



Sistemas Operativos

Práctica

Lic. Exequiel Aramburu

exequiel.aramburu@uader.edu.ar



Esta obra está bajo una [Licencia Creative Commons Atribución-CompartirIgual 4.0 Internacional](https://creativecommons.org/licenses/by-sa/4.0/).

Agenda

- **Introducción** a la administración de registros del sistema (Logs).
- **Registros locales** de S.O y **Servidores de Logs**.
- **Archivos** de registros mas importantes del S.O en GNU/Linux.
- **Rotación** de registros del S.O en GNU/Linux.
- **Visualizar y administrar** los registros del S.O en GNU/Linux desde la terminal.
- **Visualizar y administrar** los registros del S.O en GNU/Linux con Herramientas Graficas.
- **Actividad extra aúlica. Visualizar y administrar** los registros del S.O en Microsoft Windows.

Introducción

¿QUÉ SON LOS LOGS O REGISTROS?

Los logs son registros de los eventos que se generan en los servidores, aplicaciones, redes y sistemas de una organización. Cada uno de estos archivos contiene información relacionada a un evento específico que ocurrió dentro de un equipo, sistema o red. **(Vieda, 2013)**

Glosario de Términos de Ciberseguridad establecida por la Resolución 1523/2019

Registro de actividad o log: es un registro oficial de eventos durante un rango de tiempo en particular que se emplea para registrar los datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre (CCN, 2015, pág. 741).

Fuente: <https://www.boletinoficial.gob.ar/detalleAviso/primera/216860/20190918>

CENTRO CRIPTOGRÁFICO NACIONAL (ESPAÑA): GUÍA DE SEGURIDAD (CCN-STIC-401) GLOSARIO Y ABREVIATURAS

2.849.3 LOG

Un log es un registro oficial de eventos durante un rango de tiempo en particular. Para los profesionales en seguridad informática es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué (who, what, when, where y why) un evento ocurre para un dispositivo en particular o aplicación.

<http://www.inteco.es/glossary/Formacion/Glosario/>

Nota: Instituto Nacional de Tecnologías de la Comunicación (INTECO) su actividad se focalizó en el ámbito de la ciberseguridad y en 2014 paso a denominarse Instituto Nacional de Ciberseguridad (INCIBE)

Fuente: <https://www.ccn-cert.cni.es/pdf/guias/glosario-determinos/22-401-descargar-glosario/file.html>

Instituto Nacional de Ciberseguridad de España (Incibe)

Glosario de términos de ciberseguridad

2.12.5. Log

Definición:

Registros de eventos de la actividad de los usuarios y de los procesos asociados a dicha actividad, como pueden ser el inicio/salida de sesión, tiempo de actividad o conexiones, entre otros. Esta información ayuda a detectar fallos de rendimiento, mal funcionamiento, errores e intrusiones que permiten generar alertas en tiempo real gracias a los datos proporcionados a los sistemas de monitorización.

https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

- **El log es un registro oficial de eventos** que se guardan en un equipo por un periodo de tiempo establecido.
- Cuando un evento ocurre el log generado debe responde las siguientes preguntas: **¿Quién?, ¿Qué?, ¿Cuándo?, ¿Dónde? y Por qué?**
- Los logs son ficheros de texto o base de datos donde se guarda información de eventos. Estos eventos pueden ser:

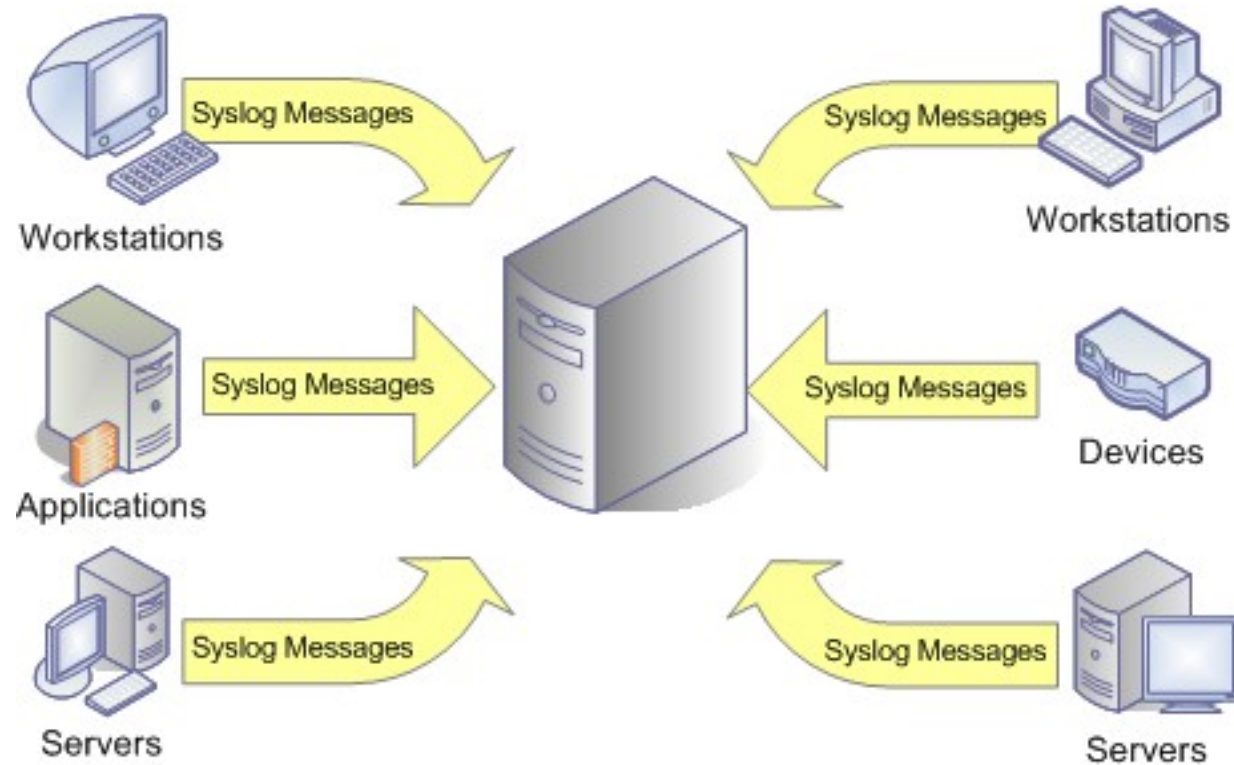
Logs de sistema: Generalmente generados por el demonio (ej:Rsyslogd). Registran información relacionada con el funcionamiento del sistema operativo. Algunos ejemplos de logs de sistema son los que registran información sobre los servicios, los que registran los accesos al equipo, los mensajes del sistema, etc.

Logs de programas: Son aquellos que registran cronológicamente los eventos más importantes mientras estamos usando una aplicación o programa. En este caso, los logs pueden ser generados por la propia aplicación o por un demonio (ej:Rsyslogd).

Logs Locales - Algunas ventajas:

- Detección de ataques e intrusos
- Detección de problemas de hardware/software
- Análisis forense de sistemas. Preservación de la información.
- Evaluación de vulnerabilidad
- Cumplimiento de la normativa legal o log de eventos con fines de auditoría.

Servidor de Logs

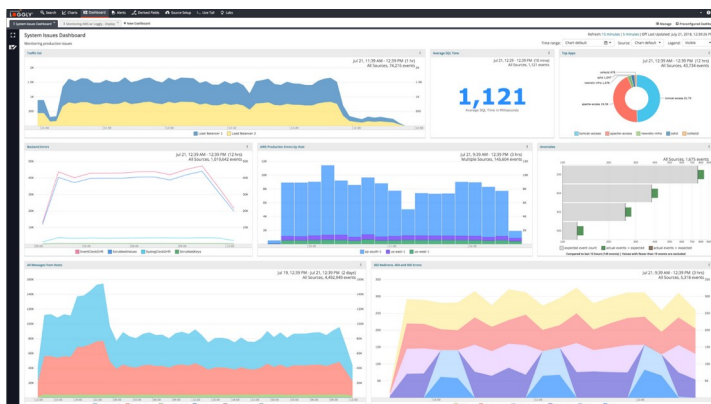


Syslog puede enviar información sobre TCP o UDP indistintamente. Por convención se usa el puerto 514 UDP

Servidor de Logs – Algunas ventajas:

- Preservación de la información.
- Respaldo centralizado.
- Almacenamiento centralizado en base de datos.
- Exploración y visualización avanzada: gráficos, tablas, etc.
- Detección de anomalías integrales.
- Cumplir estándares de seguridad.
- Trazabilidad de los eventos.
- Optimización de los análisis.
- Filtrado avanzado.

Algunos ejemplos:



Características a evaluar	LogAnalyzer	Splunk	Loggly
Software libre	X		
Visualización Web	X	X	X
Generación de Informes de estados	X	X	X
Generación de Informes estadísticos	X	X	X
Visualiza eventos de Windows	X	X	X
Visualiza eventos de Linux	X	X	X
Visualiza eventos de Oracle	X	X	X
Base de Datos incluida	X	X	
Identificador de tipo de logs	X	X	X
Monitoreo en tiempo real	X	X	X
Descarga de reportes generados	X	X	X
Envío de mensajes vía Email en caso de un evento crítico		X	X
Resuelve problemas operacionales			X
Servicio de logs en la nube		X	

Rotación de logs

Cuando hablamos de rotación de logs, nos referimos a lo siguiente:

- Determinar el tamaño máximo permitido para un archivo de log.
- Cuando se alcanza dicho tamaño, borrar el archivo, renombrarlo o comprimirlo y crear uno nuevo.
- Especificar por cuánto tiempo deseamos mantener los registros, ya sea comprimidos o no.

```
-rw-r----- 1 syslog adm 75861 ago 9 15:30 auth.log
-rw-r----- 1 syslog adm 217938 ago 7 00:00 auth.log.1
-rw-r----- 1 syslog adm 16837 jul 30 23:59 auth.log.2.gz
-rw-r----- 1 syslog adm 15902 jul 24 00:00 auth.log.3.gz
-rw-r----- 1 syslog adm 17096 jul 17 00:00 auth.log.4.gz
-rw-r----- 1 root root 9978 ago 9 14:40 host.log
```

En GNU/Linux → Logrotate

Logrotate es una utilidad de sistema que administra la compresión y rotación de archivos de logs en sistemas Linux. Si los logs no se rotan, comprimen y depuran de manera periódica, eventualmente pueden consumir todo el espacio en disco disponible en el sistema.

/etc/logrotate.conf

```
GNU nano 4.8 /etc/logrotate.d/rsyslog
/var/log/mail.info
/var/log/mail.warn
/var/log/mail.err
/var/log/mail.log
/var/log/daemon.log
/var/log/kern.log
/var/log/auth.log
/var/log/user.log
/var/log/lpr.log
/var/log/cron.log
/var/log/debug
/var/log/messages
{
    rotate 4
    weekly
    missingok
    notifempty
    compress
    delaycompress
    sharedscripts
    postrotate
        /usr/lib/rsyslog/rsyslog-rotate
    endscript
}
```

Archivos de registros mas importantes del S.O GNU/Linux.

`syslog`

Contiene todos los mensajes, excepto los de autenticación.

`auth.log`

Contiene los mensajes de autenticación.

`kern.log`

Contiene todos los mensajes del núcleo

`messages`

Contiene los mensajes del núcleo de los niveles 4-6 (*warning, notice e info*).

`daemon.log`

Contiene los mensajes de la *facility daemon*.

mail.log

Contiene todos los mensajes relativos al funcionamiento del servicio de correo. Hay otros, `mail.info`, `mail.err` y `mail.warn` que almacenan su *facility* correspondiente.

user.log

Contiene todos los mensajes de las aplicaciones de usuario.

lpr.log

Contiene todos los mensajes referentes al servicio de impresión.

btmp

Que registra los accesos fallidos al sistema.

wtmp




Que registra los accesos al sistema.

Estos ficheros, a diferencia de los restantes, tienen un formato binario y pueden leerse a través del comando **utmpdump**:

```
# utmpdump /var/log/btmp | more
```

Comando dmesg

dmesg (diagnostic message, mensajes de diagnóstico) es un comando presente en los sistemas operativos Unix que lista el buffer de mensajes del núcleo. Este buffer contiene una gran variedad de mensajes importantes generados durante el arranque del sistema y durante la depuración de aplicaciones. La información ofrecida por dmesg puede guardarse en el disco duro mediante un demonio de registro, como syslog.

- | | | |
|---------------------------------------|---|--|
| <code>dmesg -T</code> |  | Imprima marcas de tiempo legibles por humanos. |
| <code>dmesg --level=alert,crit</code> |  | imprimirá mensajes de error y advertencia solamente. |
| <code>dmesg --help</code> |  | imprimirá la ayuda. |



gnome-logs

<https://wiki.gnome.org/Apps/Logs>

Registros 14:47 - 18:57			<div><div>Q</div><div>📁</div><div>☰</div><div>—</div><div>□</div><div>✕</div></div>	
Importante	<div><div>Q</div><div></div></div>			
Todo	Aplicaciones	pam_ecryptfs: seteuid error	15:43	
	Otros	Can't find sendmail at /usr/sbin/sendmail, not mailing output	14:52	
Aplicaciones	Seguridad	Failed to start Dunst notification daemon.	14:47	
	Otros	Device: /dev/nvme0, number of Error Log entries increased from 207 to 208		
Sistema	Otros	Failed to start Take snapper snapshot of root on boot. 2		
	Sistema			
Seguridad				
Hardware	Hardware	nvme nvme0: failed to set APST feature (2)		

Herramientas Graficas

kssystemlog

<https://apps.kde.org/es/kssystemlog>



KSystemLog

Visor de registros del sistema

Registro journald — KSystemlog

Archivo Editar Registros Ventana Preferencias Ayuda

Detener Recargar Detalles Registro del sistema Registro del núcleo Registro de autenticación Registro de X.org Registro journald

Filtro: Introduzca aquí su búsqueda... Todo Seleccionar prioridades

Fecha	Unidad	Mensaje
8/8/22 18:59	user@1000.service	Setting priority nice level to 19
8/8/22 18:59	dbus-daemon	[session uid=1000 pid=1623] Successfully activated service 'org.freedesktop.Tracker1.Mi...
8/8/22 18:59	systemd	Started Tracker metadata extractor.
8/8/22 18:59	sudo	pam_unix(sudo:session): session closed for user root
8/8/22 18:59	systemd	tracker-extract.service: Succeeded.
8/8/22 19:00	systemd	Started Timeline of Snapper Snapshots.
8/8/22 19:00	dbus-daemon	[system] Activating service name='org.opensuse.Snapper' requested by ':1.170' (uid=0 pi...
8/8/22 19:00	dbus-daemon	[system] Successfully activated service 'org.opensuse.Snapper'
8/8/22 19:00	systemd	snapper-timeline.service: Succeeded.
8/8/22 19:00	dbus-daemon	[system] Activating via systemd: service name='org.freedesktop.hostname1' unit='dbus-...
8/8/22 19:00	systemd	Starting Hostname Service...
8/8/22 19:00	dbus-daemon	[system] Successfully activated service 'org.freedesktop.hostname1'
8/8/22 19:00	systemd	Started Hostname Service.
8/8/22 19:00	sudo	exequiel : TTY=unknown ; PWD=/home/exequiel ; USER=root ; COMMAND=/usr/lib/linux...
8/8/22 19:00	sudo	pam_unix(sudo:session): session opened for user root by (uid=0)
8/8/22 19:00	sudo	pam_unix(sudo:session): session closed for user root
8/8/22 19:00	tracker-store	OK
8/8/22 19:00	systemd	tracker-store.service: Succeeded.
8/8/22 19:00	kernel	pcieport 0000:00:1b.4: AER: Corrected error received: 0000:00:1b.4
8/8/22 19:00	kernel	pcieport 0000:00:1b.4: PCIe Bus Error: severity=Corrected, type=Physical Layer, (Receive...
8/8/22 19:00	kernel	pcieport 0000:00:1b.4: device [8086:a3eb] error status/mask=00000001/00002000
8/8/22 19:00	kernel	pcieport 0000:00:1b.4: [0] RxErr
8/8/22 19:00	systemd	systemd-hostnamed.service: Succeeded.

1.000 líneas. 19:00:31: Entradas de journald cargadas correctamente. Última actualización: 19:00:36.

KSystemLog muestra todos los registros del sistema, agrupados por servicios generales (registro predeterminado del sistema, autenticación, kernel, X.org...) y opcionales (Apache, Cups...). Incluye diversas funcionalidades para leer los archivos de registro de forma agradable:

- Líneas de registro coloreadas según su severidad
- Vista en pestañas para poder mostrar varios registros a la vez
- Muestra de forma automática las nuevas líneas registradas
- Información detallada para las líneas de cada registro



Nota: Los instaladores para Windows también se pueden descargar de la binary-factory.
<https://binary-factory.kde.org/>

Visor de Eventos

Visor de eventos (local)

- Vistas personalizadas
 - Eventos administrativos
 - Registros de Windows
 - Registros de aplicaciones y suscripciones

Eventos administrativos Número de eventos: 1.810

Número de eventos: 1.810

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Advertencia	9/8/2022 00:23:07	DistributedCOM	10016	Ninguno
Advertencia	9/8/2022 00:20:43	DistributedCOM	10016	Ninguno
Advertencia	9/8/2022 00:09:15	DistributedCOM	10016	Ninguno
Advertencia	8/8/2022 21:18:20	DistributedCOM	10016	Ninguno
Error	8/8/2022 21:11:04	WindowsUpdateClient	20	Agente de Windows Update
Advertencia	8/8/2022 21:03:16	User Device Registration	360	Ninguno
Error	8/8/2022 21:03:09	EventLog	1101	Procesamiento de eventos
Critico	8/8/2022 16:03:00	Kernel-Power	41 (63)	
Error	8/8/2022 21:03:09	EventLog	6008	Ninguno
Advertencia	2/8/2022 20:37:43	DistributedCOM	10016	Ninguno
Advertencia	2/8/2022 20:12:22	DistributedCOM	10016	Ninguno
Advertencia	2/8/2022 19:29:46	DistributedCOM	10016	Ninguno
Advertencia	2/8/2022 19:12:33	DistributedCOM	10016	Ninguno
Advertencia	2/8/2022 18:45:16	DistributedCOM	10016	Ninguno
Advertencia	2/8/2022 18:33:40	DistributedCOM	10016	Ninguno
Advertencia	2/8/2022 17:57:08	DistributedCOM	10016	Ninguno
Advertencia	2/8/2022 17:23:26	DistributedCOM	10016	Ninguno
Advertencia	2/8/2022 16:55:21	DistributedCOM	10016	Ninguno
Advertencia	2/8/2022 13:24:00	DistributedCOM	10016	Ninguno
Error	2/8/2022 13:23:55	Application Error	1000 (100)	
Advertencia	2/8/2022 13:23:42	User Device Registration	360	Ninguno

Evento 10016, DistributedCOM

General Detalles

La configuración de permisos específico de la aplicación no concede el permiso Activación Local para la aplicación de servidor COM con CLSID {2593F8B9-4EAF-457C-B68A-50F6B8EA6B54}

Nombre de registro: Sistema

Origen: DistributedCOM Registrado: 9/8/2022 00:23:07

Id. del 10016 Categoría de tarea: Ninguno

Nivel: Advertencia Palabras clave: Clásico

Usuario: prueba\Exequiel Equipo: prueba

Código de operación: Información

Más información: [Ayuda Registro de eventos](#)

Acciones

Eventos administrativos

- Abrir registro guardado...
- Crear vista personalizada...
- Importar vista personalizada...
- Filtrar vista personalizada actual...
- Propiedades
- Buscar...
- Guardar todos los eventos en la vista personalizada ...
- Exportar vista personalizada...
- Copiar vista personalizada...
- Adjuntar tarea a esta vista personalizada...

Ver

Actualizar

Ayuda

Evento 10016, DistributedCOM

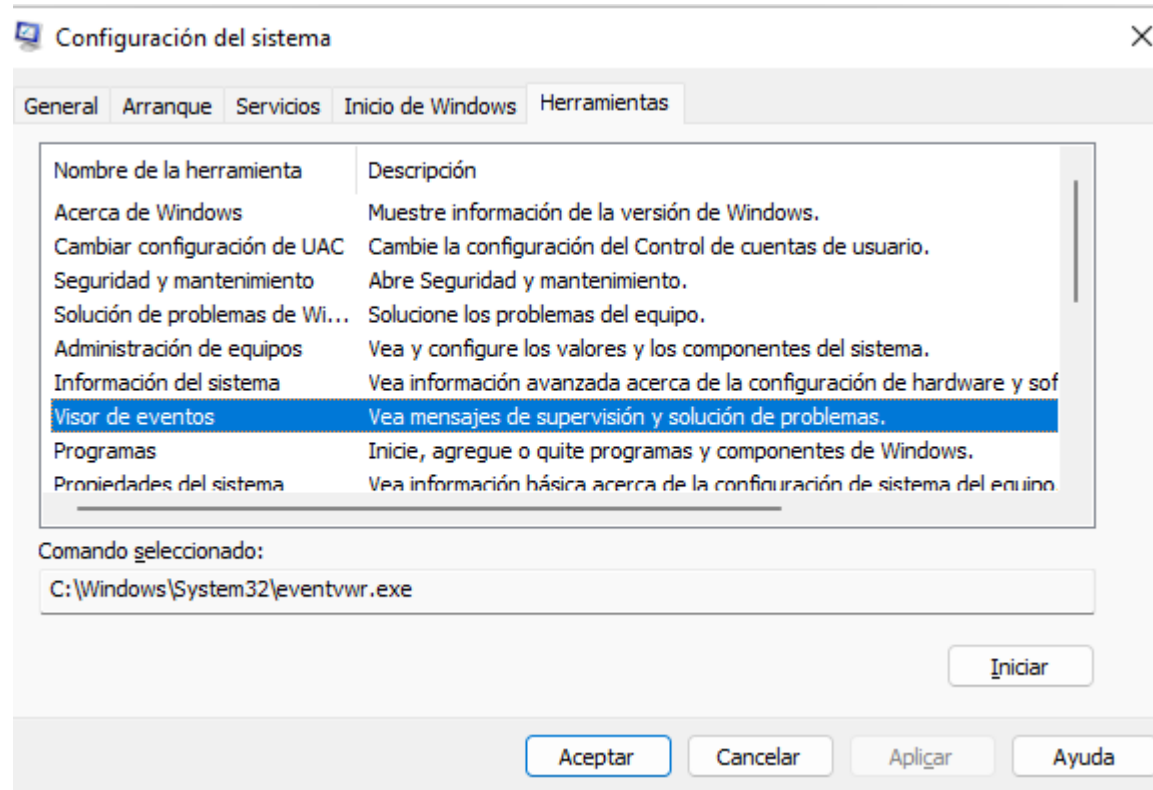
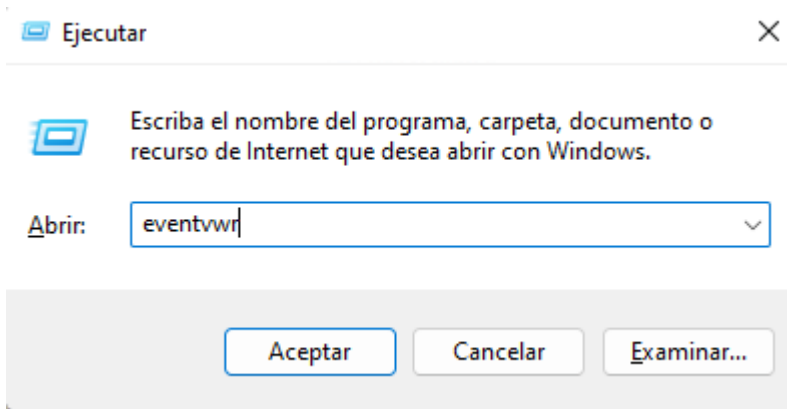
- Propiedades de evento
- Adjuntar tarea a este evento...
- Copiar
- Guardar eventos seleccionados...
- Actualizar
- Ayuda

Muestra las propiedades del evento.

Visor de Eventos

Ejecutar → eventvws

msconfig → Visor de Eventos



Visor de Eventos

El Visor de eventos puede gestionar registro de acontecimientos dentro de:

- **Eventos reenviados.** Aquellos registros que se reciben desde otra máquina.
- **Eventos de software.** Esto engloba registros como errores o avisos que proceden de nuestras aplicaciones y programas. Los eventos referidos a errores son los más importantes, las advertencias le precederían con un grado más bajo de riesgo.
- **Eventos de seguridad.** Este apartado está relacionado con los registros en relación con auditorías dentro de los inicios de sesión pudiendo saber si un usuario ha podido logarse correctamente o no. Puede darnos una idea de quién ha intentado usar nuestro equipo y cuándo.
- **Eventos del sistema.** Aquí se almacenan acontecimientos sobre el propio sistema y todo lo relacionado a cómo funciona.
- **Eventos de configuración.** Registros en relación a máquinas establecidas como controladores de dominio.

<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor>

Práctica de Laboratorio 1

Identificar intentos fallidos autenticación en el log auth.log

- 1 Ejecute dos terminales (1 y 2).
- 2 En la terminal 1 monitorear el archivo de logs ejecutando el siguiente comando:
tail -f -n 18 /var/log/auth.log
- 3 En la terminal 2, intente autenticarse con el usuario root e ingrese una contraseña incorrecta.
su root
- 4 Desde la terminal 1, identifique el intento fallido

Práctica de Laboratorio 2

Identificar usuario nuevos en el archivo de log:

- 1 Ejecute una terminal
- 2 Cree un usuario con el comando:
adduser prueba
- 3 En el archivo de log auth.log identifique el usuario creado.

Práctica de Laboratorio 3

Identificar usuario nuevos en el archivo de log:

- 1 Ejecute el visor de eventos grafico (ej: registros, KsystemLog,etc)
- 2 Identifique los eventos de la práctica de laboratorio 1 y 2

Actividad extra aúlica

- 1) Realizar ambas pruebas de laboratorio (1 y 2) en Microsoft Windows e identificar en el visor de sucesos los eventos cada una de ellas.
- 2) Crear un filtro con los eventos del punto 1.
- 3) Exportar los resultados del filtro personalizado.
- 4) Exponer en la clase próxima los 3 puntos anteriores.

GRUPO 1
GRUPO 2
GRUPO 3
GRUPO 4
GRUPO 5
GRUPO 6
GRUPO 7
GRUPO 8
GRUPO 9
GRUPO 10

Aleatorio

GRUPO 6

