWorker: Radical guest time change:
328 754 939 606 000ns (GuestNow=1 733 732 021 165 446 000 ns GuestLast=1 733 403 266 2
25 840 000 ns fSetTimeLastLoop=true)
eu@rubenrf:~$ sudo dmesg
```

9. Amosa as últimas 10 liñas do ficheiro de log syslog de forma que se manteña a escoita por se se engade outra liña:

```

eu@rubenrf:~$ tail -f /var/log/syslog
2024-12-09T09:24:09.445106+01:00 rubenrf tracker-miner-fs-3[10248]: (tracker-extract-3:
10248): GLib-GIO-WARNING **: 09:24:09.443: Error creating IO channel for /proc/self/mou
ntinfo: Parámetro incorrecto (g-io-error-quark, 13)
2024-12-09T09:24:23.766023+01:00 rubenrf tracker-miner-fs-3[10267]: (tracker-extract-3:
10267): GLib-GIO-WARNING **: 09:24:23.765: Error creating IO channel for /proc/self/mou
ntinfo: Parámetro incorrecto (g-io-error-quark, 13)
2024-12-09T09:24:51.019898+01:00 rubenrf NetworkManager[964]: <info> [1733732691.0178]
dhcp4 (enp0s3): state changed new lease, address=192.168.56.103
2024-12-09T09:24:51.026732+01:00 rubenrf dbus-daemon[878]: [system] Activating via syst
emd: service name='org.freedesktop.nm_dispatcher' unit='dbus-org.freedesktop.nm-dispatc
her.service' requested by ':1.14' (uid=0 pid=964 comm="/usr/sbin/NetworkManager --no-da
emon" label="unconfined")
2024-12-09T09:24:51.046355+01:00 rubenrf systemd[1]: Starting NetworkManager-dispatcher
.service - Network Manager Script Dispatcher Service...
2024-12-09T09:24:51.059268+01:00 rubenrf dbus-daemon[878]: [system] Successfully activa
ted service 'org.freedesktop.nm_dispatcher'
2024-12-09T09:24:51.061646+01:00 rubenrf systemd[1]: Started NetworkManager-dispatcher.
service - Network Manager Script Dispatcher Service.
2024-12-09T09:25:01.076005+01:00 rubenrf systemd[1]: NetworkManager-dispatcher.service:
Deactivated successfully.
2024-12-09T09:25:01.453034+01:00 rubenrf CRON[10285]: (root) CMD (command -v debian-sa1
> /dev/null && debian-sa1 1 1)
2024-12-09T09:25:12.462865+01:00 rubenrf tracker-miner-fs-3[10291]: (tracker-extract-3:
10291): GLib-GIO-WARNING **: 09:25:12.462: Error creating IO channel for /proc/self/mou
ntinfo: Parámetro incorrecto (g-io-error-quark, 13)
^C
eu@rubenrf:~$

```

10. Sen cerrar o terminal anterior, envía dende outro terminal, unha mensaxe a syslog usando o comando correspondente coa mensaxe “Mando unha mensaxe de proba a syslog”

```

eu@rubenrf:~$ tail -f /var/log/syslog
2024-12-09T09:24:51.019898+01:00 rubenrf NetworkManager[964]: <info> [1733732691.0178]
dhcp4 (enp0s3): state changed new lease, address=192.168.56.103
2024-12-09T09:24:51.026732+01:00 rubenrf dbus-daemon[878]: [system] Activating via syst
emd: service name='org.freedesktop.nm_dispatcher' unit='dbus-org.freedesktop.nm-dispatc
her.service' requested by ':1.14' (uid=0 pid=964 comm="/usr/sbin/NetworkManager --no-da
emon" label="unconfined")
2024-12-09T09:24:51.046355+01:00 rubenrf systemd[1]: Starting NetworkManager-dispatcher
.service - Network Manager Script Dispatcher Service...
2024-12-09T09:24:51.059268+01:00 rubenrf dbus-daemon[878]: [system] Successfully activa
ted service 'org.freedesktop.nm_dispatcher'
2024-12-09T09:24:51.061646+01:00 rubenrf systemd[1]: Started NetworkManager-dispatcher.
service - Network Manager Script Dispatcher Service.
2024-12-09T09:25:01.076005+01:00 rubenrf systemd[1]: NetworkManager-dispatcher.service:
Deactivated successfully.
2024-12-09T09:25:01.453034+01:00 rubenrf CRON[10285]: (root) CMD (command -v debian-sa1
> /dev/null && debian-sa1 1 1)
2024-12-09T09:25:12.462865+01:00 rubenrf tracker-miner-fs-3[10291]: (tracker-extract-3:
10291): GLib-GIO-WARNING **: 09:25:12.462: Error creating IO channel for /proc/self/mou
ntinfo: Parámetro incorrecto (g-io-error-quark, 13)
2024-12-09T09:26:54.565944+01:00 rubenrf root: Mando unha mensaxe de proba a syslog
2024-12-09T09:27:03.190547+01:00 rubenrf eu: Mando unha mensaxe de proba a syslog
2024-12-09T09:27:45.789289+01:00 rubenrf root: Mando unha mensaxe de proba a syslog

```

11. Comproba a configuración de rsyslog para a maioría dos ficheiros que están en /var/log/, e explica brevemente esa configuración.


```

#module(load="imudp")
#input(type="imudp" port="514")

# provides TCP syslog reception
#module(load="intcp")
#input(type="intcp" port="514")

# provides kernel logging support and enable non-kernel klog messages
module(load="imklog" permitnonkernelfacility="on")

#####
#### GLOBAL DIRECTIVES ####
#####

# Filter duplicated messages
$RepeatedMsgReduction on

#
# Set the default permissions for all log files.
#
$FileOwner syslog
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022
$PrivDropToUser syslog
$PrivDropToGroup syslog

#
# Where to place spool and state files
#
$WorkDirectory /var/spool/rsyslog

#
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf
eu@rubenrf:~$

```

A configuración de rsyslog en /var/log/ permite filtrar mensaxes por severidade e tipo, enviándoas a ficheiros como syslog, auth.log ou kern.log. Ademais, inclúe soporte para rotación de logs con logrotate e rexistros remotos en sistemas distribuídos. É personalizable segundo as necesidades do sistema.

12. Comproba a configuración da rotación das mensaxes de kern.log, e explica brevemente esa configuración.

```
eu@rubenrf:~$ cat /etc/logrotate.d/rsyslog
/var/log/syslog
/var/log/mail.log
/var/log/kern.log
/var/log/auth.log
/var/log/user.log
/var/log/cron.log
{
    rotate 4
    weekly
    missingok
    notifempty
    compress
    delaycompress
    sharedscripts
    postrotate
        /usr/lib/rsyslog/rsyslog-rotate
    endscript
}
eu@rubenrf:~$
```


Tarefa 4. Sistemas de ficheiros virtuais

4.1. MS Windows

Documenta a continuación os procesos de instalación e configuración que se plantexan a continuación, numerando e indicando cada paso, facendo capturas de pantalla que consideres que poden ser útiles. Indica sobre todos aqueles detalles nos que tiveches algunha dúbida ou problema. Se empregas algún comando ou editas algún ficheiro, indícao claramente.

4.1.1. Instalación servidor SMB/CIFS

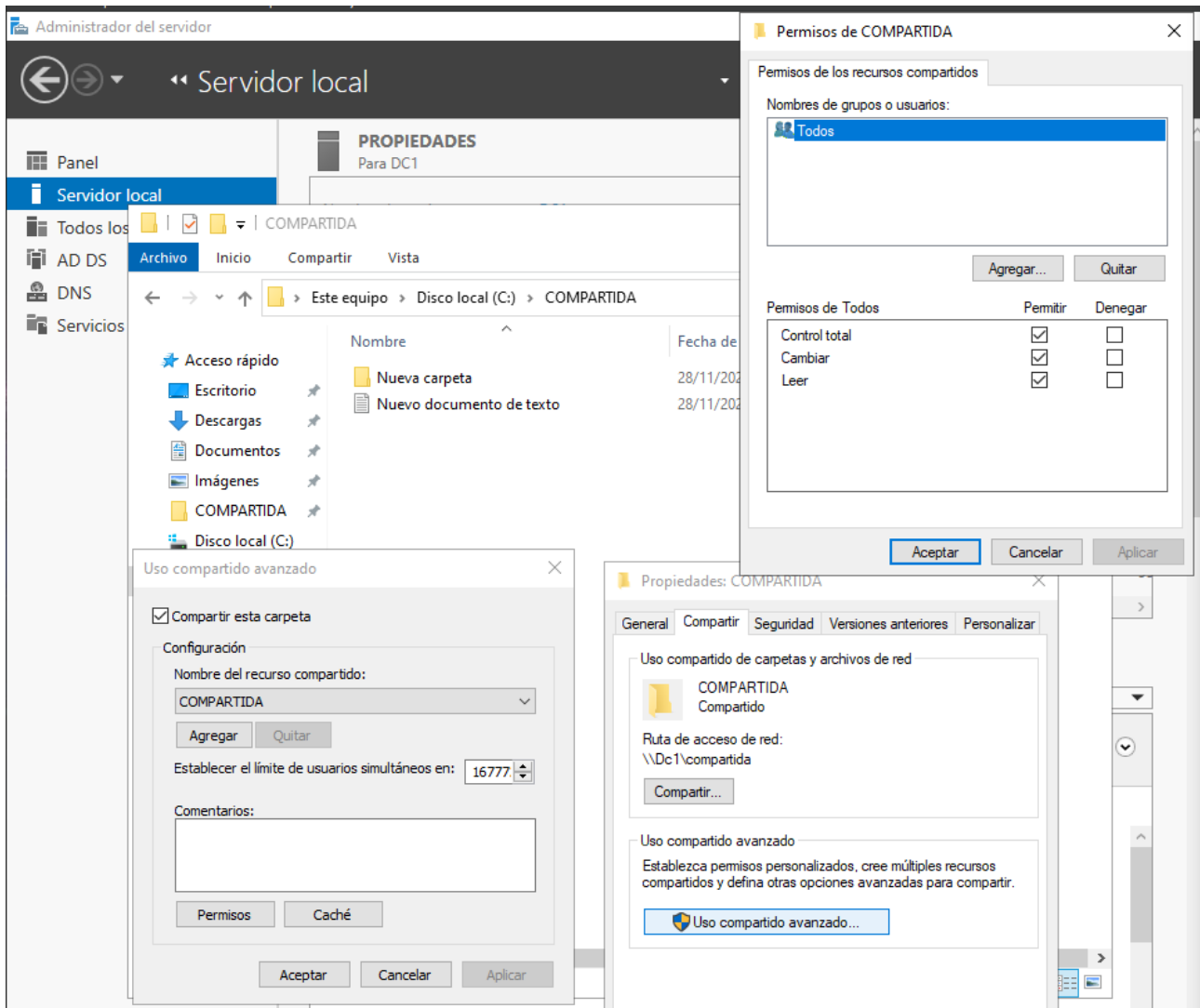
Nun servidor con Windows Server, comparte un cartafol `c:\compartido` para que sexa accesible a través de rede co nome `\\compartido`.

1.

```
[videos]
comment = Videos
path = /home/eu/Videos
browseable = yes
guest ok = yes
#writable = yes
read only = no
#valid users = @smbshare
create mask = 0755
```

4.1.2. Configuración SMB/CIFS para un cliente GNU/Linux

Fai que un cliente GNU/Linux teña acceso ao cartafol compartido anteriormente e se automonte en /mnt/compartido.

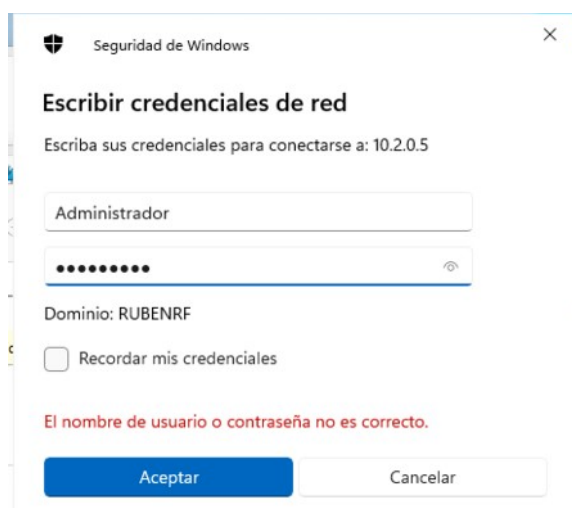
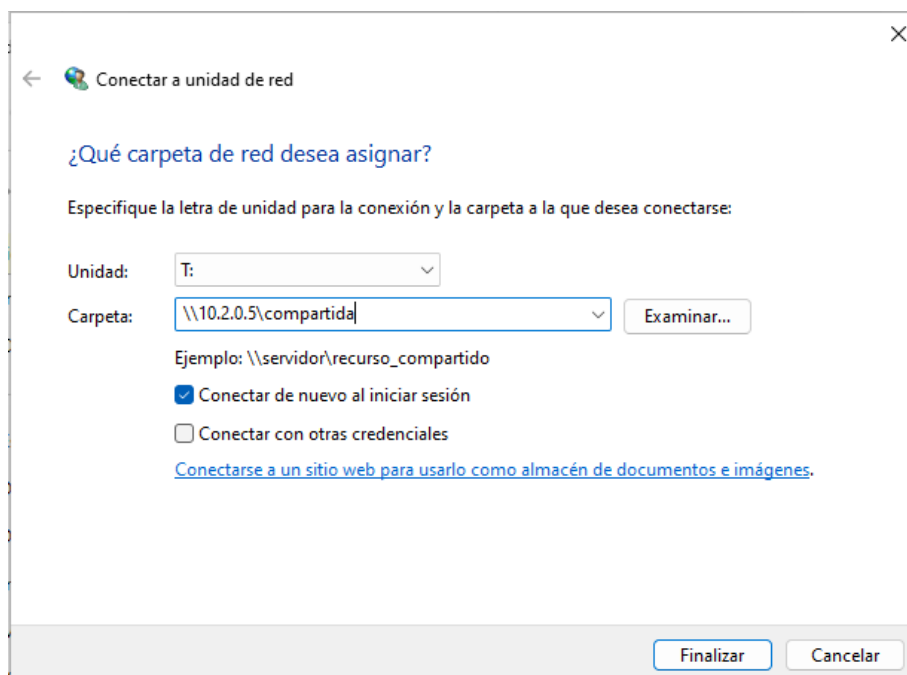


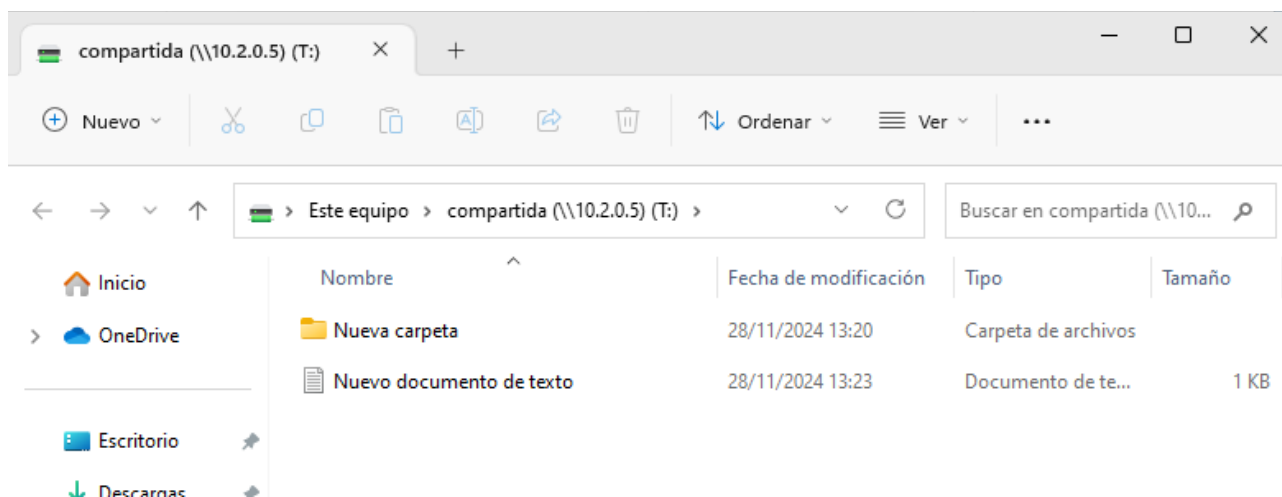
```
eu@rubenrf:/home$ sudo mkdir windows
eu@rubenrf:/home$ ls
eu rubenrf windows
```

```
eu@rubenrf:/home$ sudo mount -t cifs -o username=administador@rubenrf.local,password=A
bcd1234.,uid=1000,gid=1000 //10.2.0.5/compartida /home/windows
eu@rubenrf:/home$ ls windows
eu@rubenrf:/home$ ls windows
'Nueva carpeta'
```

4.1.3. Configuración SMB/CIFS para un cliente Windows

Fai que un cliente Windows teña acceso ao cartafol compartido anteriormente e se automonte na unidade T:.





4.2. GNU/Linux

Documenta a continuación os procesos de instalación e configuración que se formulan a continuación, numerando e indicando cada paso, facendo capturas de pantalla que consideres que poden ser útiles. Indica sobre todos aqueles detalles nos que tiveches algunha dúbida ou problema. Se empregas algún comando ou editas algún ficheiro, indícao claramente.

4.2.1. Instalación servidor SMB/CIFS

Nun servidor GNU/Linux, instala un sistema de ficheiros virtual (VFS) usando SMB/CIFS. O cartafol a compartir será /servidor/compartido con opción de lectura e escritura para todo equipo do mesmo rango da rede NAT do servidor.

2.

Sudo apt install samba

4.2.2. Configuración SMB/CIFS para un cliente GNU/Linux

1.

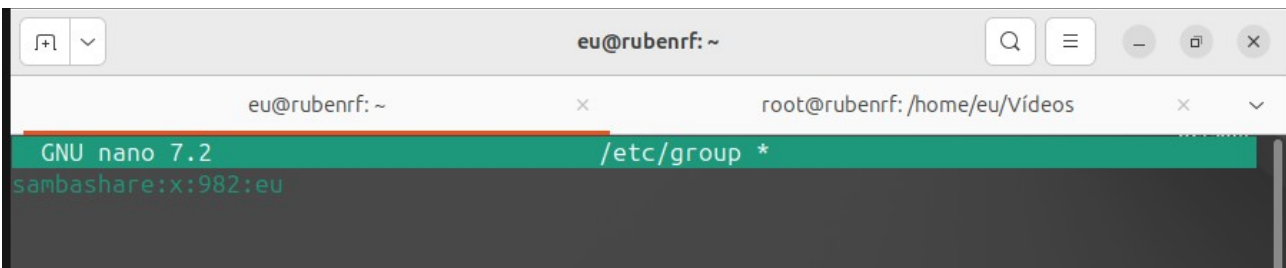
```
eu@rubenrf:~$ sudo nano /etc/samba/smb.conf
eu@rubenrf:~$ sudo systemctl restart smbd.service
eu@rubenrf:~$ sudo smbpasswd -a eu
New SMB password:
Retype new SMB password:
Added user eu.
eu@rubenrf:~$
```

```
#===== Global Settings =====
[global]

## Browsing/Identification ###

# Change this to the workgroup/NT-domain name your Samba server will part of
workgroup = iesrodolfoucha.es

# server string is the equivalent of the NT Description field
server string = %h server (Samba, Ubuntu)
```



```
eu@rubenrf: ~
GNU nano 7.2 /etc/group *
sambashare:x:982:eu
```

```
eu@rubenrf:~$ sudo nano /etc/group
eu@rubenrf:~$ id eu
uid=1000(eu) gid=1000(eu) grupos=1000(eu),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev)
,100(users),114(lpadmin),984(vboxsf),982(sambashare)
eu@rubenrf:~$
```

```

eu@rubenrf:~$ sudo pdbedit -L -v
-----
Unix username:      eu
NT username:
Account Flags:      [U          ]
User SID:           S-1-5-21-3457026252-6196863-2550620809-1000
Primary Group SID:  S-1-5-21-3457026252-6196863-2550620809-513
Full Name:          Eu
Home Directory:     \\RUBENRF\eu
HomeDir Drive:
Logon Script:
Profile Path:       \\RUBENRF\eu\profile
Domain:             RUBENRF
Account desc:
Workstations:
Munged dial:
Logon time:         0
Logoff time:        Mér, 06 Feb 2036 16:06:39 CET
Kickoff time:       Mér, 06 Feb 2036 16:06:39 CET
Password last set:  Xov, 28 Nov 2024 14:23:38 CET
Password can change: Xov, 28 Nov 2024 14:23:38 CET
Password must change: never
Last bad password   : 0
Bad password count  : 0
Logon hours        : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
eu@rubenrf:~$

```

4.2.3. Configuración SMB/CIFS para un cliente Windows

2.

Tarefa 5. Siglas

Busca e traduce as seguintes siglas **relacionados coa UD**:

	Siglas	Significado	Tradución
1	POSIX	Portable Operating System Interface	Interfaz de sistema operativo portátil
2	DOS	Disk Operating System	Sistema operativo de disco
3	DVD	Digital Versatile Disk	Disco versátil digital
4	BPA	Best Practices Analyzer	Analizador de Mejores Prácticas
5	VFS	Virtual File System	Sistema de archivos virtuales
6	NFS	Network File System	Sistema de archivos de red
7	NTDS	NT Directory Services	Servicios de directorio NT
8	IFS	Internal Field Separator	Separador de campo interno
9	WDK	Windows Driver Kit	Kit de controladores de Windows
10	EXT4	Fourth Extended File System	Cuarto sistema de archivos extendido
11	SMB	Server Message Block	Bloque de mensajes del servidor
12	CIFS	Common Internet File System	Sistema de archivos común de Internet