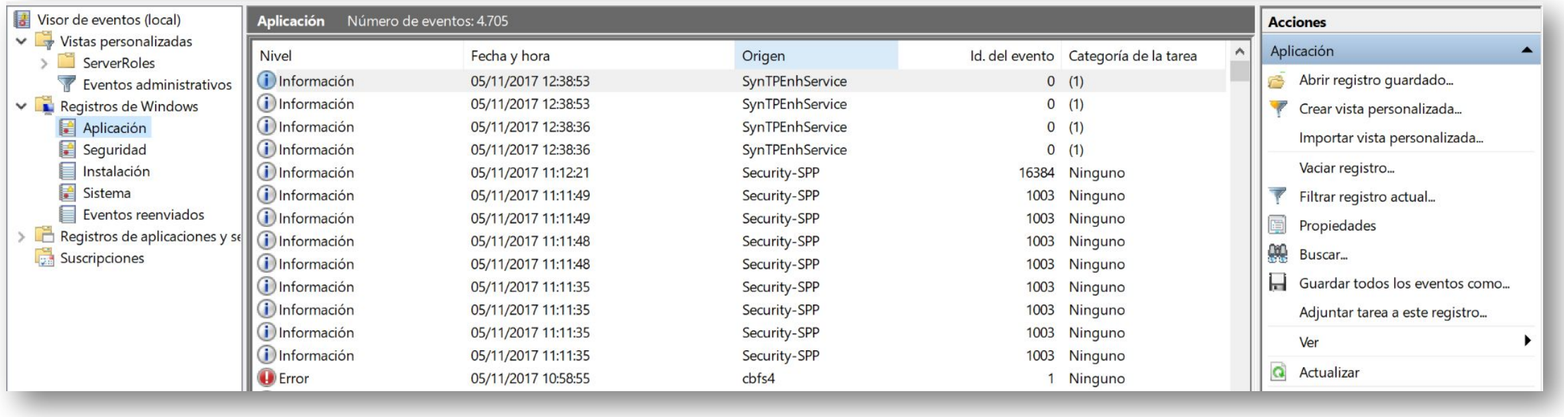
THE BRIDGE

Eventos de los LOGs de Windows

Visor de Eventos de Windows

- El Visor de Eventos de Windows recopila información en forma de "**eventos**", que son básicamente registros de lo que ha ocurrido en el sistema.
- Es una herramienta que te permite ver y analizar los registros de eventos del sistema operativo Windows.
- Estos registros contienen información detallada sobre lo que sucede en tu computadora, como errores, advertencias, auditorías de seguridad y eventos del sistema.
- Puedes usar el Visor de Eventos para diagnosticar problemas, monitorear el rendimiento del sistema y asegurarte de que todo funcione correctamente
- Para abrirlo, simplemente haz clic en el botón de Inicio, escribe "**Visor de eventos**" en la barra de búsqueda y selecciona la aplicación que aparece.

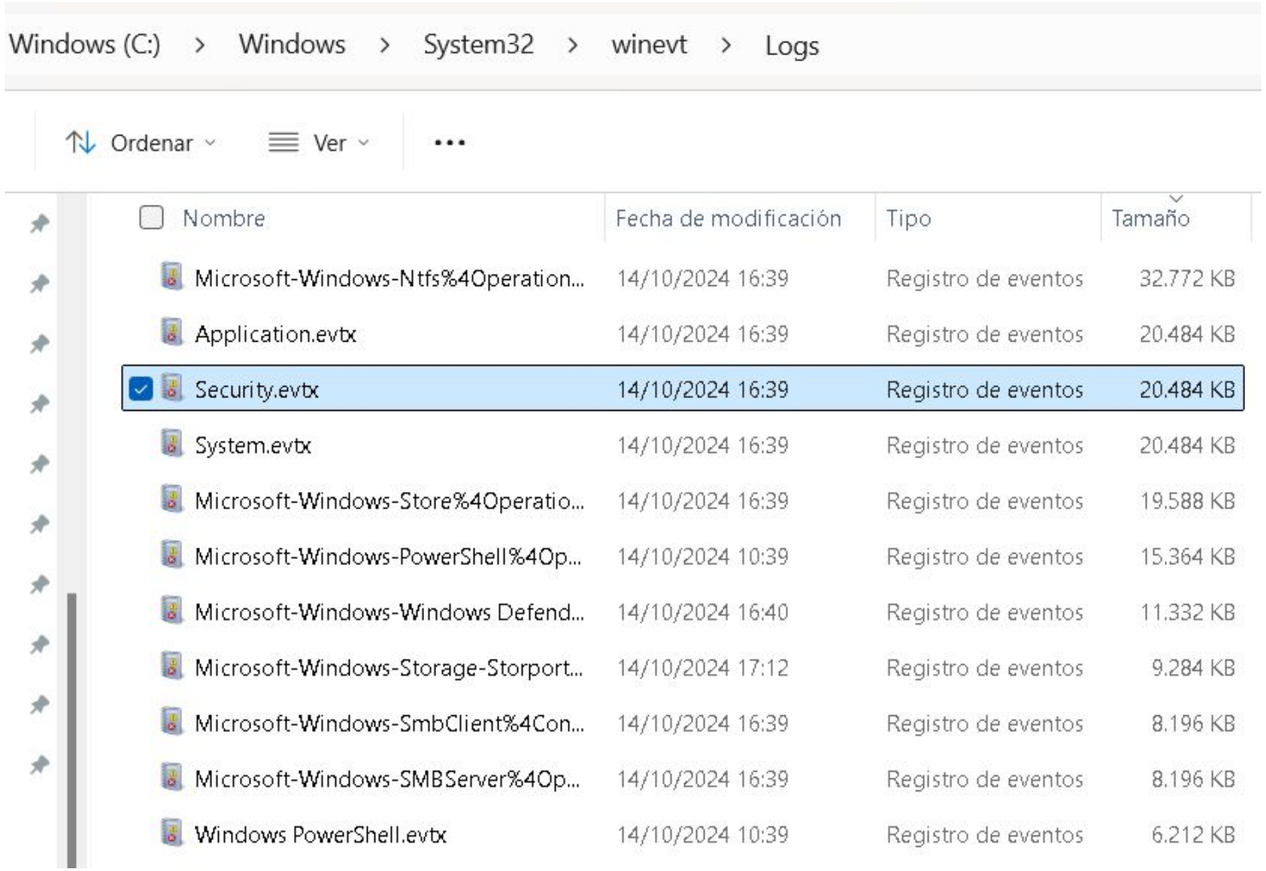


Visor de Eventos de Windows.

- Hay varios tipos de eventos que puedes encontrar:
  - **Eventos del sistema (System).**
  - **Eventos de seguridad (Security)**.
  - **Eventos de aplicaciones (Application).**
  - **Eventos reenviados.**

Visor de Eventos de Windows.

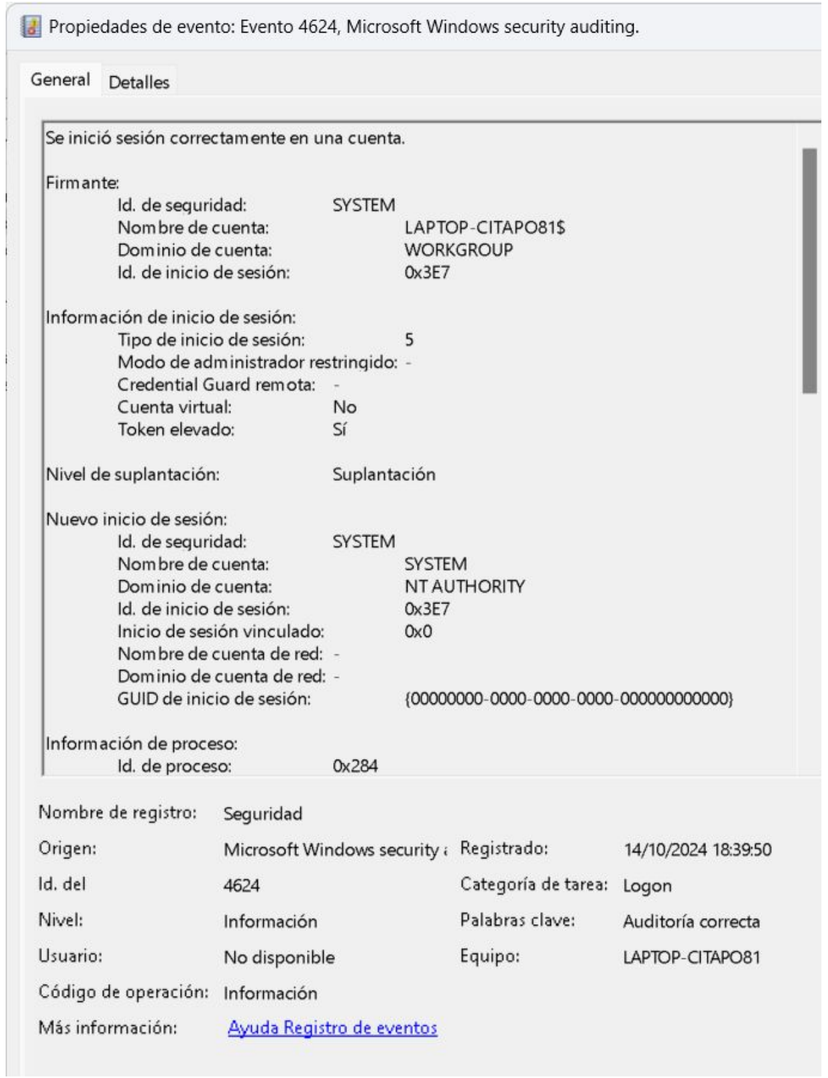
- Los registros se almacenan en archivos con extensión .evtx.
- Estos archivos están ubicados en distintas carpetas según el tipo de registro.
- Por lo general, se encuentran en la carpeta **C:\Windows\System32\winevt\Logs**.
- Aquí están algunas rutas típicas de los archivos de eventos:
  - **Eventos de aplicaciones: Application.evtx**
  - **Eventos de seguridad: Security.evtx**
  - **Eventos del sistema: System.evtx**
- Puedes acceder directamente a estos archivos y abrirlos con el Visor de Eventos para revisarlos.



Eventos Importantes del Visor de Eventos

- **Eventos de Seguridad**

Descripción del evento	Event ID
Limpieza del Event Log de Windows	1102
Inicio de sesión exitoso	4624
Intento de inicio de sesión fallido	4625
Inicio de sesión de un nuevo usuario	4626
EL usuario ha hecho una desconexión (logoff)	4647
Intento de borrado de un objeto	4659
EL objeto ha sido Borrado	4660
Acceso a un objeto	4663
Cambio de permisos de un objeto	4670
Uso de privilegios elevados	4672
Creación de un proceso	4688
Terminación de un proceso	4689
Creación de un nuevo servicio	4697
Cambio de la política de auditoría	4719
Creación de una cuenta de usuario	4720



Eventos Importantes del Visor de Eventos

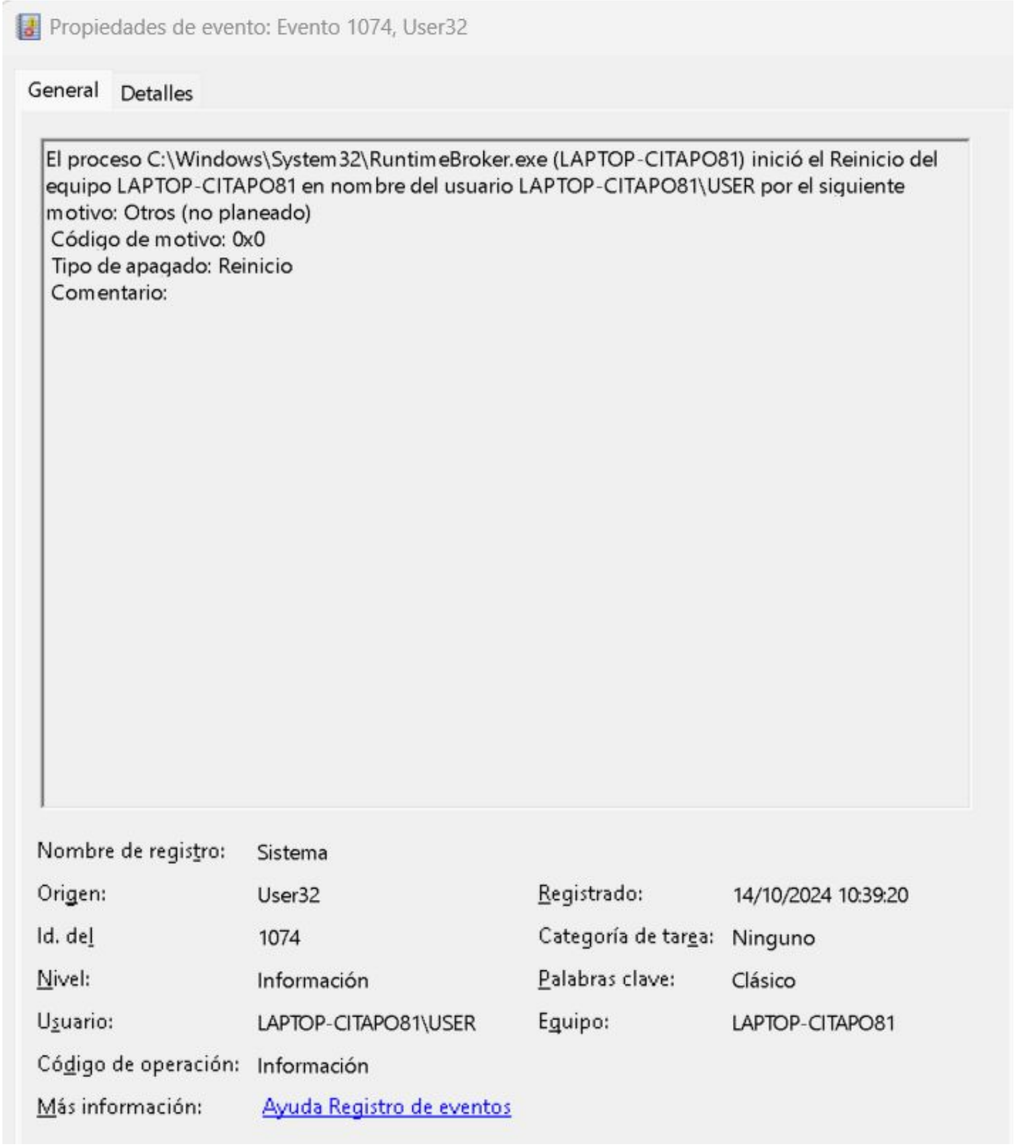
- **Eventos de Seguridad**

Descripción del evento	Event ID
La cuenta de usuario esta activa	4722
Cambio de la contraseña de una cuenta de usuario	4723
Reinicio de la contraseña de un usuario	4724
Usuario añadido a un Grupo	4732
Usuario removido de un Grupo	4733
Cambio de los parámetros de configuración de la cuenta de usuarios	4738
La cuenta está bloqueada	4740
La cuenta se ha desbloqueada	4767
Intento de inicio de sesión fallido debido a la cuenta bloqueada (kerberos)	4771
Reconexión de una sesión de Terminal Services	4778
Desconexión de una sesión de Terminal Services	4779
Modificación de un objeto en el AD	5136
Creación de un objeto en el AD	5137

Eventos Importantes del Visor de Eventos

- **Eventos del Sistema**

Descripción del evento	Event ID
Reinicio o apagado del servidor	1074
Servicio del event Log iniciado	6005
Servicio del event Log detenido	6006
Reinicio del sistema forzado	6008
Creación de Servicio que es interactivo con el escritorio	7030
El servicio termino de forma inesperada	7034
El Servicio ha cambiado a iniciado	7036
El Servicio ha cambiado a detenido	7038
Cambio del tipo de inicio del sistema (disabled, manual, Automatic)	7040
Creación de un servicio en el sistema Operativo	7045



Eventos Importantes del Visor de Eventos

- **Eventos de Aplicación**

Descripción del evento	Event ID	Event
Falla la acrualizacion de AV	2001	MS defender
Cambios en el firewall	4950	Firewall
El AV tiene un error y ha terminado	5008	MS defender
El firewall se ha detenido	5025	Firewall
Indica que la directiva de AppLocker bloquearía el archivo	8003	AppLocker
AppLocker bloqueó el archivo EXE o DLL con el nombre indicado	8004	AppLocker
Indica que la directiva de AppLocker bloquearía el script o el archivo de .msi	8006	AppLocker
AppLocker bloqueó el script o MSI con el nombre indicado	8007	AppLocker


THE
BRIDGE

Permiso SGID

- Crear directorio **compartido**
- Establecer permisos **770** con **SGID**.
  - **chmod 2770 /compartido**
- Validar los permisos de compartido
- Cambiar al usuario **root.**
- Crear archivo **test.txt** en compartido.
- Validar los permisos de test.
- Cambiamos al usuario normal.
- Validamos los permisos.
- Editamos el archivo.
- ¿Pudimos editar?