EJERCICIOS

TEMA 4: WINDOWS 10Windows 10. PARTE II

Consideraciones previas

La documentación a entregar será **un único fichero pdf** con las **capturas de pantalla** de los puntos indicados en cada práctica.

Preparación Máquinas virtuales

En esta práctica vamos a necesitar 2 máquinas virtuales para poder conectarlas en la misma red y trabajar con recursos compartidos.

Para crearlas, en lugar de hacer dos instalaciones, quiero que conozcáis una herramienta llamada **sysprep**. Este comando es una utilidad que se encuentra en *C:\Windows\System32\sysprep* llamada **herramienta de preparación del sistema** y que se ejecuta una vez instalado el sistema, configurado e instalado el software necesario.

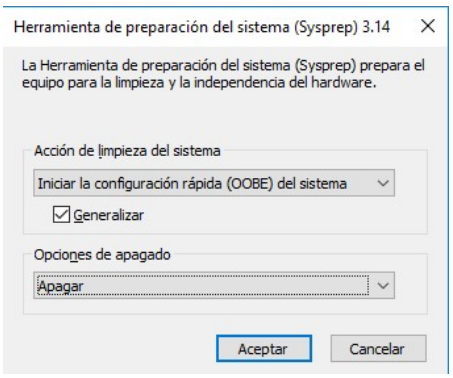
Sysprep prepara una instalación de Windows para la duplicación, permitiendo capturar una imagen de Windows personalizada que se puede usar varias veces en una organización. El modo auditoría permite agregar controladores de dispositivos o aplicaciones adicionales a una instalación de Windows.

Si se pretende transferir una imagen de Windows a un equipo distinto, se debe ejecutar *sysprep /generalize*, incluso aunque el equipo tenga la misma configuración de hardware. El comando *sysprep /generalize* elimina información única de la instalación de Windows que permite reutilizar la imagen en distintos equipos. La próxima vez que se inicie la imagen de Windows, se ejecuta el ciclo de configuración *specialize*. Durante este ciclo de configuración, muchos componentes tienen acciones que se deben procesar cuando se inicia una imagen de Windows en un equipo nuevo. Cualquier método de traslado de una imagen de Windows a un equipo nuevo, bien mediante creación de imagen, duplicación de disco duro u otro método debe prepararse mediante el comando *sysprep /generalize*.

Una vez arrancado el equipo con la nueva imagen se finaliza el proceso de instalación de Windows, solicitando usuarios, nombres de equipo, etcétera.

PRÁCTICA 0. Preparación de las máquinas

1. Crea una máquina virtual llamada W10_1. Configúrala según las características de tu equipo. Ten en cuenta que vamos a trabajar con 2 máquinas virtuales arrancadas al mismo tiempo, así que no te excedas en los recursos que le asignas.
2. Instala el SO Windows 10 Education. No introduzcas la clave del producto.
3. Durante la creación nos pedirá un nombre de usuario y contraseña. Puedes ponerle el que quieras, pero no pongas **Alumno** que será el que después crearemos. Después se quedará en el sistema con privilegios de Administrador.
4. Este sería el momento de instalar todo el software que nos gustaría incluir en la imagen del sistema. Nosotros sólo ponemos las Guest Additions.
   Una vez instalado el SO, instala las Guest Additions y reinicia la máquina virtual.
5. Entra en W10_1 con el usuario creado durante la instalación (tiene privilegios de Administrador).
6. En el menú contextual del botón Inicio selecciona la opción **Símbolo del Sistema (Administrador)**.
7. Cámbiate al directorio C:\Windows\System32\Sysprep
8. Ejecuta el comando
   > sysprep /generalize
9. Selecciona en el cuadro de diálogo **Iniciar la configuración rápida (OOBE) del sistema** y marca la opción **Generalizar**. Y en opciones de apagado selecciona **Apagar**.



10. Al finalizar el proceso de generalización la máquina se apaga automáticamente.
11. Entra en el administrador de medios virtuales de VirtualBox y copia el disco duro W10_1.vdi a W10_2.vdi
12. Crea una nueva máquina virtual llamada W10_2. El disco duro de esta máquina será el disco W10_2.vdi creado en el punto anterior.
13. A partir de este momento, cuando arranquemos cualquiera de estas 2 máquinas, comenzará el último paso del proceso de instalación de Windows 10. Deberemos introducir usuario, configuración de red, idioma, clave del producto, etc. La ventaja es que ya tendremos instalado el software base que hayamos preinstalado antes del sysprep.
14. Arranca las 2 máquinas virtuales y finaliza el proceso de instalación. En usuario, pon en ambas **Alumno** y contraseña **alumno**
15. En ambas máquinas cambia el nombre del equipo y pon respectivamente W10_1 y W10_2.

Las máquinas ya deberían tener las Guest Additions instaladas, pues se instalaron antes de hacer el *sysprep*.

PRÁCTICA 1. Perfiles de usuario

Para entregar, captura la pantalla durante el punto 13.

1. Arranca la máquina virtual W10_1.
2. Entra con el usuario **Alumno** (tiene privilegios de Administrador).
3. Cambia la opción en el Explorador de Archivos para que se vean siempre las extensiones de los ficheros. Acostúmbrate a trabajar así.
4. Desde la consola de **administración de equipos** crea un usuario llamado ***usr1*** la contraseña será *usr1* la cual no caducará y no deberá cambiar al inicio de su sesión. El usuario será miembro del grupo existente *Usuarios*.
5. Abre el explorador de Windows y comprueba que en la carpeta **\Users** aún no se ha creado la carpeta correspondiente al usuario **usr1**.
6. En la misma carpeta **\Users** hay una carpeta oculta llamada **Default**. Entra en esa carpeta y crea dentro una nueva carpeta llamada **Películas**. La carpeta *Default* es

la que contiene el perfil de usuario por defecto sobre el cual se crearán los nuevos perfiles de usuario.

7. Cierra sesión
8. Abre sesión como el usuario **usr1**. Fíjate que el primer inicio de sesión siempre es más costoso, pues está creando el perfil de usuario.
9. Abre el explorador de Windows y comprueba que ya se ha creado la carpeta personal del usuario usr1. Además de *Documentos, Imágenes*, etc, debe incluir una carpeta llamada *Películas*.
10. Entra en la carpeta **Documentos** y crea con el botón secundario del ratón un nuevo fichero de texto. Llámalo como quieras y escribe algo dentro de él.
11. Cierra sesión.
12. Abre sesión con el usuario **Alumno** (el administrador).
13. **Vamos a eliminar el usuario creado. Siempre que vayamos a crear usuarios o eliminarlos o modificarlos, lo haremos desde la consola de administración de equipos. Esta vez lo vamos a hacer desde el panel de control. Accede al Panel de Control, Cuentas de Usuario. Elimina la cuenta usr1, pero conservando los archivos.**
14. Comprueba que hay una carpeta nueva en tu escritorio. Entra y revisa qué es lo que hay y qué no hay en ella.

PRÁCTICA 2. Usuarios y grupos

Para entregar, captura la pantalla durante los puntos 17 y 25.

15. Configura el sistema para que la longitud mínima de las contraseñas sean 5 caracteres.
16. Del mismo modo, el sistema debe guardar un historial de 2 contraseñas para cada usuario, de manera que no pueda poner 2 veces consecutivas la misma contraseña.
17. **Habilita que se bloqueen las cuentas después de 3 intentos no válidos de poner la contraseña.**
18. Desde la consola de administración de equipos, crea los siguientes 4 usuarios (las contraseñas son las que hay entre paréntesis):

1. adm11 (adm11).
2. adm12 (adm12).
3. usr11 (usr11).
4. usr12 (usr). No debería dejarte poner esa contraseña. Pon usr12

19. Los usuarios admXX serán administradores. Deben pertenecer por tanto al grupo *Administradores*.
20. Los usuarios usrXX serán usuarios restringidos (usuarios normales).
21. Crea un grupo llamado ***Buenos*** y otro grupo llamado ***Malos***.
22. Los usuarios **adm12** y **usr12** pertenecerán al grupo ***Malos*** y el usuario **usr11** y **adm11** pertenecerá al grupo ***Buenos***.
23. Cierra sesión.
24. Intenta abrir sesión con el usuario **adm11**, pero equivócate 3 veces en la contraseña. Se debe bloquear la cuenta.
25. **Entra al sistema como *Alumno* (administrador) y desbloquea la cuenta desde la ficha del usuario (pestaña General).**

PRÁCTICA 3. Permisos

Para entregar, captura la pantalla durante los puntos 37 y 42.

26. Estando como el usuario *Alumno* (administrador) crea una carpeta en la raíz (C:\) llamada **Docs**
27. Dentro de la carpeta crea un archivo de texto llamado **Nombre.txt**
28. En los permisos de la carpeta modifica lo necesario para que el usuario **Alumno** (el propietario de la carpeta) tenga Control Total.
29. Elimina los permisos de *Usuarios Autentificados, System, Administradores* y *Usuarios*. Son permisos heredados, hay que tenerlo en cuenta para poder eliminarlos.
30. Permite que el grupo *Buenos* tenga permisos de **Control Total.**
31. Cierra sesión y entra como el usuario *adm12*.
32. El usuario *adm12* es administrador pero pertenece al grupo *malos*. Si todo ha ido bien no debe poder acceder a la carpeta. Aunque no se ha denegado explícitamente, no se le han dado permisos. Compruébalo.

33. Cierra sesión y entra como el usuario *usr11*.
34. El usuario *usr11* no es administrador pero pertenece al grupo *buenos*. Si todo ha ido bien debe poder acceder a la carpeta y escribir algo en ella. Compruébalo.
35. Cierra sesión y entra como el usuario *Alumno*.
36. Crea una carpeta llamada **Pública** dentro de **Docs**.
37. **Configura la carpeta Pública para que el grupo Todos** (un grupo del sistema que engloba a todos los usuarios dados de alta) **puedan tener acceso de Control Total a la carpeta, excepto el usuario *usr11* que no tendrá ningún tipo de acceso. Hazlo todo sin cambiar los permisos de Docs. Haz varias capturas de pantalla.**
38. Cierra sesión y entra como el usuario *adm12*.
39. Este usuario debería poder entrar en la carpeta llamada **Pública**, pero al encontrase dentro de **Docs** (que no tiene acceso) no puede navegar hasta ella desde el explorador de Windows. Compruébalo.
40. Para poder entrar en la carpeta **Pública** deberás teclear la ruta absoluta de dicha carpeta en la barra de direcciones del explorador de ficheros de Windows.
41. Comprueba que *adm12* sí puede entrar y grabar ficheros en dicha carpeta utilizando esta ruta absoluta.
42. **Ahora, aprovechando que el usuario *adm12* es administrador, y aunque no tenga permisos sobre la carpeta Docs, vamos a acceder a las propiedades de seguridad de dicha carpeta y vamos a determinar que el nuevo propietario de la carpeta es el usuario *adm12* (esto lo podemos hacer por ser administrador)**.
43. Cerramos las propiedades y las volvemos a abrir para que surtan efecto los cambios.
44. Veremos que ahora podemos cambiar los permisos y permitir o denegar el acceso desde el usuario *adm12*.

PRÁCTICA 4. Gestión de Procesos

Para entregar, captura la pantalla durante el punto 47.

45. Cierra sesión y entra con el usuario *Alumno* (administrador).

46. Ejecuta el Notepad (bloc de notas). No lo cierres. Ejecuta la calculadora. No la cierres.
47. **Ve al administrador de tareas, en la pestaña de detalles selecciona las columnas siguientes a visualizar: PID, Uso de CPU, Tiempo de CPU, Uso de Memoria y Prioridad Base.**
48. Finaliza desde el administrador de procesos los 2 programas lanzados a ejecución (calculadora y notepad).
49. Cierra el administrador de tareas.

PRÁCTICA 5. Instalación de programas y gestión de servicios

Para entregar, captura la pantalla durante el punto 53.

50. Crea en el escritorio una nueva consola de administración con los siguientes complementos:
    1. Servicios.
    2. Usuarios y Grupos Locales.
    3. Carpetas Compartidas.
51. Ve a la pantalla donde aparecen todos los servicios y comprueba que en Windows 10 no aparece el servicio FTP de Microsoft (el servidor de FTP). Este protocolo se utiliza para la transferencia de archivos. Es posible configurar nuestro equipo como un servidor FTP.
52. En el panel de control, ve a *Programas* → *Activar Características de Windows* y Activa el **Servidor FTP** (se encuentra dentro de Internet Information Services)
53. **Ya debe aparecer el servicio del servidor FTP. Arranca el servicio *FTP* y configúralo para que se inicie unos minutos después de cada vez que se arranque el equipo.**

PRÁCTICA 6. Compartición de datos

Para entregar, captura la pantalla durante los puntos 71 y 73.

54. Cambia los adaptadores de red de las máquinas virtuales W10_1 y W10_2 para que estén en modo puente.
55. Arranca las 2 máquinas virtuales, W10_1 y W10_2.
56. Accede a ambas con el usuario *Alumno* (administrador).
57. Incluye la máquina W10_1 en el grupo de trabajo BigBang
58. Incluye la máquina W10_2 en el grupo de trabajo BigBang
59. Abre el intérprete de comandos
60. Asegúrate que se ven mediante un ping entre ambas máquinas. Es posible (seguro) que tengas que desactivar el firewall de ambas máquinas.
61. En ambas máquinas cambia la opción de carpeta del Explorador de Ficheros para no utilizar el asistente para compartir.
62. En W10_1 crea en C: una carpeta llamada Datos1 y la compartes.
63. En W10_2 crea en C: una carpeta llamada Datos2 y la compartes.
64. Crea en la máquina W10_2 los siguientes usuarios (contraseñas):
    1. adm21 (adm21)
    2. adm12 (adm12). (Fíjate que ya existe uno igual en W10_1)
    3. usr21 (usr21)
    4. usr12 (usr12). (Fíjate que ya existe uno igual en W10_1)
65. Los usuarios admXX serán administradores.
66. Los usuarios usrXX serán usuarios restringidos.
67. Crea en W10_2 un grupo llamado Buenos y otro grupo llamado Malos.
68. Los usuarios adm12 y usr21 pertenecerán al grupo Malos y el usuario usr12 y adm21 pertenecerá al grupo Buenos.
69. Cierra sesión en W10_1 y entra con el usuario adm11.
70. Cierra sesión en W10_2 y entra con el usuario adm21.
71. **Desde W10_2 Entra en RED y comprueba que se ve el equipo W10_1**
72. Intenta acceder desde W10_2 a W10_1. Al no existir el usuario adm21 en la máquina W10_1 nos debe pedir credenciales. No las pongas. Cancela.
73. **Para que no pida credenciales, en W10_2, mediante Administrar Credenciales del Panel de Control, guarda la contraseña del usuario adm11.**
74. Intenta acceder a W10_1. Ahora, aunque no exista el usuario adm21 en la máquina W10_1 **no** nos debe pedir credenciales pues estamos conectados a W10_1 con el usuario adm11.

75. En la máquina W10_2 accede al Panel de Control, Herramientas administrativas, **Directivas de seguridad local**.
76. Dentro de la **Configuración de Seguridad**, accede a **Directivas Locales**, **Opciones de Seguridad**.
77. Modifica la directiva **Acceso a Redes: Modelo de seguridad y uso compartido para cuentas locales** y déjalo como **Sólo Invitado**
78. Accede desde la máquina W10_1 a W10_2
79. Al cambiar la directiva, el acceso a W10_2 se realizará como si lo hiciera la cuenta Invitado.
80. Lo normal es que en W10_2 la cuenta Invitado esté desactivada, con lo que se produciría la circunstancia que nadie podría validarse para entrar en esa máquina por red (sólo estamos permitiendo la entrada por red a Invitado y esta cuenta está desactivada).
81. Vuelve a dejar la directiva de W10_2 como estaba.

PRÁCTICA 7. Permisos de red

Para entregar, captura la pantalla durante los puntos 84 y 91.

82. En la máquina W10_2 (entra como el usuario adm21) crea una carpeta en la raíz (C:\) llamada **Datos**
83. Dentro de la carpeta crea un archivo de texto llamado **Nombre.txt**
84. **Comparte la carpeta. Asigna permisos de red de Escritura para TODOS.**
85. En los permisos NTFS permite que el grupo *Buenos* tenga permisos de Control Total y el grupo *Malos* no tenga permisos de lectura ni de escritura.
86. En la máquina W10_1 entra como el usuario adm12.
87. El usuario adm12 es en ambas máquinas administrador pero en W10_2 pertenece al grupo *malos*. Si todo ha ido bien no debe poder acceder a la carpeta. Compruébalo.
88. En W10_2 crea una carpeta llamada **Pública** dentro de **Datos**.
89. Configura la carpeta **Pública** para que todos puedan tener acceso a la carpeta sin cambiar los permisos de **Datos**. No la compartas.
90. En W10_1 comprueba que se puede entrar a esa carpeta.

91. **Crea en W10_1 una unidad de red vinculada a la carpeta Pública con la letra X:**
92. Accede al **Equipo** y comprueba que aparece la nueva unidad.

PRÁCTICA 8. Recursos compartidos

Para entregar, captura la pantalla durante los puntos 95 y 100.

93. Accede desde W10_1 con un usuario válido al fichero **nombre.txt** de la carpeta **Datos** que hay en W10_2
94. En W10_2 accede a la consola de Administración de Equipos
95. **Comprueba los Archivos Abiertos de las carpetas compartidas.**
96. Desde la consola, cierra la sesión abierta desde W10_1
97. En W10_2 crea una carpeta en la Raíz de C: llamada **Oculta**
98. Desde la consola de Administración de Equipos, dentro de los recursos compartidos, crea un nuevo recurso para compartir la carpeta Oculta. Cuando pida el nombre del recurso, pondremos Oculta$ (terminada en dólar). De esta manera no se mostrará, pero estará accesible.
99. En la máquina W10_1 accede a Red y entra en W10_2. No debe aparecer la carpeta Oculta.
100. **En la barra de direcciones, añade a la ruta el nombre de la carpeta Oculta$ y ya se puede acceder.**

PRÁCTICA 9. Escritorio Remoto

Para entregar, captura la pantalla durante el punto 101.

101. **Desde la máquina W10_1 inicia una sesión de escritorio remoto en W10_2.**

PRÁCTICA 10. Cifrado de unidades con Bitlocker

El Cifrado de unidad BitLocker es una característica de seguridad integral del sistema operativo Windows 10 que ayuda a proteger los datos almacenados en unidades de datos fijas y extraíbles y en la unidad del sistema operativo. BitLocker protege de "ataques sin conexión", que son aquéllos que se realizan deshabilitando o evitando el sistema operativo instalado, o bien, quitando físicamente el disco duro para atacar los datos por separado. En el caso de las unidades de datos fijas y extraíbles, BitLocker ayuda a garantizar que los usuarios pueden leer y escribir datos en la unidad solo cuando cuentan con la contraseña correspondiente, con credenciales de tarjeta inteligente o cuando usan la unidad de datos en un equipo protegido con BitLocker que tenga las claves adecuadas.

La protección de BitLocker en unidades del sistema operativo admite la autenticación de dos factores mediante el uso del Módulo de plataforma segura (TPM, chip especial de cifrado que se encuentra en la placa base) junto con un número de identificación personal (PIN) o clave de inicio, así como la autenticación de un solo factor mediante el almacenamiento de una clave en una unidad flash USB o mediante el uso solo del TPM. El uso de BitLocker con un TPM proporciona una mayor protección a los datos y ayuda a garantizar la integridad del componente de arranque inicial. Esta opción requiere que el equipo disponga de un microchip de TPM y una BIOS compatibles.

Para entregar, captura la pantalla durante el punto 128.

PASO 1. Adición nuevo disco duro a la máquina virtual.

102. Con la máquina virtual W10_1 apagada crea un nuevo disco duro virtual SATA de 1 GB. Lo llamarás **Datos.vdi**. (Importante que para esta prueba no ocupe mucho el disco duro).
103. Introduce una unidad de USB en la máquina anfitrión.
104. Crear un nuevo filtro de USB en la MV para que la reconozca.
105. Arranca la máquina.
106. Desde el administrador de discos formatea el nuevo disco duro. Para ello seleccionaremos el disco del tipo MBR y crearemos un Nuevo Volumen Simple en el disco. Finalmente se formateará como NTFS.

107. Después de unos segundos acabará el formateo y le aplicará la nueva letra a la unidad. Podemos cerrar el administrador de discos.
108. Crea 2 carpetas llamadas Apuntes y Mis Datos en la raíz de la nueva unidad de disco.
109. Pon algún fichero dentro de las nuevas carpetas.
110. Asegúrate que se ve la unidad USB en la máquina virtual.

PASO 2. Configurar BitLocker.

111. Para que BitLocker funcione necesita copiar la clave maestra en una unidad externa. O bien lo hace en un chip TPM o en una unidad USB flash externa. En nuestro caso lo haremos en la unidad USB.
112. En versiones anteriores a Windows 10, para poder almacenar la clave maestra en la unidad USB había que cambiar una directiva de grupo. En principio en Windows 10 no nos va a hacer falta. Los siguientes puntos no son necesarios ejecutarlos en Windows 10.
113. Ejecutamos la consola gpedit.msc para acceder a las directivas de grupo.
114. Accedemos a Directivas equipo local → Configuración de Equipo → Plantillas Administrativas → Componentes de Windows → Cifrado de Unidad Bitlocker → Unidades del SO → Requerir Autenticación Adicional
115. Configuramos la directiva para *Activarla* y ver que *Permitir Bitlocker sin un TPM compatible* está marcado.
116. Cerramos la consola de las directivas de grupo.

PASO 3. Activando BitLocker

117. Desde el equipo, con el botón derecho del ratón (menú contextual) Activa Bitlocker en la nueva unidad de disco duro.
118. Nos aparece un nuevo asistente de cifrado.
119. Seleccionamos la primera opción: Usar contraseña para cifrar unidad.
120. La contraseña debe cumplir los requerimientos de seguridad (mayúsculas, minúsculas, números, longitud, …). Pondremos como contraseña *Valencia1*
121. Seleccionamos Guardar la clave de recuperación en una unidad flash.
122. Nos solicita si deseamos cifrar la unidad entera o solamente los datos. Esto es importante, porque si seleccionamos la unidad entera, aunque esté vacía, cifrará

igualmente los espacios en blanco. Por eso os he pedido que el disco virtual no ocupara mucho, pues si éste era de almacenamiento dinámico, lo cifrará en su totalidad, apareciendo el disco virtual como si estuviera lleno, es decir, el fichero vdi ocupará el máximo aunque esté vacío en su mayor parte. Para ir más rápidos, seleccionamos la primera opción.

123. Nos pide a continuación que seleccionemos el modo de cifrado, el nuevo de Windows 10 o el compatible con versiones anteriores.
124. La unidad está cifrada. Si conectamos ese disco duro a otra máquina no debemos poder tener acceso a los datos.
125. Reinicia la máquina y comprueba que es necesaria la contraseña para poder acceder a los datos de este disco.
126. Apaga la máquina y desconecta el disco de W10_1 y pínchalo en W10_2.
127. Arranca la máquina W10_2 y accede a la unidad.
128. **Captura la pantalla cuando te solicite la contraseña**
129. Si olvidáramos la clave de desbloqueo, podríamos recuperarla mediante la clave de recuperación almacenada en la unidad USB