Creación de un entorno basado en grupo de trabajo en Windows.

Creación de instancias para un entorno Windows
Crear las siguientes instancias en el Cloud, en el proyecto individual de cada alumno, con las siguientes características:

> Instancia de Windows 7 basada en la imagen *Windows 7 Enterprise 64 bits Activado*, de Server name W7, con Flavor m1.tiny
>
> Instancia de Windows 7 basada en la imagen *Windows 7 Enterprise 64 bits Activado*, de Server name W7T, con Flavor m1.tiny.
>
> Instancia de Windows XP basada en la imagen *Windows XP sin Firewall*, de Server name WXP, con Flavor m1.tiny.

Para las instancias Windows 7 tienen como usuario: *Administrador*, password: *asd.123*.
Para la instancia XP tiene como usuario: *Administrador*, password: *usuario*.

Modificación de una de las instancia de Windows 7.
Como las máquinas con Windows 7 de nuestro entorno de trabajo son idénticas, tendrán por tanto idéntico SID (Security IDentifier), es por ello que necesitamos cambiarlo.
Para ello necesitamos descargar en la máquina de Server name W7T las systinternals suite. Guardaremos esta suite en c:\software. En concreto necesitamos la aplicación PsGetSid. PsGetSid es una aplicación que deberemos ejecutar desde la línea de comandos. Deberemos copiar la salida del comando en un fichero de texto que guardaremos en la carpeta c:\antiguo\SID.txt.
Para cambiar el SID de W7T, necesitamos la aplicación sysprep, que ya viene por defecto en Windows 7, aplicaremos la opción: Acción de limpieza del sistema, iniciar configuración rápida y marcaremos la casilla Generalizar. Realizadas estas acciones se nos reinicializará la máquina con un nuevo SID. Copiaremos este nuevo SID en c:\antiguo\SIDnuevo.txt y comprobaremos que realmente tenemos uno nuevo. Lamentablemente el periodo de activación se reduce en días.

Configuración del entorno de trabajo.
Las tres instancias deben pertenecer al mismo grupo de trabajo WORKGROUP.

Las tres instancias deben tener las actualizaciones automáticas desactivadas.

Las tres instancias deben tener el usuario *admin*, que pertenecerá al grupo de administradores y tendrá como password: *asd.123*.

Las tres instancias deberán sincronizar sus relojes con el servidor SNTP *papion.gonzalonazareno.org*.

La instancia XP deberá tener la Directiva de seguridad local: *Acceso de red: modelo de seguridad y para compartir para cuentas locales* en Modo Clásico.

La instancia W7T, deberá compartir su carpeta c:\software para que las máquinas del WORKGROUP puedan acceder, pero únicamente los administradores.

Comprobación de que el testigo de acceso filtrado deja sin ningún privilegio de manera predeterminada a un administrador.
Para ello se creará un fichero con permisos de control total para el grupo de administradores locales de la máquina. El fichero se llamará *pruebapermisos.txt*. De esta forma los miembros pertenecientes al grupo tendrán control total sobre el fichero.

Agregamos el usuario *admin1* al grupo de administradores locales de la máquina. Deberá tener como contraseña la misma que el resto de administradores, es decir *asd.123*. Ahora intentar eliminar el fichero *pruebapermisos.txt* como admin1. ¿Qué ocurre?, ¿cómo deberías proceder para poder eliminarlo?.

Si en una consola y como admin1 ejecutas *whoami /all*, ¿que te está indicando la línea de BUILTIN\administrators?. Razona la respuesta.

Estudio de la propiedad requestedExecutionLevel de ficheros Manifest
Mediante la aplicación *sigcheck* visualiza el contenido del fichero Manifest asociado a los ficheros ejecutables de c:\windows\system32.
¿Que valores puede tener la propiedad requestedExecutionLevel y cuales son sus significados?.
Ejemplos :

```
sigcheck.exe -m c:\windows\system32\notepad.exe
strings.exe *.exe | findstr -i "Propiedad requestedExecutionLevel"
```

Copiar y cortar ficheros en sistemas NTFS.
La copia de ficheros necesita el permiso de lectura en origen y el de escritura en el destino. El cortar necesita además el de modificación en el directorio origen.

Si la copia o el cortado y pegado se produce en un sistema de ficheros NTFS diferente, el fichero o directorio heredan los permisos del directorio padre destino.

Si se copia y se pega, dentro del mismo sistema de ficheros NTFS el fichero hereda los permisos del directorio destino. En caso de cortado y pegado dentro del un mismo sistema de ficheros NTFS los permisos situados en origen se mantienen.

Prueba estas aseveraciones, y di si son ciertas.

Recursos compartidos *C$* y *ADMIN$*
Desde W7 conéctate a los recursos compartidos C$ y ADMIN$ de W7T y WXP.

¿Qué conseguimos con estas acciones?. Haz pruebas con la herramienta administrativas *administrador de equipos*. ¿Es posible controlar los servicios de las máquinas remotas, los recursos compartidos y las cuentas de usuario?. ¿Dónde se ejecuta la aplicación de administrador de equipos?, en la máquina desde donde la ejecutamos o en la máquina remota. ¿Cómo puede saberlo?.

¿Cómo podrías mejorar la seguridad de las máquinas controladas?.