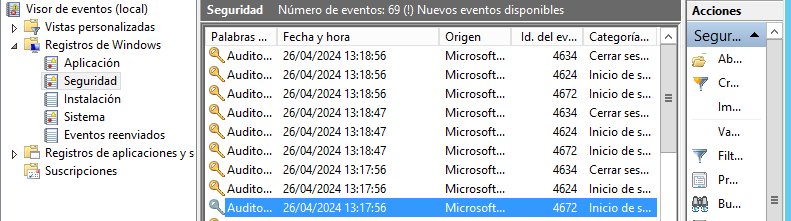
**ACTIVIDAD PRÁCTICA- VISOR DE EVENTOS**

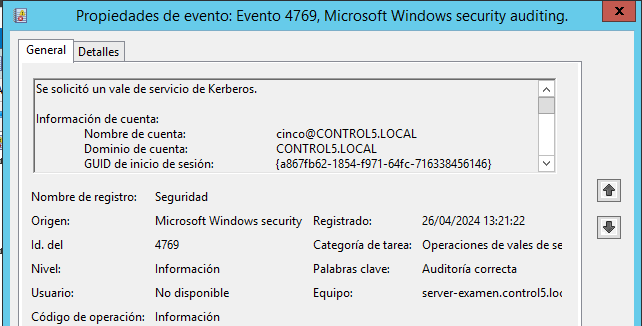
Para cada pregunta, el estudiante deberá utilizar el Visor de eventos de Windows Server para identificar el evento concreto solicitado, proporcionar el ID de evento correspondiente y especificar en qué registro se encuentra dicho evento.

**Pregunta 1:**

**Utilice el Visor de eventos de Windows Server para identificar el evento que se produce cuando un usuario inicia sesión en el servidor controlador de dominio. ¿Cuál es el ID del evento y en qué registro se encuentra este evento? Realiza la misma tarea para el caso de un usuario que inicia sesión en un cliente del dominio. ¿Qué diferencias encuentras?**



ID del cliente:



**Pregunta 2:**

**Utilice el Visor de eventos de Windows Server para identificar el evento que se produce cuando intentamos acceder al servidor con una cuenta que no existe. ¿Cuál es el ID del evento y en qué registro se encuentra este evento?**



El ID de evento es 4625 y se encuentra en el registro de Seguridad

**Pregunta 3:**

**Utilice el Visor de eventos de Windows Server para identificar el evento que se produce cuando un usuario modifica la hora del sistema. ¿Cuál es el ID del evento y en qué registro se encuentra este evento para cada una de estas dos acciones?**

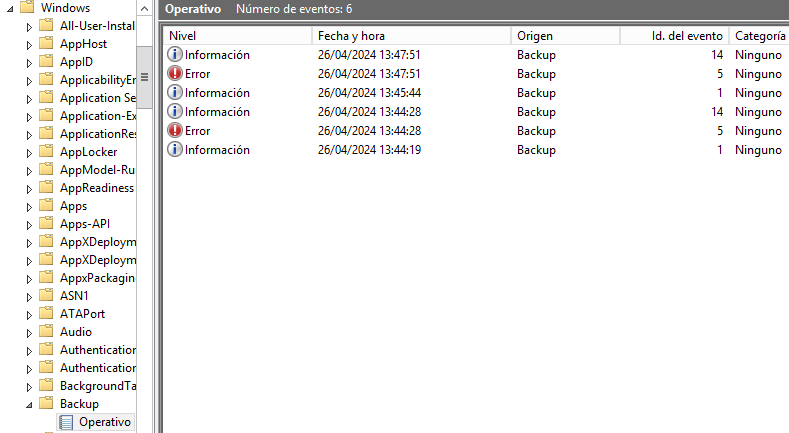
**Para modificar la hora del sistema debes hacerlo por comandos. Comando “time”**



El ID de evento es 4616 y se encuentra en el registro del sistema

**Pregunta 5:**

**Utilice el Visor de eventos de Windows Server para identificar el evento que se produce cuando se realiza una copia de seguridad de un archivo. ¿Cuál es el ID del evento y en qué registro se encuentra este evento?**



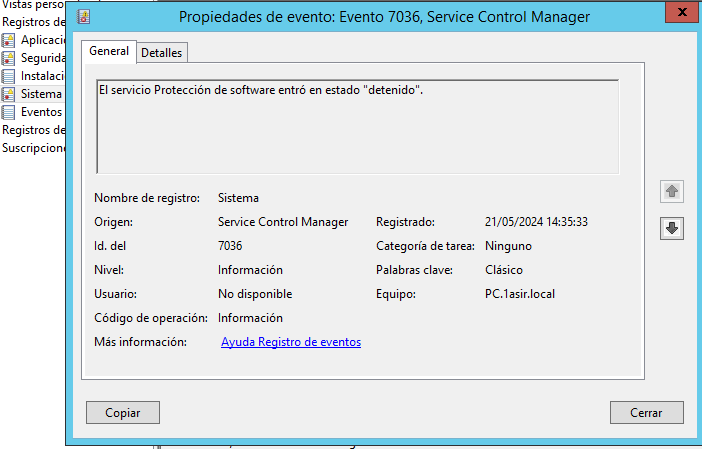
El ID de evento 1 hace referencia a que se inició la copia de seguridad

El ID de evento 5 hace referencia a un fallo en la copia de seguridad

El ID de evento 14 hace referencia a el éxito de la copia de seguridad

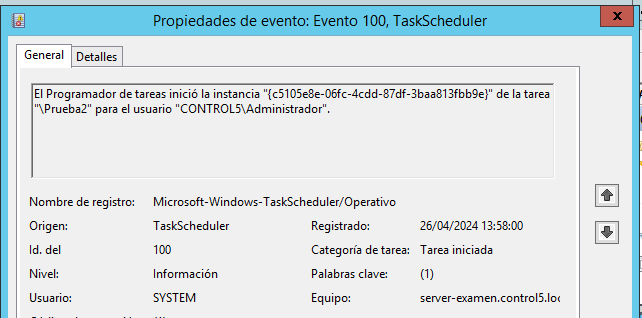
**Pregunta 6:**

**Utilice el Visor de eventos de Windows Server para identificar el evento que se produce cuando se desactiva el servicio de Firewall. ¿Cuál es el ID del evento y en qué registro se encuentra este evento?**



**Pregunta 7:**

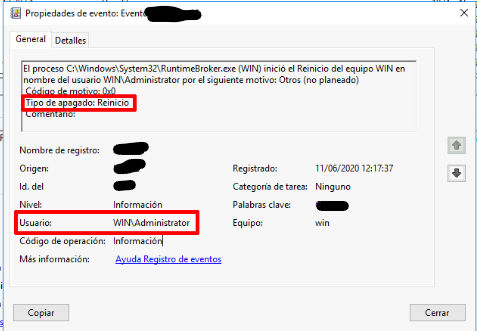
**Utilice el Visor de eventos de Windows Server para identificar el evento que se produce cuando se crea una tarea programada. ¿Cuál es el ID del evento y en qué registro se encuentra este evento?**

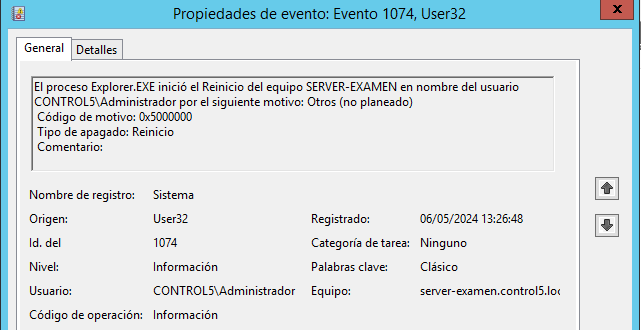


El ID de evento es 100 y se encuentra dentro de: Registro de aplicaciones → Microsoft → Windows → TaskScheduler → Operativo

**Pregunta 8:**

**Utilice el Visor de eventos de Windows Server para identificar el evento que se produce cuando un usuario reinicia el servidor. ¿Cuál es el ID del evento y en qué registro se encuentra este evento? Deberás obtener la información de qué usuario realizó la tarea. Aquí tienes un ejemplo:**

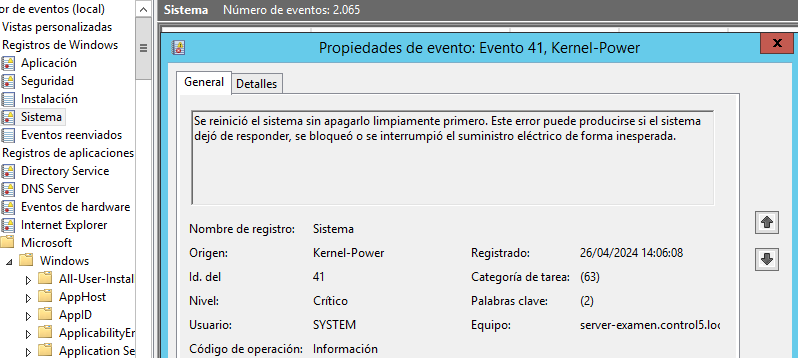




El ID de evento es 1074 y se encuentra dentro de registros del sistema

**Pregunta 9:**

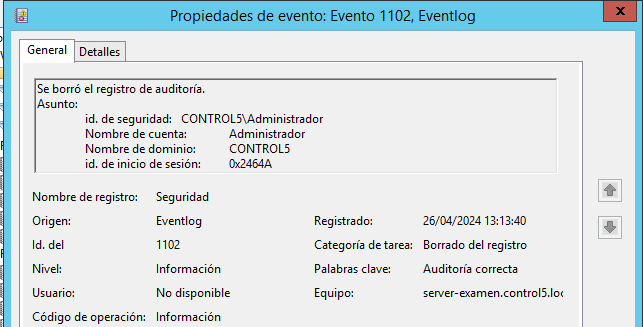
**Utilice el Visor de eventos de Windows Server para identificar el evento que se produce cuando se apaga el servidor de forma inesperada. Puedes realizar el apagado “brusco” a través del interfaz de VirtualBox. ¿Cuál es el ID del evento y en qué registro se encuentra este evento? Aquí tienes un ejemplo:**



Este evento se encuentra en Registros de Windows → Sistema → Crítico

**Pregunta 10:**

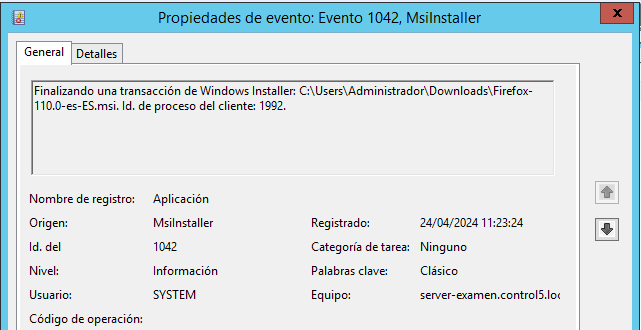
**Utilice el Visor de eventos de Windows Server para identificar el evento que se produce cuando se borran los registros del visor de sucesos. Es poco probable que los datos del registro de eventos se borren durante las operaciones normales y es probable que un atacante malintencionado intenta cubrir sus pistas borrando un registro de eventos. ¿Cuál es el ID del evento y en qué registro se encuentra este evento?**



El ID de evento es 1102 y se encuentra dentro de Registro de Seguridad

**Pregunta 11:**

**Utilice el Visor de eventos de Windows Server para identificar los eventos que se producen cuando se instala una aplicación “MSI” o se añade un nuevo servicio al servidor (Por ejemplo, IIS, servidor web).**

****

El ID de evento es 1042 y se encuentra dentro del Registro de Aplicaciones y filtrando por nombre de MsiInstaller