



TRABAJO FINAL

[Cristian Barrientos Montoya](#)

Administración de usuarios y grupos en OpenSUSE:

Linux es un sistema multiusuario. Varios usuarios diferentes pueden iniciar sesión en el sistema a la vez. Para evitar confusiones, cada usuario debe tener una identidad exclusiva. Además, cada usuario debe pertenecer como mínimo a un grupo.

Usuarios y grupos:

Esta es la ventana de administración de Yast donde se puede visualizar información de los usuarios y hacer gestión completa sobre ellos.

Tienes la posibilidad de hacer las siguientes opciones:

Añadir: Permite agregar un nuevo usuario.

Editar: permite cambiar valores guardados para los usuarios.

Eliminar: permite eliminar la cuenta de los usuarios.

Los usuarios y grupos se organizan en conjuntos. Puede cambiar el conjunto que se muestra actualmente en la tabla con la opción Definir filtro. También puede personalizar su vista de filtros usando Personalizar filtro.

Haga clic en Opciones avanzadas para editar varios ajustes avanzados, tales como el tipo de cifrado, el método de autenticación, los valores por defecto para los usuarios nuevos o los ajustes de inicio de sesión. La opción Escribir cambios permite guardar todos los cambios hechos hasta el momento si salir del módulo de configuración.

Para guardar en el sistema los ajustes de los grupos y los usuarios modificados, haga clic en Terminar.

Opciones predeterminadas para nuevos usuarios

Defina aquí los valores predeterminados que se deben usar a la hora de crear usuarios nuevos locales o de sistema.

* Grupo predeterminado: El nombre del grupo principal de un usuario nuevo.

* Grupos secundarios: Nombres de los grupos adicionales a los que se asignarán usuarios nuevos.

* Shell de inicio de sesión predeterminada: El nombre de la shell de inicio de sesión de un nuevo usuario. Seleccione una de la lista o introduzca su propia ruta a la shell.

* Directorio personal por defecto: El prefijo de la ruta inicial para el directorio personal de un usuario nuevo. El nombre de usuario se añade al final de este valor para crear el nombre por defecto del directorio personal.

* Directorio esqueleto: El contenido de este directorio se copia en el directorio personal del usuario cuando se añade un usuario nuevo.

* Umask de directorio personal: umask utilizado al crear nuevos directorios personales.

* Fecha de expiración: La fecha en la que se deshabilitará la cuenta de usuario. La fecha debe tener el formato AAAA-MM-DD. Deje esta opción en blanco si la cuenta no debe caducar nunca.

* Validez del inicio de sesión (en días) tras caducar la contraseña: Los usuarios pueden iniciar sesión después de que las contraseñas hayan caducado. Establezca cuántos días después de la caducidad de la contraseña se puede iniciar sesión. Use -1 para permitir un acceso ilimitado.

Configuración de autenticación

* Resumen de la configuración: Aquí puede ver un resumen de los módulos que podrían afectar a las fuentes de las cuentas de usuario o al tipo de autenticación.

* Cambiar de valores: Puede configurar estos ajustes ejecutando los módulos adecuados. Seleccione el módulo con la opción Configurar.

Configuración del cliente NIS Introduzca el dominio NIS (p. ej. ejemplo.com) y la dirección del servidor NIS (p. ej. nis.ejemplo.com o bien 10.20.1.1).

Seleccione el modo en que la configuración de NIS será modificada. Normalmente, esto es realizado por el guión netconfig, que combina los datos definidos aquí estáticamente con aquellos datos obtenidos dinámicamente (p. ej.: de DHCP, NetworkManager, etc.). Esta es la directiva predeterminada y es suficiente para la mayoría de las configuraciones. Si escoge Sólo cambios manuales, netconfig no permitirá modificar la configuración. Sin embargo, usted podrá editar este archivo manualmente. Escogiendo Directiva personalizada, usted puede especificar una línea de valores personalizados que consiste de una lista, separada por espacios, de nombres de interfaces, incluyendo caracteres comodín, con los valores predefinidos STATIC y STATIC_FALLBACK. Para más información lea la página del manual de netconfig.

Puede especificar múltiples servidores separando sus direcciones con espacios.

La opción Difusión permite buscar un servidor en la red local si los servidores especificados en un principio no responden. Implica un riesgo de seguridad.

Automounter es un demonio que monta directorios automáticamente, como por ejemplo los directorios locales de los usuarios. Se asume que sus archivos de configuración (auto.*) ya existen, ya sea localmente o mediante NIS.

Las configuraciones de NFS las cuales afectan cómo opera el automounter podrían ser configuradas en el Cliente NFS, que pueden ser configuradas utilizando el botón Configuración de NFS.

En Configuración de los cortafuegos active Puerto abierto en los cortafuegos para abrir los cortafuegos y permitir el acceso al servicio 'ypbind' desde equipos remotos. Para seleccionar las

interfaces en las que desea abrir el puerto, pulse Detalles de los cortafuegos. Esta opción sólo está disponible si el cortafuego está activado.

Configuración del cliente LDAPConfigure su equipo como cliente LDAP.

Seleccione Usar LDAP para autenticar a los usuarios con un servidor OpenLDAP. NSS y PAM serán configurados en consecuencia.

Para desactivar los servicios LDAP, pulse No usar LDAP. Si desactiva LDAP, la entrada actual LDAP para contraseñas en `/etc/nsswitch.conf` se eliminará. La configuración de PAM se modificará y se eliminará la entrada LDAP.

Para activar LDAP pero prohibir a los usuarios que inicien sesión en este equipo, seleccione Usar LDAP pero inhabilitar inicios de sesión.

Seleccione Usar el System Security Services Daemon si desea que el sistema use SSSD en lugar de `nss_ldap`.

Escriba la dirección del servidor LDAP (p. ej. `ldap.ejemplo.com` o `10.20.0.2`) en el campo de las direcciones y el nombre completo de la base de búsqueda (DN base como, por ejemplo, `dc=ejemplo,dc=com`). Si especifica más de una dirección, sepárelas con espacios. Debe ser posible que las direcciones se puedan resolver sin usar LDAP. También puede especificar el puerto en el que se está ejecutando el servidor usando la sintaxis "servidor: puerto", por ejemplo, `ldap.ejemplo.com:379`.

Con Buscar puede seleccionar el servidor LDAP de la lista proporcionada por el protocolo de localización de servicios (SLP). La opción Obtener DN le permite leer el DN base del servidor.

Algunos Servidores LDAP soportan StartTLS (RFC2830). Si tu servidor lo soporta y está configurado, activa LDAP TLS/SSL para cifrar tu comunicación con el servidor LDAP. Debes descargar el archivo de certificado CA en formato PEM desde el enlace dado.

Para acceder a la configuración avanzada de LDAP, pulse Configuración Avanzada.

El automounter es un demonio que monta automáticamente directorios, como los directorios locales de usuario. Sus archivos de configuración (`auto.*`) deberían existir ya localmente o a través de LDAP. Si automounter no está instalado y desea usarlo, se instalará automáticamente.

Configuración del cliente KerberosLa configuración del cliente Kerberos actualiza los parámetros de PAM para permitir la autenticación mediante Kerberos. El sistema debe tener acceso a un servidor Kerberos de la red para que funcione. Configuración básica del cliente Introduzca su Dominio por defecto, el Dominio (Realm) por defecto y el nombre de host o la dirección del centro de distribución de claves (Dirección del servidor KDC). Puede agregar varios valores para KDC separados por espacios.

Es habitual poner el nombre del dominio en mayúsculas como nombre de dominio (realm) por defecto, pero queda a su elección. Si el dominio (realm) no está disponible en el servidor, no podrá iniciar sesión. Consulte al administrador del servidor si necesita más información.

Active Usar DNS para adquirir los datos de configuración en tiempo de ejecución para permitir a su cliente utilizar los datos de autenticación Kerberos proporcionados mediante DNS. Esta opción no se puede seleccionar si el servidor DNS no proporciona dichos datos. Para configurar más opciones, pulse Configuración avanzada.

Pertenencia a dominio de Windows (Samba) Un cliente Linux puede ser miembro de un grupo de trabajo, un dominio NT o un dominio de Active Directory. Especifique aquí el nombre del tipo de pertenencia.

Usar la información SMB para la autenticación de Linux permite verificar las contraseñas con el servidor NT o Kerberos al unirse a un dominio de AD.

Compruebe Cambiar sufijo de DNS primario para añadir su servidor AD en la lista de servidores de nombres. Esta opción sólo está disponible para configuraciones de redes estáticas.

Al pulsar sobre Aceptar, el sistema comprueba la pertenencia y, si es un dominio NT o Active Directory, permite a este equipo unirse a él.

Marque Crear directorio de usuario (home) al iniciar la sesión para crear el directorio local de usuario en el primer inicio de sesión.

Autenticación sin conexión permite al usuario iniciar una sesión aunque no haya ninguna conexión con el controlador de dominio. Para que esta opción funcione, deberá iniciar sesión en el dominio al menos una vez. Las credenciales del usuario se almacenan cifradas en el equipo y se reutilizan para un inicio de sesión de dominio cuando no se puede establecer una conexión con el controlador de dominio. Esto resulta especialmente útil para los usuarios móviles.

Seleccione Configuración avanzada para habilitar características avanzadas como WINS, o montar directorios personales del servidor desde dominios Active Directory.

Permitir a los usuarios compartir sus directorios permite que los miembros del grupo de Grupo permitido compartan los directorios que poseen con otros usuarios. Por ejemplo, los usuarios con ámbito local o los de Usuarios de DOMINIO\ para un ámbito de dominio. El usuario también debe comprobar que los permisos del sistema de archivos permiten el acceso.

Número máximo de recursos compartidos permite limitar la cantidad total de recursos compartidos que pueden crearse.

Para permitir el acceso a los recursos compartidos de los usuarios sin autenticación, active Permitir acceso de invitado.

Configure su sistema como cliente NTP para sincronizar la hora del sistema con la de un servidor NTP. Puede acceder a la configuración con Configuración de NTP.

UNIX

Es importante recalcar que opensuse al ser una distribución de Linux, maneja también la gestión de bajo nivel de UNIX, así que observemos éstas:

Hay tres tipos de cuentas en un sistema Unix:

1. Cuenta Root: Esta es también llama superUsuario y también tiene un control total sobre el sistema. Un superusuario puede ejecutar cualquier comando sin tener alguna restricción. Este usuario también puede ser asumido como el administrador del sistema.
2. Cuentas del sistema: Una cuenta del sistema es aquella necesitadas para hacer operaciones específicas sobre componentes del sistema, por ejemplo cuentas de correo o cuentas ssh. Estas cuentas son usualmente necesitadas para algunas funciones específicas dentro del sistema y cualquier modificación que hagan, afectará al sistema.
3. Cuentas de usuarios: Las cuentas de usuarios proveen interactividad en el acceso al sistema por medio de usuarios y grupos de usuarios. Usuarios generales son típicamente asignados a estas cuentas y estos usuarios poseen acceso limitado a los archivos del sistema y directorios críticos del mismo.

Unix soporta el concepto de cuenta de grupo que lógicamente agrupa un número de cuentas de usuario. Cada cuenta será parte de cualquier grupo. Los grupos de UNIX juegan papeles importantes manejando permisos de archivos y en la gestión de procesos.

Control de cuentas de usuarios y grupos en UNIX:

Hay 3 tipos principales de archivos de administración de usuarios:

1. `/etc/passwd`: Guarda la información de cuentas de usuario y contraseñas. Este archivos contiene la mayoría de información acerca de las cuentas en el sistema UNIX
2. `/etc/shadow`: Contiene las contraseñas encriptadas correspondientes a las cuentas. No todos los sistemas soportan este archivo.
3. `/etc/group`: Contiene la información de los grupos para cada cuenta
4. `/etc/gshadow`: Contiene información seguro hacer de los grupos de cuentas.

Se pueden comprobar todas la anteriores con el comando `cat`.

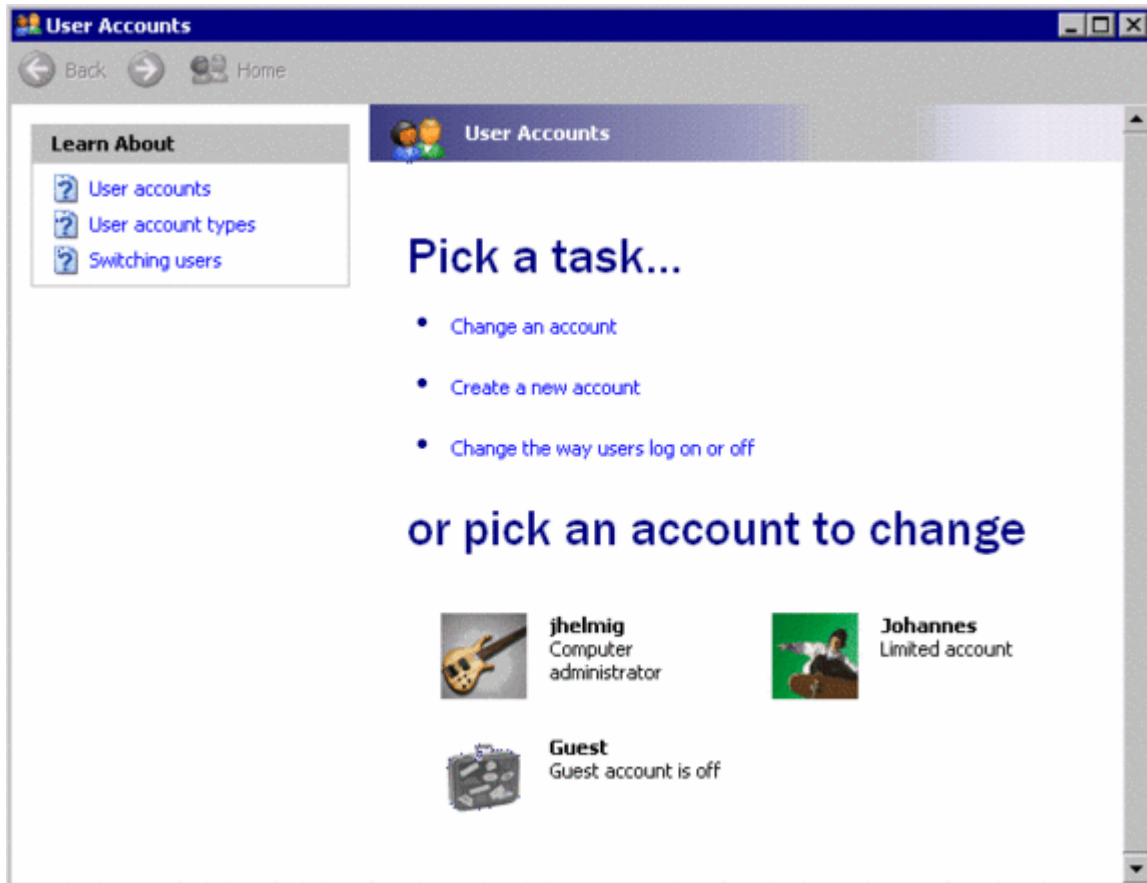
Los siguientes comandos están disponibles en la mayoría de los sistemas UNIX para crear y administrar cuentas de usuario y grupos.

| Comando | Descripción |
|----------|------------------------------------|
| Useradd | Agrega cuentas al sistema. |
| Usermod | Modifica atributos de las cuentas. |
| Userdel | Elimina cuentas del sistema |
| Groupadd | Agrega grupos al sistema |
| Groupmod | Modifica atributos de los grupos |
| groupdel | Elimina grupos de sistema. |

También se puede utilizar la ayuda de Manpage para una referencia completa de la sintaxis de los comandos mencionados.

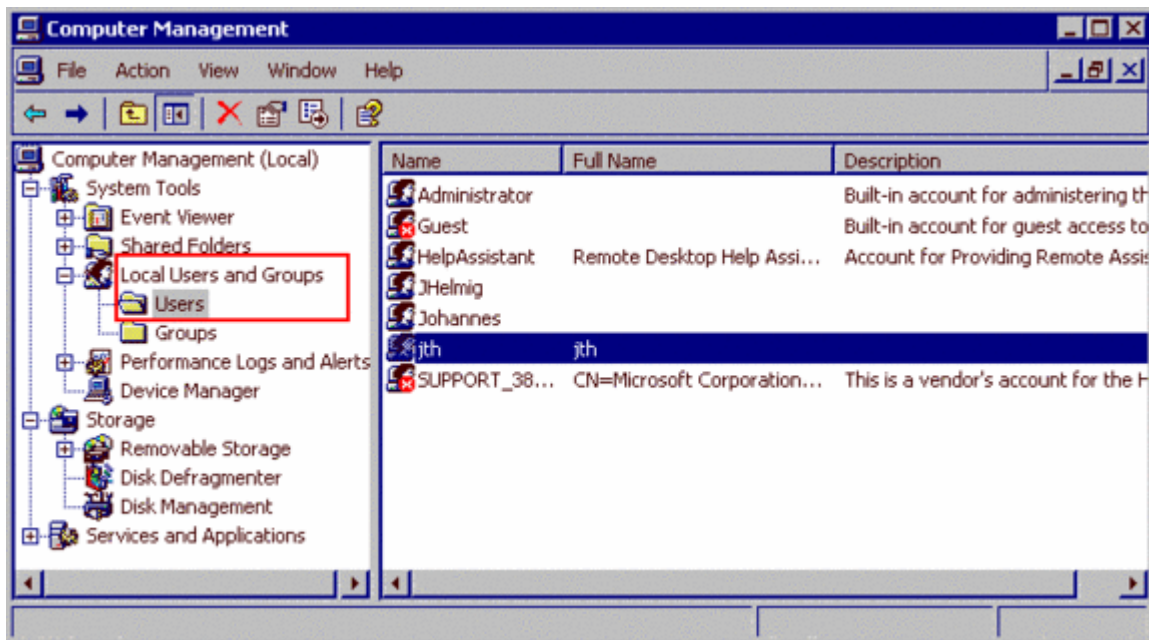
Windows XP

Windows xp ofrece la posibilidad de ser simple en este sentido y administrar el nivel de seguridad en solo 2 niveles en el panel de control: “Cuentas de usuario”:



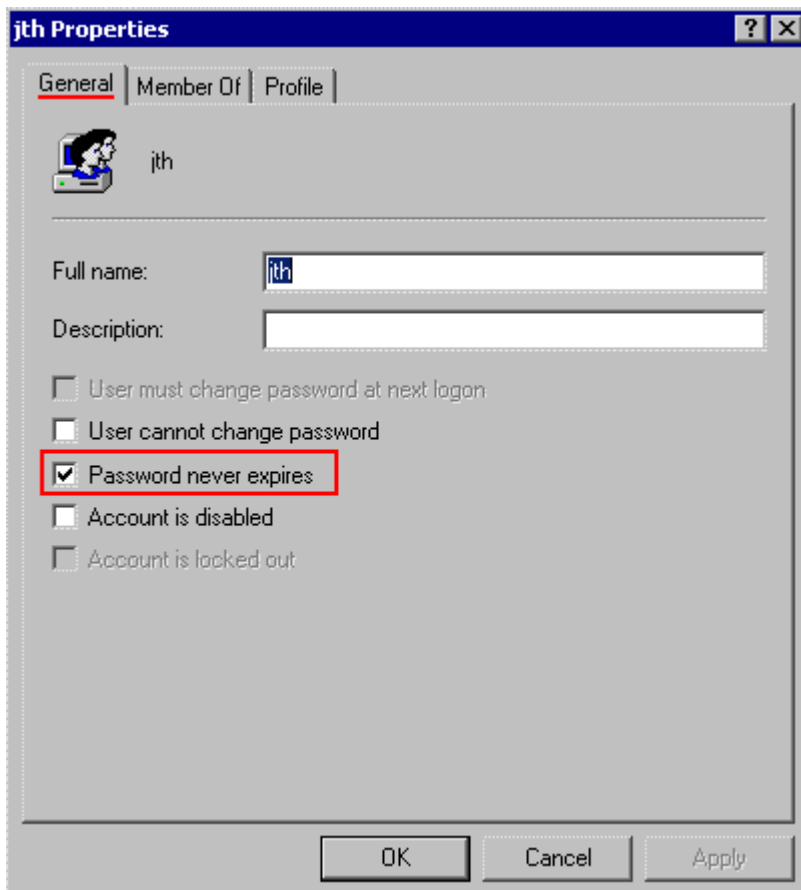
Esta es una manera simplificada de la administración de cuentas en Windows XP, permitiendo la definición de Usuarios y contraseñas.

Para tener la habilidad de usar la característica completa de administración de usuarios en Windows xp se debe ir a Panel de control y seleccionar: “Herramientas administrativas.”:



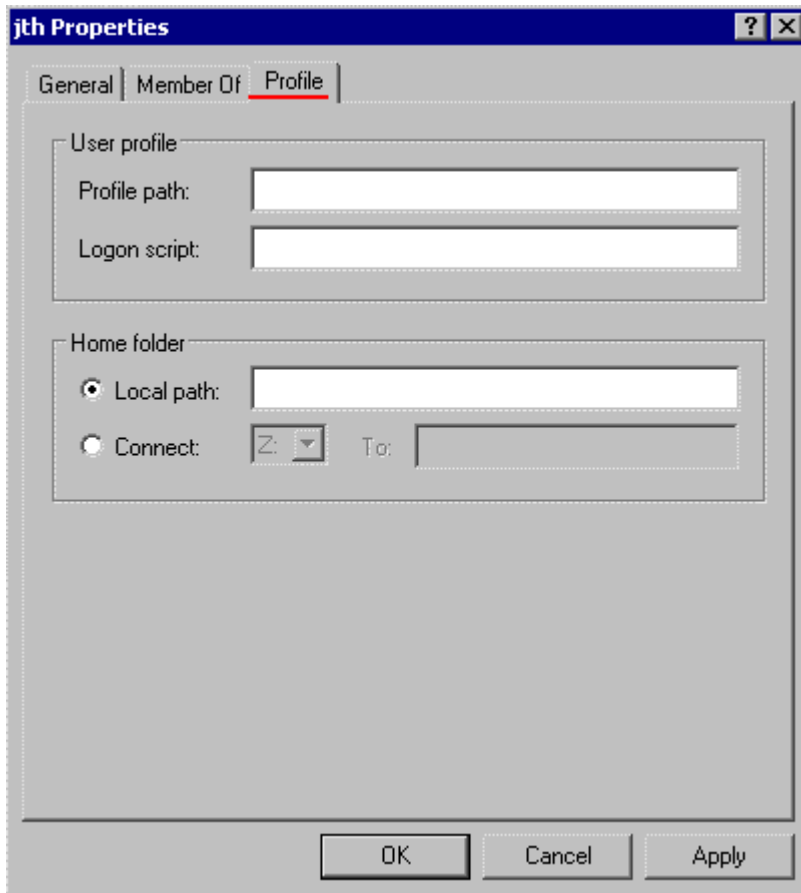
Administración de usuarios hace parte de “Administrador de computador”

Selección en la vista de la izquierda: “Herramientas del sistema / Usuarios locales y grupos / Usuarios”:

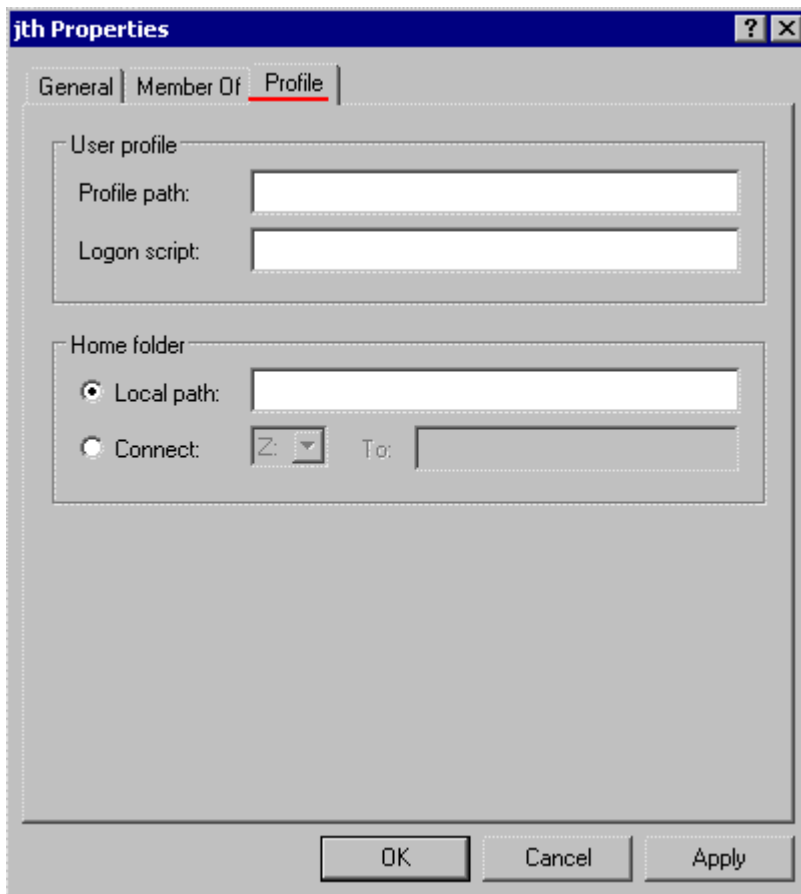


Doble clic en el nombre de la cuenta de usuario que se quiera editar y en la pestaña que dice: “General”: se encontraran todas las opciones de seguridad de Windows XP, tales como políticas de contraseña, entre otros.

En la pestaña de perfil: se pueden crear scripts (listas de comandos a ser ejecutados) cuando se ejecute un cierre de sesión en el sistema.



En la pestaña “Miembro de”: Cuando Windows XP es instalado, predefine un grupo de usuarios, cada uno con diferentes niveles de permisos, lo cual se instala sobre el sistema operativo. Por ser parte de un grupo de usuarios, un usuario tiene los permisos predefinidos por el grupo.



Un usuario puede ser miembro de múltiples grupos, obteniendo los permisos de cada grupo.

Todos los usuarios son automáticamente parte del grupo “Everyone” que no está listado en esta página, así que, si un usuario no hace parte de algún grupo de usuarios, este usuario todavía tiene los permisos de grupo “Everyone”.

SAM

El administrador de seguridad de cuentas (SAM) es una base de datos en un archivo, hace parte de Windows xp, Windows vista y Windows 7 que almacena las contraseñas de los usuarios. Puede ser usado para autenticar usuarios locales y remotamente. Empezando en Windows 2000 SP4, El directorio activo es usado para autenticar usuarios remotos. SAM usa medidas criptográficas para prevenir usuarios prohibidos ganar acceso al sistema.

Las contraseñas de los usuarios son almacenadas en un formato Hash por medio de un registro, ya sea como LM hash o como NTLM hash. Este archivo puede ser encontrado en **%SystemRoot%/system32/config/SAM** and is mounted on **HKLM/SAM**.

En un intento de mejorar la seguridad de la base de datos SAM contra Software offline de Crackeo, Microsoft introdujo la función SYSKEY en Windows NT 4.0. Cuando SYSKEY está activada, la copia en disco del archivo SAM está parcialmente encriptada, por lo que los valores de hash de contraseña para todas las cuentas locales almacenados en el SAM se cifran con una clave (por lo general también se refiere como el "SYSKEY"). Se puede activar mediante la ejecución del programa syskey

Windows 7

Cambio de la contraseña

Una contraseña segura debe incluir una combinación de letras, números y caracteres especiales.

La forma más sencilla de cambiar su contraseña cuando se está en el sistema es presionar Ctrl-Alt-Supr y haga clic en Cambiar la contraseña. En esta ventana, simplemente escriba su contraseña antigua y la nueva, y luego lo confirme. Los administradores también pueden sobrescribir el nombre de usuario y cambiar la contraseña de otro usuario.

Cambio de imagen

Windows 7 le permite elegir una imagen para asociar con su cuenta. Esta es la imagen que haga clic para iniciar sesión en el equipo. Para cambiarla, abra el Panel de control y seleccione Cuentas de usuarios. En Usuarios, haga clic en Cambiar tu cuenta de fotos. Puede seleccionar entre una serie de imágenes incorporadas, o usted puede navegar a una de sus propias imágenes.

Creación de un disco de restablecimiento de contraseña

Un disco de restablecimiento de contraseña es útil si usted olvida su contraseña, pero el problema es que tienes que crearlo mientras usted está en el sistema - si ya ha olvidado su contraseña, ya es demasiado tarde. Es probable que no tiene una unidad de disco en su PC, pero una unidad USB funcionará bien. Para crear un disco de restablecimiento de contraseña, Panel de control abierto y seleccione Cuentas de usuario y protección infantil, en Cuentas de usuario. Haga clic en Crear un disco de restablecimiento de contraseña en el panel izquierdo. Un asistente le guiará a través del procedimiento, pidiendo en qué unidad para colocar la llave de la contraseña, así como lo es su contraseña actual. Tenga cuidado donde se almacenan en el disco o unidad USB - cualquiera que pueda acceder a él puede utilizarlo para entrar en su cuenta.

Restablecimiento de la contraseña mediante el disco de restablecimiento de contraseña

Si introduce la contraseña incorrectamente cuando intenta iniciar sesión en el equipo, Windows mostrará un enlace Restablecer contraseña en el cuadro contraseña. Haga clic en él para iniciar el Asistente para restablecer una contraseña. Cuando se le solicite, seleccione la unidad que contiene la clave de contraseña y escriba una nueva contraseña y sugerencia de contraseña.

Uso de la herramienta "Usuarios y grupos locales"

Aunque el Windows 7 herramientas de gestión de usuario basada en asistentes son grandes y fáciles de usar, algunas personas prefieren la herramienta de legado, llamado 'Usuarios y grupos locales'. Esta herramienta ha cambiado poco desde su introducción en Windows 2000. Para acceder a ella, haga clic en Equipo en el menú Inicio y seleccione Administrar. Esto abrirá en Administración de equipos. A partir de ahí, expanda Usuarios y grupos locales.

Creación de un nuevo usuario: Haga clic en Usuarios, seleccione Nuevo usuario e introduzca el nombre de usuario. Opcionalmente se puede suministrar un nombre completo, la descripción y contraseña. Haga clic en Crear para hacer la cuenta.

Modificación de los usuarios: En "Usuarios y grupos locales", expanda Usuarios y haga doble clic sobre el nombre de usuario correspondiente.

En la ficha General, puede modificar los siguientes ajustes marcando la casilla correspondiente:

El usuario debe cambiar la contraseña en el siguiente inicio de sesión

El usuario no puede cambiar la contraseña

La contraseña nunca caduca

Cuenta deshabilitada

La cuenta está bloqueada (para desbloquear una cuenta que Windows ha bloqueado en respuesta a un usuario de ingresar una contraseña incorrecta demasiadas veces, según lo especificado por la política de seguridad local, desactive esta casilla de verificación)

Una nota acerca de cómo deshabilitar cuentas de usuario: Una práctica administrativa común es desactivar una cuenta en lugar de eliminarlo cuando un empleado deja. De esa manera, si otro usuario sustituye al empleado, usted puede simplemente cambiar el nombre y volver a activar la cuenta, y el nuevo empleado tendrá todos los mismos valores que la anterior.

La cuenta Invitado: Windows 7 incluye una cuenta llamada de huéspedes, que tiene un mínimo de permisos y está desactivado por defecto. Si desea utilizar esta cuenta, haga clic en Usuarios y grupos locales, expanda Usuarios, haga doble clic en la cuenta de invitado, y desactive la casilla de verificación Cuenta deshabilitada.

Windows proporciona muchos grupos para tareas específicas.

Grupos de gestión: Cada cuenta de Windows es un miembro de al menos un grupo. La pertenencia a grupos define qué conjunto de permisos de cada cuenta tiene. La mayoría de las personas utilizan los grupos integrados en Windows (llamado Tipos de cuenta cuando estás en el asistente Crear usuario), pero son libres de crear y personalizar su propio. Existen grupos para agilizar la administración de una computadora más fácil al permitir que el administrador de la flexibilidad necesaria para aplicar permisos y políticas para más de una cuenta al mismo tiempo.

Además de los usuarios (o Usuarios estándar) y Administradores, encontrará una multitud de otros grupos en Windows 7. Algunos de que se destinen a la compatibilidad hacia atrás, mientras que otros están diseñados para fines especializados, tales como permitir el acceso a una copia de seguridad y restaurar archivos , para leer los archivos de registro, o para conectarse a través de escritorio remoto.

Crear un nuevo grupo: Haga clic en Grupos en los "Usuarios y grupos locales" de herramientas, y seleccione Nuevo grupo. Especifique un nombre y una descripción, y haga clic en Agregar para agregar los miembros. Por último, haga clic en Crear.

Administración de cuentas de usuario para los miembros del dominio

Cada equipo es miembro de cualquiera de un grupo de trabajo o un dominio. Los equipos que forman parte de un dominio por lo general tienen un administrador de red que administra las cuentas de usuario. Estas cuentas no se encuentran en equipos individuales, sino en una base de datos central llamado Active Directory. Un grupo de trabajo es más de una red ad-hoc en la que cada equipo está administrado por separado. Sólo los equipos que ejecutan Windows 7 Professional o superior tienen la opción de unirse a un dominio.

Cuando un PC se une a un dominio, las opciones de gestión de usuarios cambian un poco. Los controles para padres no están disponibles, la herramienta de cuentas de usuario sustituye a las "Cuentas de usuario y protección infantil" herramienta, y usted puede crear usuarios locales sólo a través de los "Usuarios y grupos locales" herramienta de gestión.

Adición de un usuario de dominio a un grupo local: En el Panel de control, abra Cuentas de usuario, y haga clic en Dar otros usuarios el acceso a este equipo. A partir de ahí, escriba el nombre de usuario de la persona y el dominio (o haga clic en Examinar para seleccionarlo en Active Directory), haga clic en Siguiente para agregarlos a un grupo, y luego haga clic en Finalizar.

Cuentas de Administrador, estándar, y los invitados en Windows 8

La pantalla de bienvenida muestra las cuentas y los tipos de cuenta en el equipo. Haga clic en una cuenta en la pantalla de bienvenida para iniciar sesión.

Windows 8 ofrece tres tipos de cuentas de usuario:

- **Administrador** tiene el más alto nivel de control del sistema operativo y:
- Puede crear cuentas.
- Puede configurar y cambiar los privilegios.
- Puede cambiar las contraseñas a las cuentas de usuario y del huésped.

Usuario estándar:

- Se puede cambiar, editar o borrar la contraseña.
- Puede cambiar la imagen de la cuenta.
- No se puede instalar ni abrir ciertos programas.

Invitado tiene acceso limitado y:

- Puede utilizar sólo ciertos programas instalados por otros.
- No se puede acceder a los archivos personales o protegidas por contraseña.

Crear una nueva cuenta en Windows 8

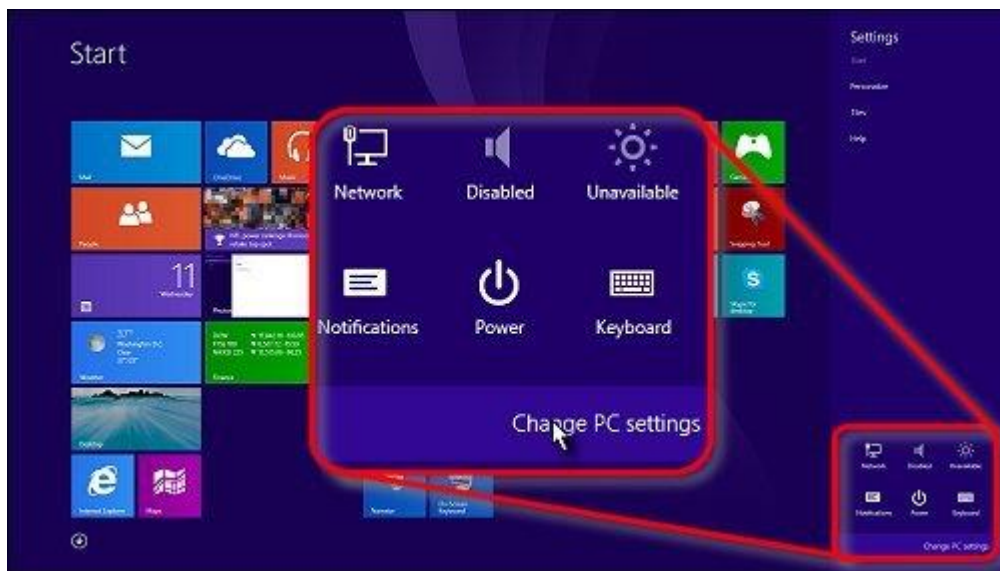
Para crear una nueva cuenta, inicie sesión en una cuenta de administrador y siga los pasos a continuación.

1. En la pantalla Inicio, mueva el puntero del ratón a la esquina inferior derecha para abrir el menú Charms, y haga clic en **Configuración**.
2. **Figura 1: menú Charms**



- 3.
4. Seleccione **Cambiar la configuración de PC** en la esquina inferior derecha de la pantalla.

Figura 2: Cambiar la configuración de PC



5. Seleccione **Cuentas**

6. Haga clic en **Otras cuentas.**

- **Crear una cuenta local**

1. En la **ficha Otras cuentas**, haga clic en **Agregar una cuenta** en el panel derecho.
2. En el **¿Cómo va este signo persona en pantalla**, haga clic en el **signo de un enlace sin cuenta de Microsoft?**
3. Haga clic en el botón de **la cuenta local.**
4. En los campos de contraseña, escriba un nombre de usuario para la nueva cuenta, la contraseña y la contraseña indirecta y, a continuación, haga clic en **Siguiente.**
5. Haga clic en **Finalizar.**

La nueva cuenta y la contraseña son ahora activa.

- **Crear una cuenta de Microsoft**

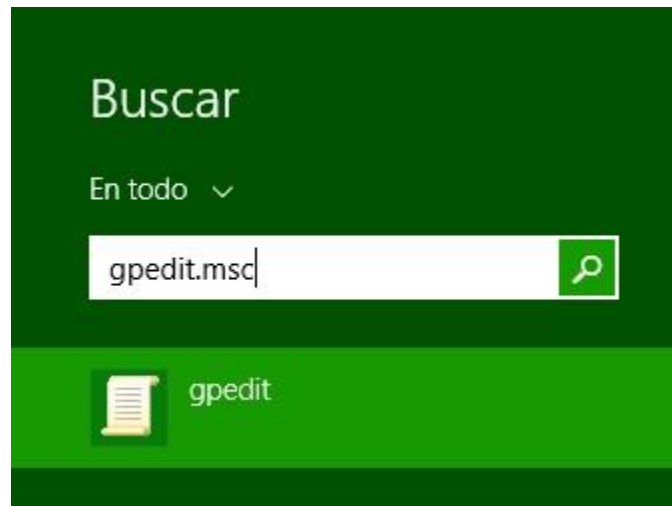
1. En la **ficha Otras cuentas**, haga clic en **Agregar una cuenta** en el panel derecho.
2. En el **¿Cómo va a iniciar sesión este usuario en Windows?** la pantalla, escriba la dirección de correo electrónico de Microsoft en el campo **de dirección de correo electrónico** y, a continuación, haga clic en **Siguiente.**
3. Click en finalizar.

Ahora puede iniciar sesión en Windows 8 con cuenta Microsoft.

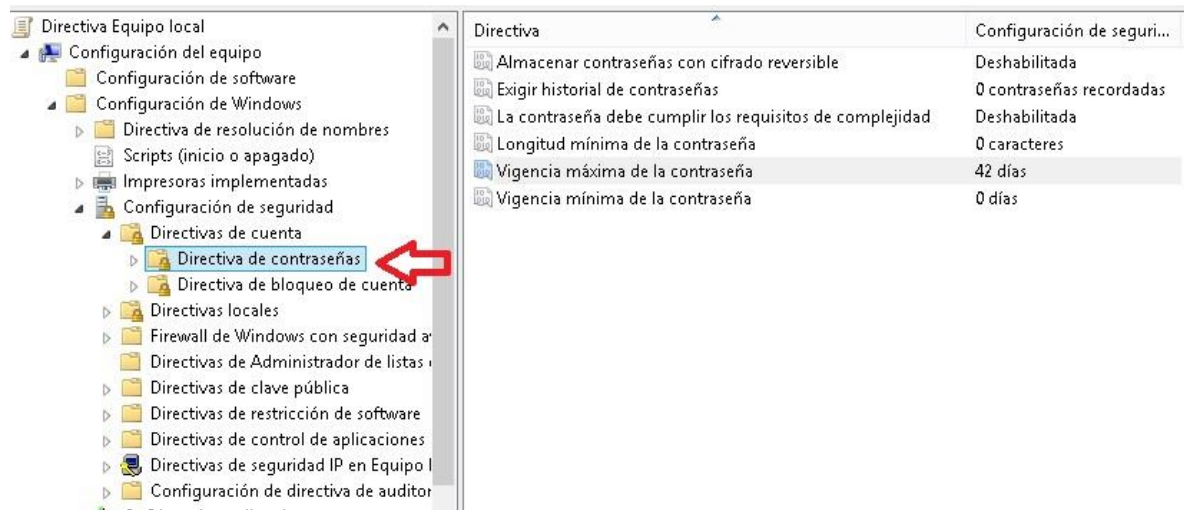
Seguridad

Exigir historial de contraseñas

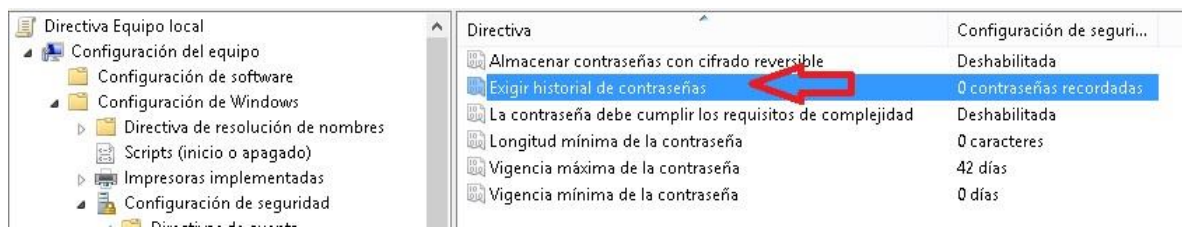
Primero abrimos el panel de búsqueda y dentro de él buscamos el archivo gpedit.msc



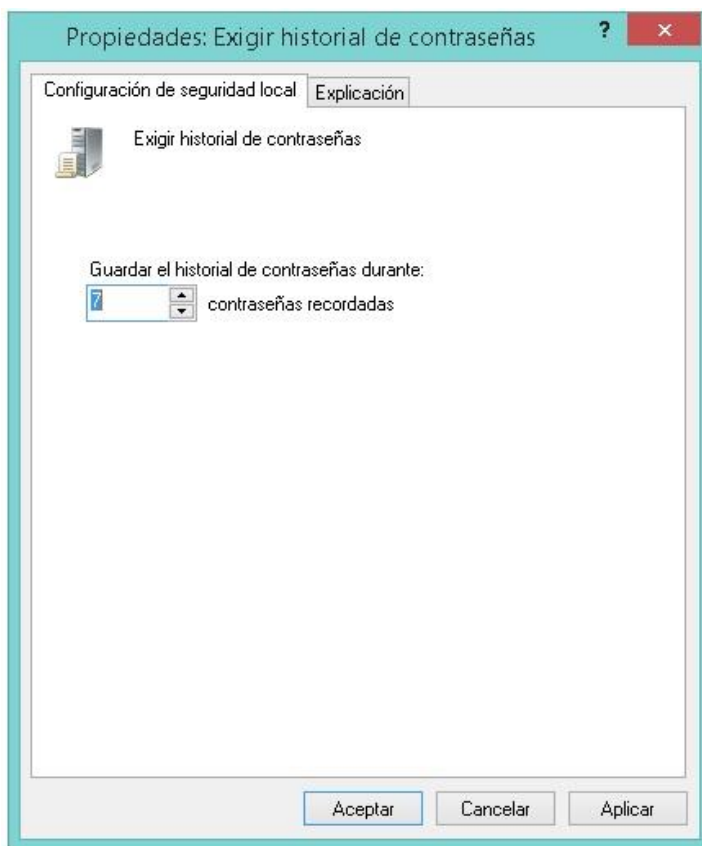
Luego del Editor de directivas de grupo local, desplegamos el menú de configuración de equipo, y vamos a la ruta configuración de windows, configuración de seguridad, directivas de cuenta, directiva de contraseña.



Luego elegimos la opción de exigir historial de contraseñas, esta opción se configura para que windows recuerda una cantidad establecida de contraseñas de las cuentas, y cuando se proceda a cambiar la contraseña no se pueda ingresar una almacenada.

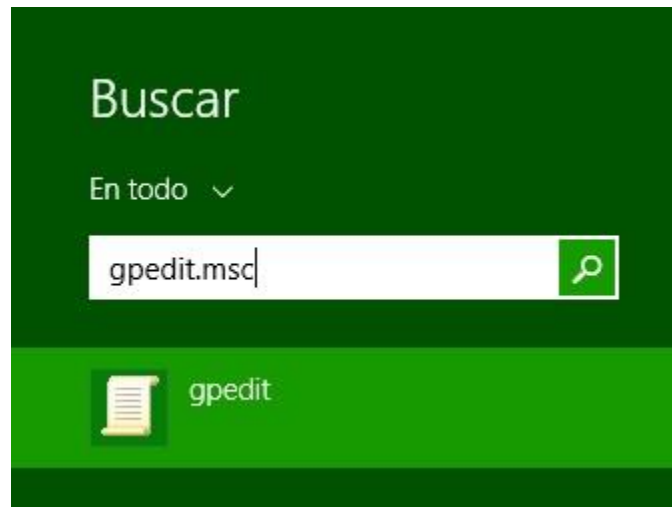


Luego solamente configurar el valor de las contraseñas a recordar.

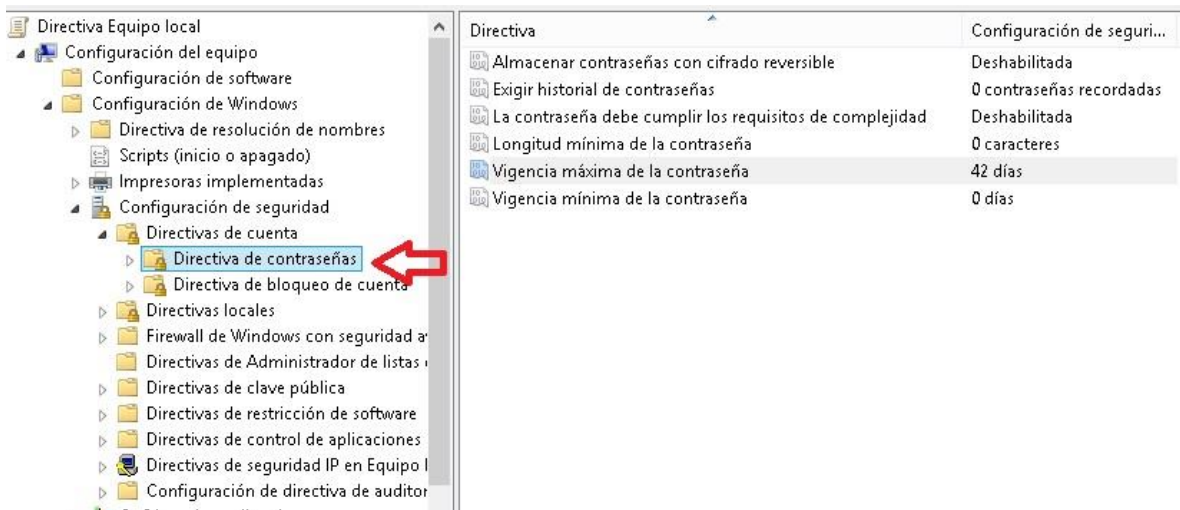


Exigir longitud mínima de la contraseña

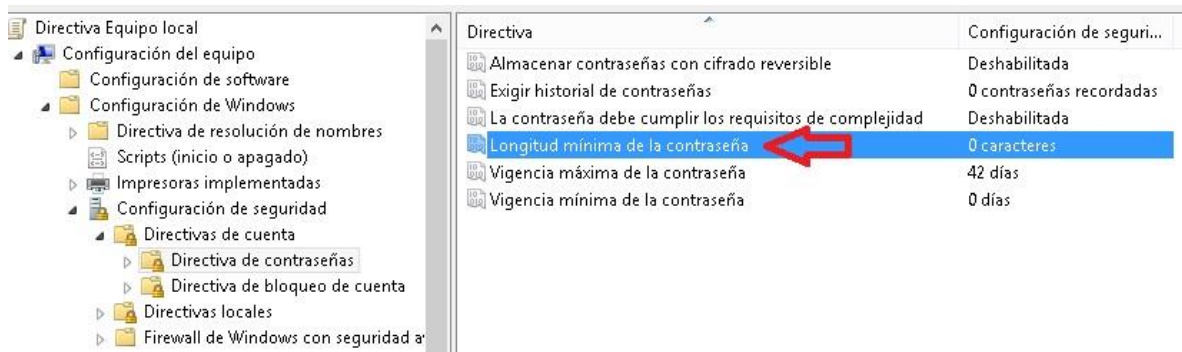
Primero abrimos el panel de búsqueda y dentro de él buscamos el archivo gpedit.msc



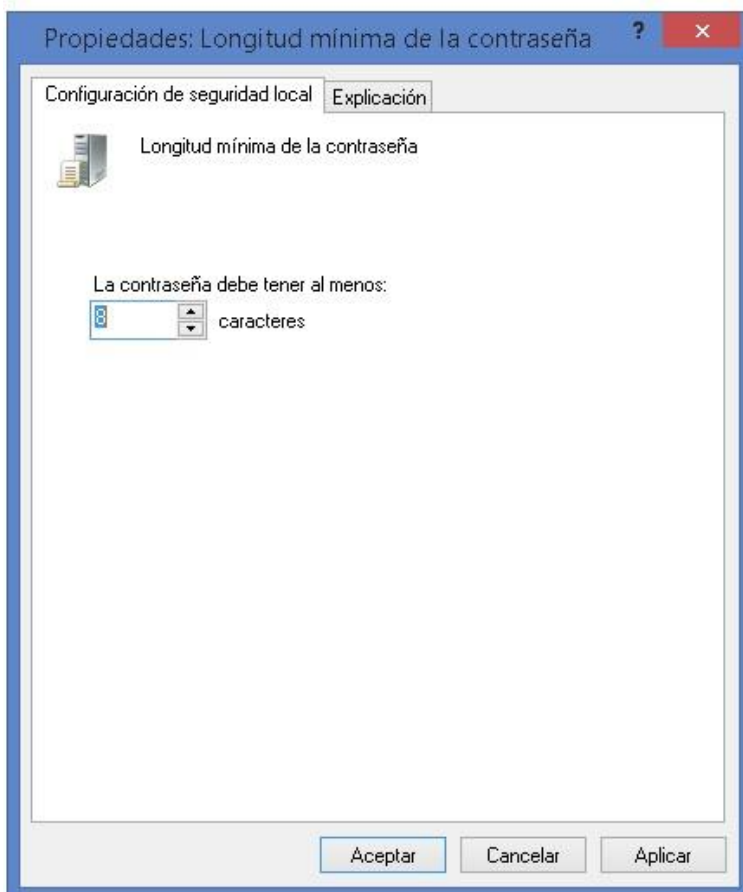
Luego del Editor de directivas de grupo local, desplegamos el menú de configuración de equipo, y vamos a la ruta configuración de windows, configuración de seguridad, directivas de cuenta, directiva de contraseña.



Posteriormente seleccionamos la opción de longitud mínima de la contraseña para modificar los valores correspondientes a esta opción:

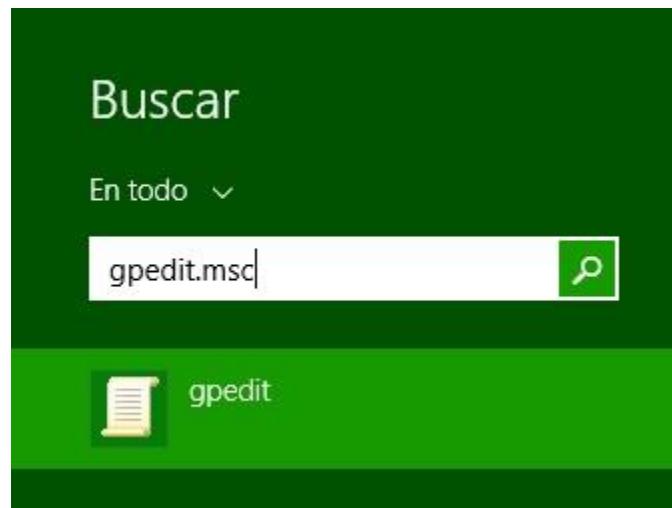


Luego, veremos el recuadro en el cual se nos pide que ingresemos la cantidad de caracteres y presionamos el botón aceptar para realizar los cambios.

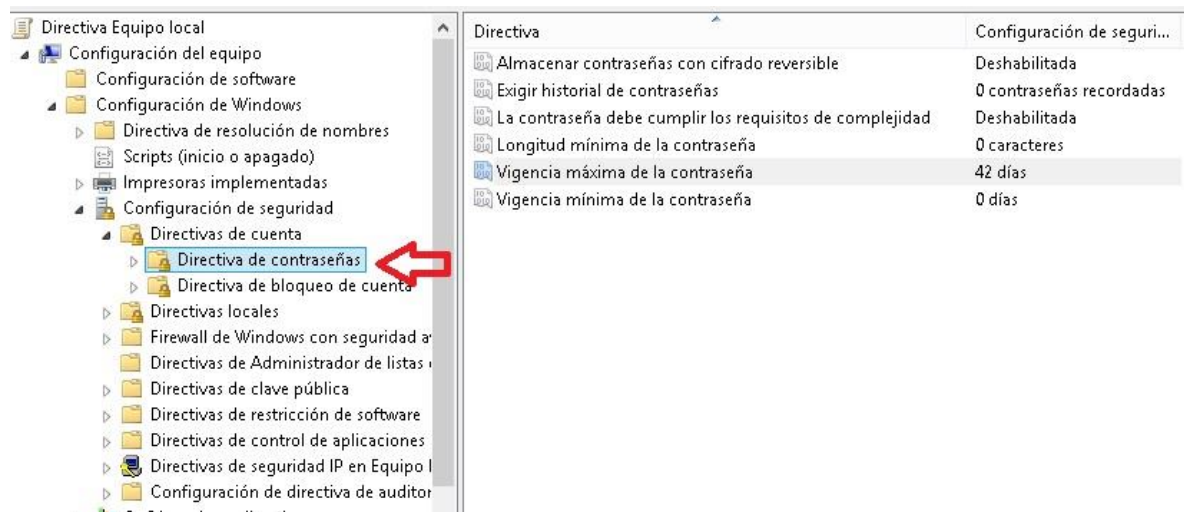


Exigir requisitos de complejidad

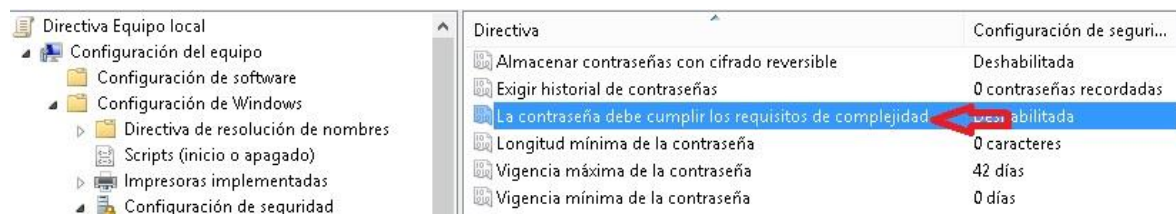
Primero abrimos el panel de búsqueda y dentro de él buscamos el archivo gpedit.msc



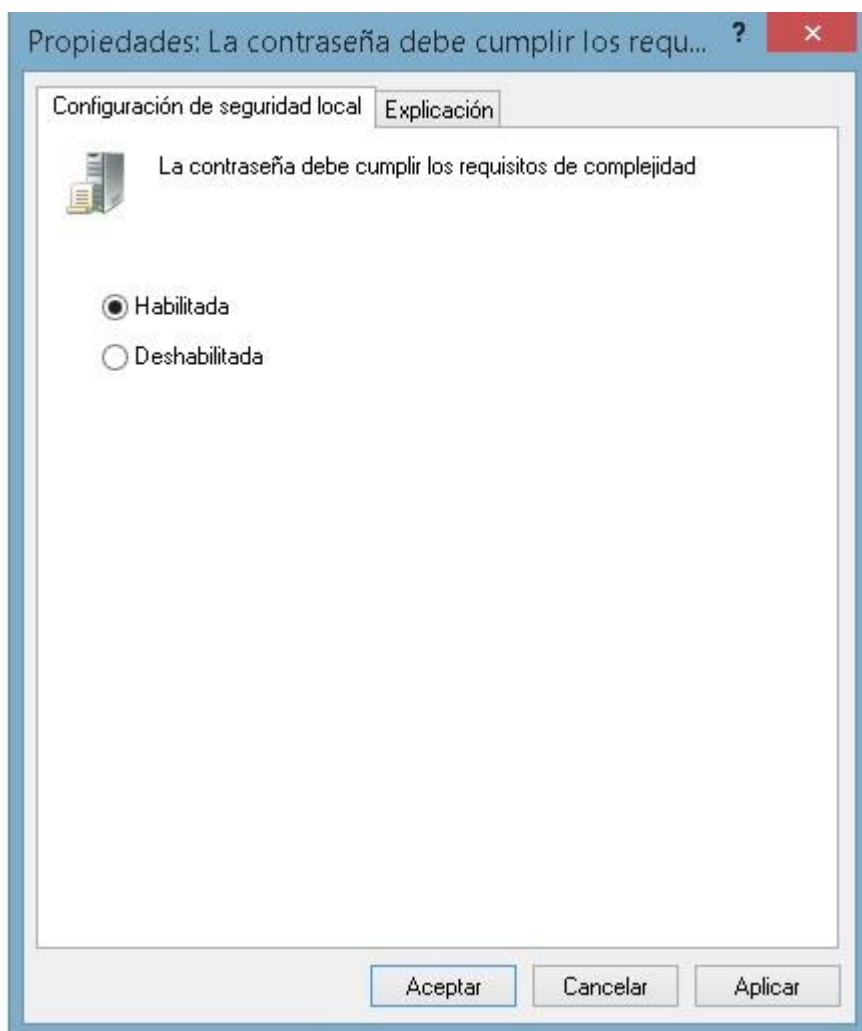
Luego del Editor de directivas de grupo local, desplegamos el menú de configuración de equipo, y vamos a la ruta configuración de windows, configuración de seguridad, directivas de cuenta, directiva de contraseña.



Allí seleccionamos la opción de la contraseña debe cumplir los requisitos de complejidad

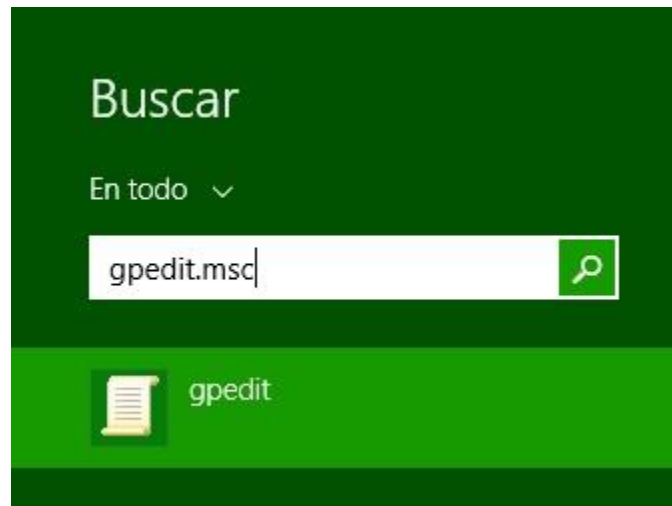


Luego se nos mostrará un cuadro de diálogo con las opciones de habilitar o deshabilita. Cuando se habilita esta opción las contraseñas deben: longitud de 6 caracteres, mayúscula, minúscula, dígitos y caracteres alfanuméricos.

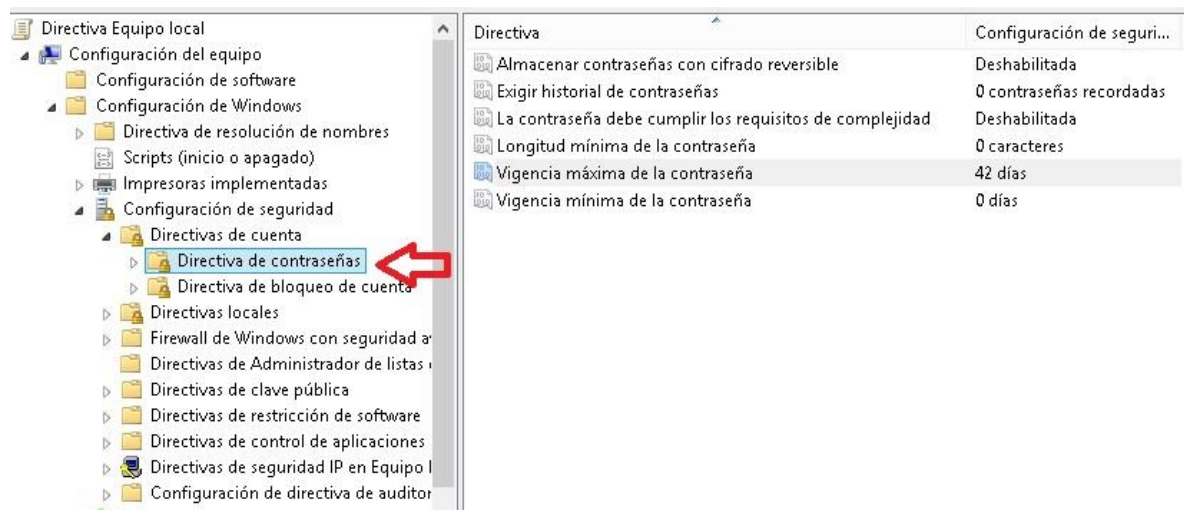


Activar vigencia máxima de contraseña

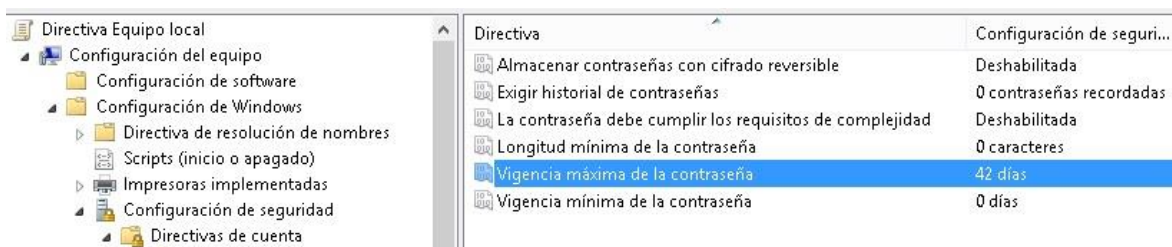
Primero abrimos el panel de búsqueda y dentro de él buscamos el archivo gpedit.msc



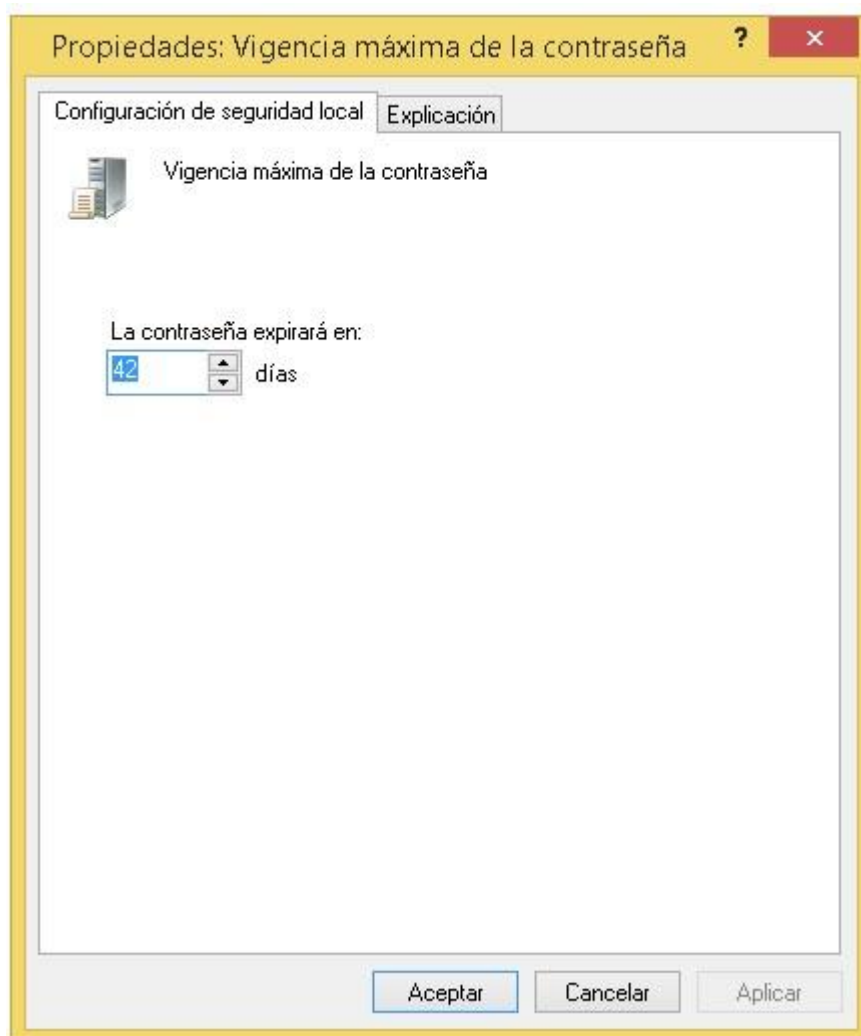
Luego del Editor de directivas de grupo local, desplegamos el menú de configuración de equipo, y vamos a la ruta configuración de windows, configuración de seguridad, directivas de cuenta, directiva de contraseña.



Ahora elegimos la opción de vigencia máxima de contraseña para establecer la cantidad de días.

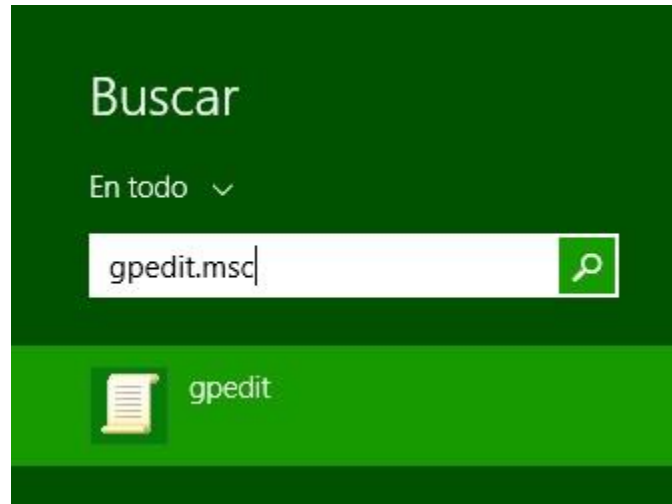


Por último ingresamos la cantidad de días de vigencia de la contraseña, y damos click en aceptar para guardar los cambios.

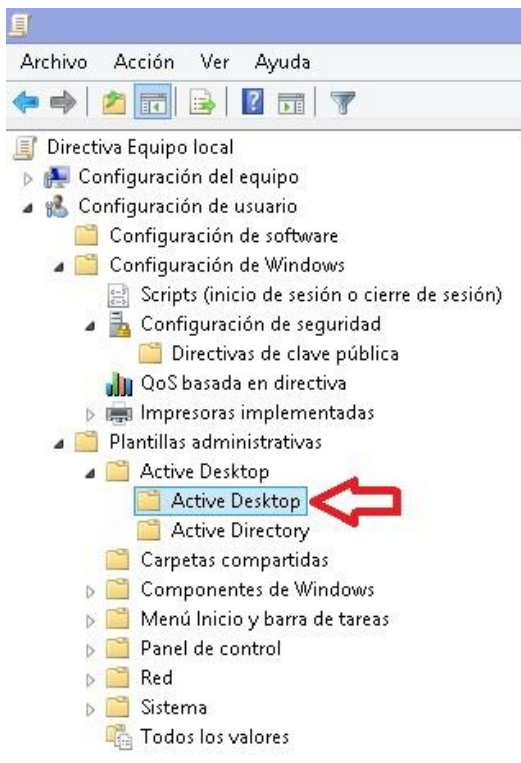


Crear un escritorio activo (Active Desktop) en Windows 8.1





Primero abrimos el panel de búsqueda y dentro de él buscamos el archivo gpedit.msc














Luego del Editor de directivas de grupo local, despliegue el menú de configuración de usuario, plantillas administrativas, Active Desktop y seleccione la carpeta Active Desktop



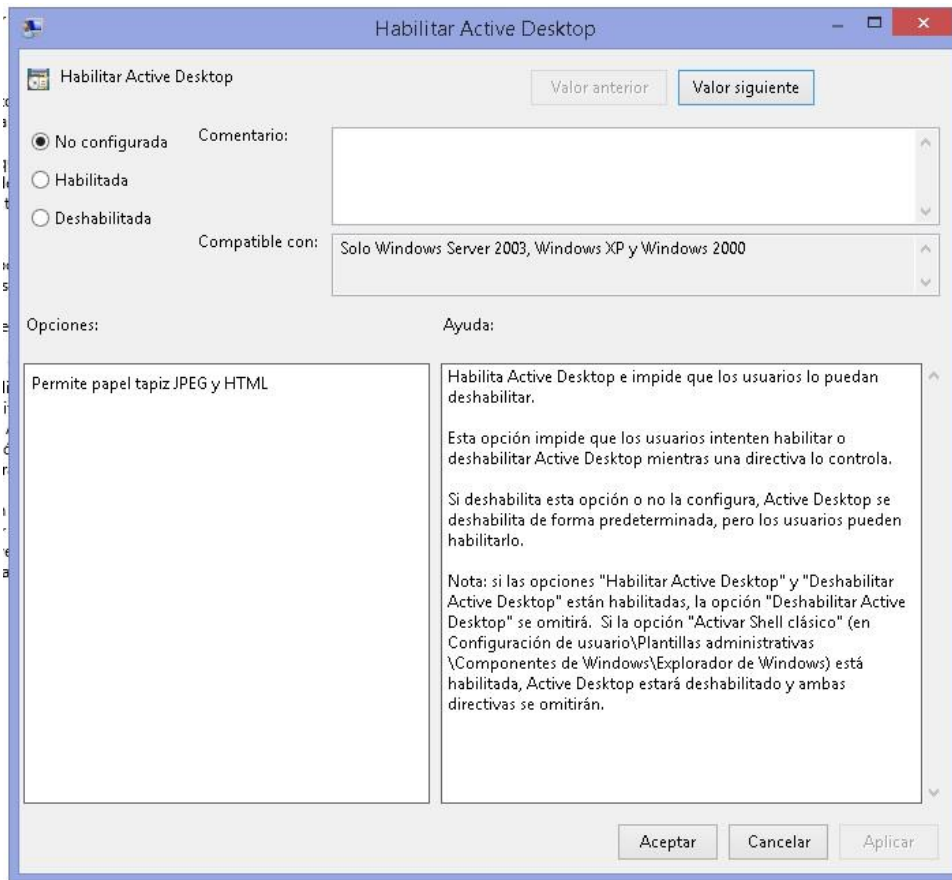
Cuanto haga esto verá todas las directivas de configuración disponibles y su estado, e incluso podrá ver los comentarios configurados.

| Active Desktop | | | |
|--|---|----------------|------------|
| Habilitar Active Desktop | Configuración | Estado | Comentario |
| Editar configuración de directiva Requisitos: Solo Windows Server 2003, Windows XP y Windows 2000 Descripción: Habilita Active Desktop e impide que los usuarios lo puedan deshabilitar. Esta opción impide que los usuarios intenten habilitar o deshabilitar Active Desktop mientras una directiva lo controla. |  Habilitar Active Desktop | No configurada | No |
| |  Deshabilitar Active Desktop | No configurada | No |
| |  No permitir cambios | No configurada | No |
| |  Tapiz del escritorio | No configurada | No |
| |  Prohibir agregar elementos | No configurada | No |
| |  Prohibir cerrar elementos | No configurada | No |
| |  Prohibir eliminar elementos | No configurada | No |
| |  Prohibir modificar elementos | No configurada | No |
| |  Deshabilitar todos los elementos | No configurada | No |
| |  Agregar o quitar elementos | No configurada | No |
| |  Permitir solo papel tapiz de mapa de bits | No configurada | No |

Ahora solamente se pasa a seleccionar la directiva Habilitar Active Desktop, dando doble click sobre ella

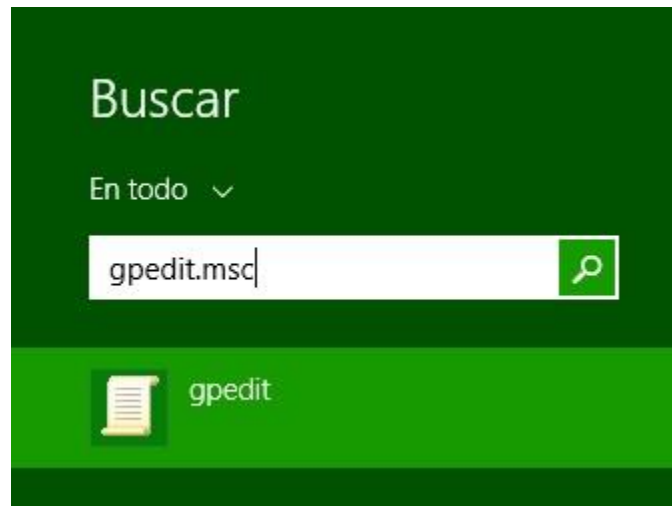
| Active Desktop | | | |
|--|---|----------------|------------|
| Habilitar Active Desktop | Configuración | Estado | Comentario |
| Editar configuración de directiva Requisitos: Solo Windows Server 2003, Windows XP y Windows 2000 Descripción: Habilita Active Desktop e impide que los usuarios lo puedan deshabilitar. Esta opción impide que los usuarios intenten habilitar o deshabilitar Active Desktop mientras una directiva lo controla. |  Habilitar Active Desktop | No configurada | No |
| |  Deshabilitar Active Desktop | No configurada | No |
| |  No permitir cambios | No configurada | No |
| |  Tapiz del escritorio | No configurada | No |
| |  Prohibir agregar elementos | No configurada | No |
| |  Prohibir cerrar elementos | No configurada | No |
| |  Prohibir eliminar elementos | No configurada | No |
| |  Prohibir modificar elementos | No configurada | No |
| |  Deshabilitar todos los elementos | No configurada | No |
| |  Agregar o quitar elementos | No configurada | No |
| |  Permitir solo papel tapiz de mapa de bits | No configurada | No |

Por último con la directiva ya abierta solamente se pasa a escoger la opción de Habilitada, se ingresa un comentario si se quiere y se presiona el botón de aceptar.

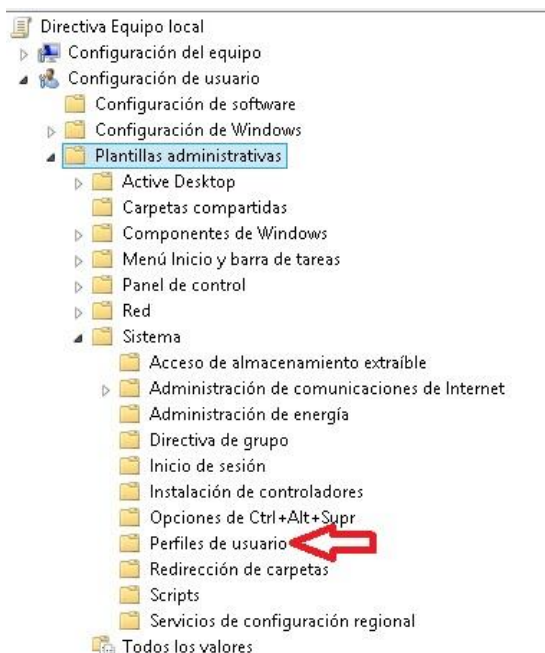


Limitar tamaño del perfil

Primero abrimos el panel de búsqueda y dentro de él buscamos el archivo gpedit.msc



Luego del Editor de directivas de grupo local, despliegue el menú de configuración de usuario, plantillas administrativas, Perfiles de usuario.



Seguidamente escogemos la última opción que corresponde a limitar el tamaño del perfil.

| Perfiles de usuario | | |
|--------------------------------------|---|----------------|
| Limitar el tamaño del perfil | Configuración | Estado |
| | Conectar el directorio principal a la raíz del recurso compartido | No configurada |
| Editar configuración de directiva | Especificar directorios de red que se sincronizarán solo al iniciar y cerrar sesión | No configurada |
| | Excluir directorios en el perfil móvil | No configurada |
| Requisitos: Al menos Windows 2000 | Limitar el tamaño del perfil | No configurada |

Por último escogemos la opción habilitada, y se nos activarán la opción para establecer el tamaño máximo del perfil en KB, además se puede configurar un mensaje para mostrar cuando se haya excedido este espacio y el mensaje a mostrar.

Limitar el tamaño del perfil

Valor anterior Valor siguiente

☐ No configurada ☒ Habilitada ☐ Deshabilitada

Comentario:

Compatible con: Al menos Windows 2000

Opciones:

Mensaje personalizado: Ha excedido su espacio de almacenamie

Tamaño máx. del perfil (KB): 30000

☐ Mostrar archivos de Registro en la lista de archivos

☐ Notificar al usuario cuando se exceda el espacio de almacenamiento de perfiles.

Recordar al usuario cada X minutos: 15

Ayuda:

Esta configuración de directiva establece el tamaño máximo de cada perfil de usuario y determina la respuesta del sistema cuando un perfil alcanza el tamaño máximo. Esta configuración de directiva afecta a ambos perfiles, local y móvil.

Si deshabilita esta configuración de directiva o no la configura, el sistema no limita el tamaño de los perfiles de usuario.

Si habilita esta configuración de directiva, puede:

- Establecer el tamaño máximo permitido del perfil de usuario.
- Determinar si los archivos del Registro se incluyen en el cálculo del tamaño de perfil.
- Determinar si se avisa a los usuarios cuando el perfil supera el tamaño máximo permitido.
- Especificar un mensaje personalizado que notifique a los usuarios que se ha superado el tamaño del perfil.
- Determinar la frecuencia con que se muestra el mensaje personalizado.

Nota: en sistemas operativos anteriores a Microsoft Windows

Aceptar Cancelar Aplicar

Administración de hardware

Administración de hardware en Microsoft® Windows® incluye una serie de características diseñadas para mejorar la gestión del hardware del servidor. Estas características permiten a los administradores de sistemas para administrar de forma segura el hardware del servidor remoto a través de un servidor de seguridad, el uso de un protocolo basado en servicios Web estándar. Trabajar con controlador de administración de placa base (BMC) hardware conectado a un servidor que soporte WS-Management, los componentes de administración de hardware de Windows pueden comunicarse con el sistema remoto, incluso si el sistema operativo de Windows aún no ha arrancado o ha fallado.

Un BMC es un microcontrolador que está conectado localmente a un servidor. BMC incluyen una conexión de red independiente que puede comunicarse a través de la red, incluso si el servidor está fuera de línea. A través de la BMC, los administradores del sistema pueden controlar de forma remota el estado de hardware y los errores y controlar el hardware en respuesta.

Administración de hardware no se instala de forma predeterminada al instalar Windows. Debe habilitar desde la sección Herramientas de administración y supervisión de la opción Agregar / Quitar Asistente para componentes de Windows. Los administradores del sistema pueden gestionar los componentes de administración de hardware a través de herramientas de línea de comandos y las interfaces de secuencias de comandos que se describen a continuación. Sin interfaz gráfica de usuario de Windows está disponible para administrar funciones de gestión de hardware en Windows.

Los tres componentes de administración de hardware son Interface Plataforma de Gestión Inteligente (IPMI), Administración remota de Windows (WinRM), y el recopilador de sucesos.

Intelligent Platform Management Interface (IPMI)

Administración de hardware incluye un Windows Management Instrumentation (WMI) y un controlador para IPMI, un estándar industrial para BMC arquitectura de hardware. Al igual que con todos los proveedores de WMI, la funcionalidad del proveedor IPMI trabaja tanto a nivel local como a distancia utilizando la comunicación remota de WMI sobre Distributed Component Object Model (DCOM), oa través de los servidores de seguridad mediante el protocolo WS-Management. El proveedor de IPMI y la compatibilidad de controladores administración de hardware "en banda", es decir, cuando el sistema operativo se está ejecutando.

El proveedor IPMI WMI expone varias clases que permiten scripts y aplicaciones para comunicarse con el hardware de BMC a través del controlador IPMI a nivel de kernel. Las clases de las revelaciones de proveedores son:

- AdminDomain
- ComputerSystem
- SystemSpecificCollection
- LogRecord
- Sensor

- RecordLog

Para más detalles sobre las clases del proveedor IPMI WMI, propiedades y métodos, consulte el Kit de desarrollo de software WinRM .

El proveedor es una implementación de Microsoft de un subconjunto del estándar IPMI Common Information Model (CIM) Mapeo Especificación.

Administración remota de Windows (WinRM)

Administración remota de Windows (WinRM) es la implementación de Windows de WS-Management, un protocolo basado en servicios web estándar de la industria. WinRM proporciona una forma segura y eficiente para aplicaciones de administración y secuencias de comandos para comunicarse con los equipos locales y remotos. El servicio de Windows que WinRM instala y usa también se nombra WinRM.

Cuando un servidor está conectado a un BMC que admita el estándar WS-Management, aplicaciones y scripts pueden usar WinRM para comunicarse directamente con el BMC, incluso cuando el sistema operativo está en línea (previo al inicio o después del fracaso).

Cuando un servidor no está conectado a un BMC, WinRM todavía se puede utilizar para conectarse a WMI de forma remota en situaciones en que se impide la comunicación DCOM (por ejemplo, a través de un firewall). Esto es posible porque el estándar WS-Management es compatible con firewalls y utiliza un único puerto configurable por el administrador del sistema.

WinRM expone su propia interfaz de programación de aplicaciones (API) para secuencias de comandos, que puede ser usado por los scripts escritos en cualquier lenguaje compatible con Windows Script Host. La API de scripting comunica con WMI utilizando la sintaxis diferente de secuencias de comandos estándar de WMI. Sintaxis WinRM se documenta en el Kit de Desarrollo de Software WinRM . Gestión del hardware utiliza un plug-in de WMI para exponer clases WMI para WinRM. Para llamar a estas clases, el espacio de nombres WMI y la clase deben ser convertidos en un Uniform Resource Identifier (URI). (Consulte Configuración y seguridad .)

WS-Management se basa en las siguientes especificaciones estándar:

- HTTPS
- SOAP sobre HTTP (perfil de WS-I)
- SOAP 1.2
- WS-Addressing
- WS-Transfer
- WS-Enumeración
- WS-Concurso Completo

Comando WinRM herramienta Línea (Winrm.cmd)

La herramienta de línea de comandos proporcionada como la interfaz administrativa principal para administrar WinRM es un archivo por lotes (Winrm.cmd) que se ejecuta un script de Visual Basic Scripting Edition (VBScript) llamado Winrm.vbs. Debido a que es una secuencia de comandos, puede abrirlo como un archivo de texto y ver el código de aprender cómo funciona. También puede

escribir sus propios scripts VBScript que se aprovechan de la API de scripting WinRM. Winrm.vbs ejecuta bajo Cscript.exe, el motor de secuencias de comandos de línea de comandos de Windows Script Host.

Winrm.vbs permite a los administradores del sistema para configurar y administrar WinRM. Debido a que WS-Management es un servicio Web que utiliza XML como su formato de mensaje, salida Winrm.vbs es XML nativa también. La herramienta proporciona interruptores de salida XML más legible o texto plano.

El uso de línea de comandos (/?) De la herramienta proporciona la sintaxis detallada y ejemplos de su uso. Herramienta de línea de comandos de administración remota de Windows (Winrm.cmd) cubre antecedentes y la información conceptual en la herramienta y también proporciona ejemplos extensos.

Recopilador de eventos

El servicio Recopilador de eventos es el tercer componente de administración de hardware en Windows. Este servicio es un cliente de administración remota de Windows que se utiliza para crear las suscripciones a los proveedores de eventos de WS-Management y almacenar los eventos recibidos en el Sistema de Registro de Eventos de Windows (SEL). Dos escenarios se admiten en R2:

- El registro de eventos de hardware de la SEL local cuando el sistema operativo está en funcionamiento ("in-band"), utilizando el controlador IPMI y el proveedor WMI.
- El registro de eventos de hardware de BMC de un servidor remoto mediante WS-Management (cuando el hardware BMC soporta esto).

En caso de cierre del sistema operativo o el fracaso, Windows registra los eventos en IPMI SEL del BMC. El administrador puede acceder SEL del BMC utilizando herramientas "fuera de banda" para determinar por qué una máquina no se está ejecutando.

Recopilador de eventos es gestionado con una herramienta de línea de comandos, la utilidad del colector de eventos de Windows (Wecutil.exe).

Hardware BMC tiene su propia SEL en el que registra los eventos significativos. A través de un plug-in de registro de eventos y recopilador de eventos, instalado como parte de la administración de hardware, Windows puede suscribirse a los eventos almacenados en SEL del BMC para que aparezcan en el Visor de eventos de Windows.

Con Wecutil.exe, los administradores del sistema pueden crear y administrar suscripciones de eventos para eventos de BMC. Suscripciones requieren un archivo de configuración XML: una muestra, %windir%\system32\WsmSelRg.xml, se incluye con Windows.

La herramienta proporciona un amplio uso de línea de comandos (/?) Con ejemplos. Se proporciona más información en el tema Evento Collector .

Otros temas de administración remota de Windows

Los temas siguientes describen cómo configurar y utilizar las funciones de administración de hardware, y describir la arquitectura subyacente.

Administración de hardware Habilitación

Debido a la característica de administración de hardware no está habilitado de forma predeterminada en Windows, debe habilitar explícitamente con la opción Agregar / Quitar Asistente

para componentes de Windows. En este tema se explica cómo. También discute Plug and Play para el controlador IPMI.

Configuración y seguridad

Instalación de Hardware Management implica configurar WinRM para trabajar con HTTP o HTTPS. Para utilizar HTTPS, se requiere un certificado de servidor. Este tema se explica el trabajo con los certificados, oyentes configuración y otros problemas de configuración.

Integración con WMI

En este tema se explica cómo utilizar el plug-in de WinRM WMI para acceder a clases de WMI a través del protocolo WS-Management. Describe cómo convertir un espacio de nombres WMI a un WS-Management URI.

Interfaces de línea de comandos

Dos nuevas interfaces de línea de comandos se instalan con el componente de administración de hardware de Windows: Winrm.cmd y Wecutil.exe. Estas herramientas se utilizan para la gestión de WinRM y la recopilación de eventos, respectivamente.

- Ventanas de gestión remota de línea de comandos de la herramienta (Winrm.cmd)
- Eventos de Windows Utilidad Collector (Wecutil.exe)

Bibliografía

<http://www.xml.com/ldd/chapter/book/ch08.html>

<http://h10025.www1.hp.com/ewfrf/wc/document?cc=us&lc=en&docname=c03596656>

<http://superuser.com/questions/511885/how-do-i-modify-user-groups-in-windows-8>

http://www.pcworld.com/article/258875/adding_and_managing_users_in_windows_8.html

http://www.pcworld.com/article/171933/manage_users_in_windows_7.html?page=2

http://en.wikipedia.org/wiki/Hash_function

http://en.wikipedia.org/wiki/Security_Accounts_Manager

http://www.mcmcse.com/microsoft/guides/manage_users.shtml

<http://www.windowsnetworking.com/articles-tutorials/windows-xp/wxppusrm.html>

<https://www2.opengroup.org/ogsys/catalog/t101>

