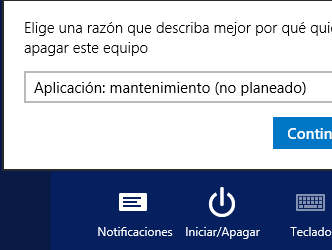
UD 8-P2

Auditar eventos de reinicio y apagado del servidor

Realiza los siguientes ejercicios y haz captura de pantallas a medida que los vas desarrollando, dando las explicaciones necesarias. Ayúdate de la referencia web ya utilizada en el tema anterior: consulta el siguiente sitio web:  
<https://blogvirtualizado.com/eventos-de-reinicio-apagado-de-windows-server-en-el-visor-de-eventos/>

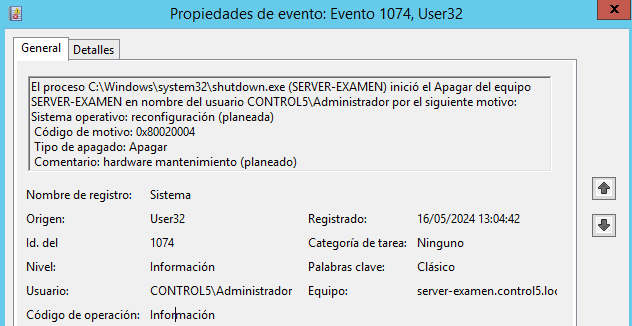
1. Inicia sesión en el servidor con el usuario gestor empleado en la práctica anterior.

Realiza un *apagado* del servidor indicando como motivo “hardware mantenimiento (planeado).

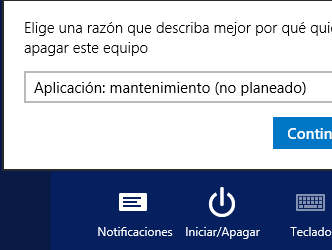


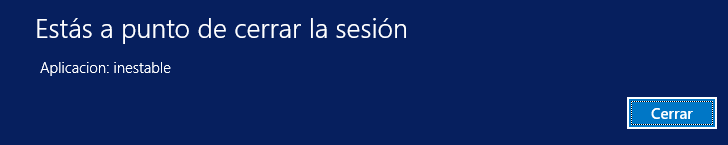
1. Arranca de nuevo el servidor, inicia sesión con el administrador y obtén por medio del visor de eventos la siguiente información en relación a este reinicio

| **Id de evento** | 1074 |
| --- | --- |
| **Texto descriptivo del evento** |  |
| **Nombre de registro** | Sistema |
| **Tipo de Apagado** | Apagar |
| **Usuario**  **Equipo** | CONTROL5\Administrador  server-examen.control5.local |



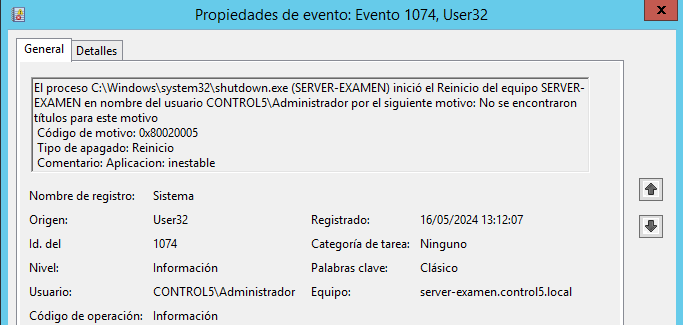
1. **A continuación haz un reinicio del servidor marcando como motivo de reinicio “*Aplicación:inestable*”. Hazlo con el propio administrador**





1. **Una vez que arranque el servidor, inicia sesión con el administrador y obtén por medio del visor de eventos la siguiente información en relación a este reinicio**

| **Id de evento** | 1074 |
| --- | --- |
| **Texto descriptivo del evento** |  |
| **Nombre de registro** | Sistema |
| **Tipo de Apagado** | Reinicio |
| **Usuario**  **Equipo** | CONTROL5\Administrador  server-examen.control5.local |

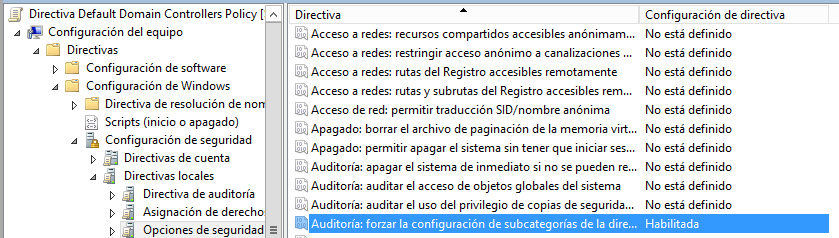


1. **¿Qué proceso inicia el apagado en el apartado anterior?**

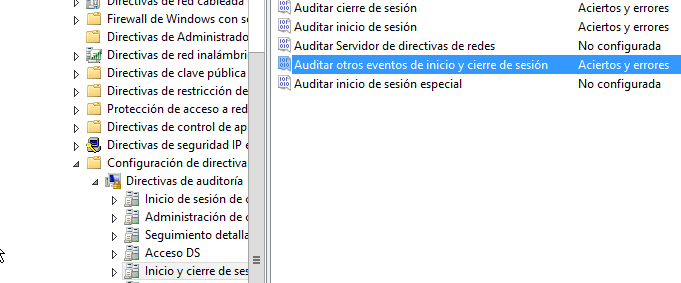
shutdown /r /d p:2:5 /c "Aplicación: inestable"

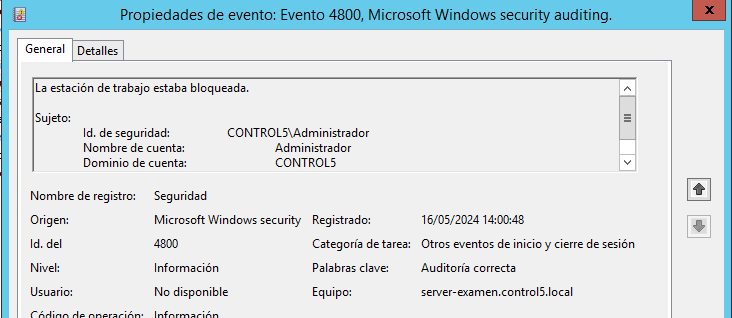
1. **A continuación, bloquea la sesión actual (Ctrl+Alt+Supr)**

Para realizar esta configuración, primero deberemos configurar la auditoría para poder ver los cambios realizados en la auditoría avanzada, para ello activaremos la siguiente directiva

****

**Y una vez hecho esto, actualizaremos las dos siguiente directivas**





1. **Desbloquea la sesión, y localiza en el evento el cierre e inicio de sesión relacionados con este bloqueo. ¿Qué valor numérico asigna Windows al campo “Tipo de inicio de sesión”.**

El valor numérico es 7

**Compara este valor con el indicado en la página web del enlace**[**https://docs.microsoft.com/es-es/windows/security/threat-protection/auditing/basic-audit-logon-events**](https://docs.microsoft.com/es-es/windows/security/threat-protection/auditing/basic-audit-logon-events)

**¿Tiene sentido? Razona la respuesta.**

