

SISTEMAS OPERATIVOS – Administrador de Tareas

Objetivos

- ✓ Que el alumno aprehenda el concepto del uso del Administrador de Tareas de Windows XP

Requisitos

- ✓ Haber asistido a las clases teóricas
- ✓ Haber leído el material suministrado por la cátedra

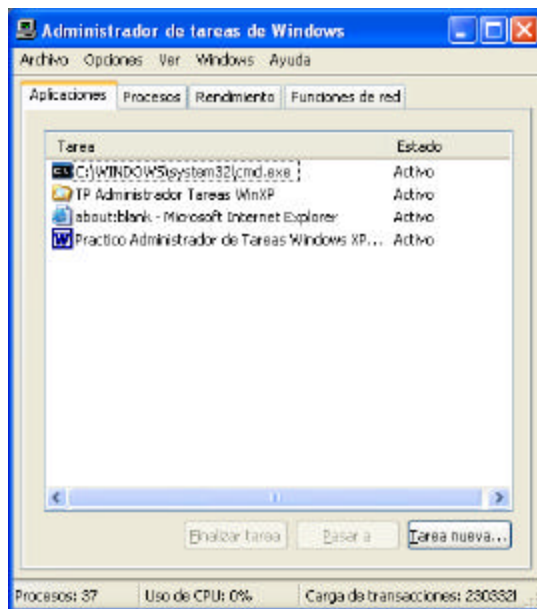
Ejercitación

Punto N° 1- Mencione las diferentes formas para acceder al Administrador de Tareas de Windows XP

Punto N° 2- ¿Que función cumple el Administrador de Tareas de Windows XP?

Punto N° 3- Realice una breve descripción de las 4 fichas del Administrador y enumere las distintas opciones de cada una de ellas y su función.

Punto N° 4 Investigue, identifique y clasifique todos los procesos que se están ejecutando en su equipo actualmente. (puede utilizar el recurso publicado en el Entorno Virtual, en la sección Materiales “Información sobre procesos que corren en tu Windows”)



Punto N° 5- ¿Cuales serian los procesos que deberían ejecutarse normalmente en Windows XP?

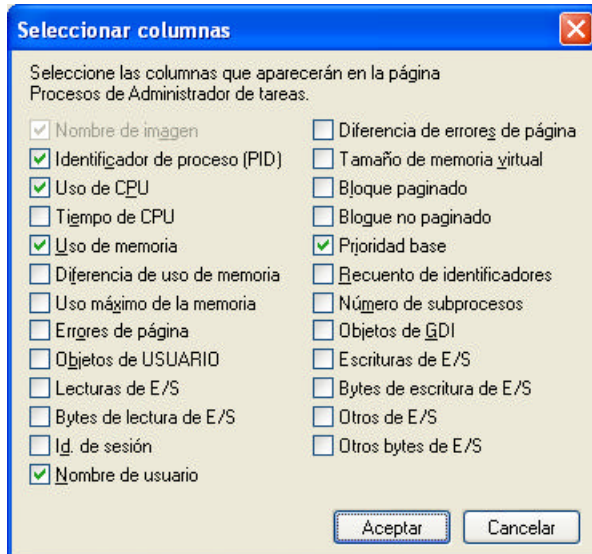
Punto N° 6- Analice los procesos que está ejecutando actualmente su sistema y observe si existe alguno que no sea necesario para la actividad que Ud. normalmente desarrolla. ¿Cómo puede determinar esto?

Punto N° 7- ¿Se puede bloquear el acceso al Administrador de Tareas? En caso afirmativo determine como sería el procedimiento para habilitar/deshabilitar el acceso al mismo?

Punto N° 8- ¿Que información se puede visualizar de cada proceso que se está ejecutando actualmente en su sistema?

Punto N° 9 - Accede a la pestaña Procesos y allí a la opción de menú **Ver** y luego **Seleccionar columnas**. Observe que opciones se le permiten.

SISTEMAS OPERATIVOS – Administrador de Tareas



Punto N°10- Trate de dar una descripción sencilla de cada una de las columnas que se le permite visualizar. Algunas de ellas relacionadas con la E/S o la memoria se verán posteriormente.

Punto N°11- ¿Cree Ud. que algunos de estos valores se almacenan en el PCB del proceso? ¿Cuáles?

Punto N°12 - Seleccione Número de subprocesos. Analice cuantos tiene una aplicación WIN32 respecto de una WIN16 (Ejemplo una ventana MSDOS).

Punto N° 13- Identifique el IP de los procesos actualmente en ejecución. Observe aquellos que tienen menor valor. ¿Tiene esto algo que ver con los procesos que se ejecutan en la inicialización?

Punto N° 14- ¿Que operaciones se pueden realizar sobre los procesos que se están ejecutando?

Punto N° 15- ¿El administrador de tareas muestra todos los procesos que se están ejecutando en su sistema actualmente? Justifique.

Punto N° 16- ¿Existen otras aplicaciones alternativas al Administrador de Tareas? ¿Cuales? ¿Hay alguna que sea GNU/GPL?

Punto N° 17- ¿Como seria el procedimiento para detectar y eliminar un proceso que este ligado a un virus o gusano que este infectado su sistema?

Punto N° 18- Desde la línea de comandos (ventana MSDOS) ejecute el comando **tasklist** ¿Qué información suministra?

Punto N° 19- Analice las opciones del comando anterior. ¿Qué información puede obtener de ellas?

Punto N° 20- Analice los siguientes comandos y explique que hace cada uno de ellos.

- ✓ **tasklist /v /fi "PID gt 1000" /fo csv**
- ✓ **tasklist /fi "USERNAME ne NT AUTHORITY\SYSTEM" /fi "STATUS eq running"**
- ✓ **tasklist /v /fi "STATUS eq running"**
- ✓ **tasklist /s srvmain /nh tasklist /s srvmain /svc /fi "Modules eq ntdll*"**
- ✓ **tasklist /s srvmain /u maindom\hiropln /p p@ssW23 /nh**

Punto N° 21- Investigue el comando **taskkill**.

SISTEMAS OPERATIVOS – Administrador de Tareas

Punto N° 22- Analice los siguientes comandos y explique que hace cada uno de ellos.

- ✓ **taskkill /pid 1230 /pid 1241 /pid 1253**
- ✓ **taskkill /f /fi "USERNAME eq NT AUTHORITY\SYSTEM" /im notepad.exe**
- ✓ **taskkill /s srvmain /f /im notepad.exe**
- ✓ **taskkill /s srvmain /u maindom\hiropln /p p@ssW23 /fi "IMAGENAME eq note*" /im ***
- ✓ **taskkill /s srvmain /u maindom\hiropln /fi "USERNAME ne NT*" /im ***
- ✓ **taskkill /pid 2134 /t /fi "username eq administrator"**
- ✓ **taskkill /f /fi "PID ge 1000" /im ***

Punto N° 22- Ejecute **tasklist /SVC**. ¿Para qué nos sirve?

Punto N° 23- Desarrolle un programa que permita visualizar todos los procesos que se están ejecutando actualmente en su sistema, y además permita realizar tareas de administración de los mismos.

ANEXOS

Tasklist

Muestra una lista de los procesos en ejecución actualmente en un equipo local o remoto.

Sintaxis

tasklist [/s *equipo* [/u *dominio\usuario* [/p *contraseña*]] [{ /m *módulo* | /svc | /v}] [/fo {**TABLE** | **LIST** | **CSV**}] [/nh] [/fi *filtro* [/fi *filtro* [...]]]

Parámetros

/s *equipo*

Especifica el nombre o la dirección IP de un equipo remoto (no utilice barras diagonales inversas). El valor predeterminado es el equipo local.

/u *dominio\usuario*

Ejecuta el comando con los permisos de cuenta del usuario especificado por *usuario* o *dominio\usuario*. El valor predeterminado son los permisos del usuario que inició la sesión actual en el equipo que emite el comando.

/p *contraseña*

Especifica la contraseña de la cuenta de usuario especificada en el parámetro **/u**.

/m *módulo*

Enumera todas las tareas en las que se han cargado módulos DLL que concuerdan con el nombre de patrón especificado. Si no se especifica el nombre de módulo, esta opción muestra todos los módulos cargados por cada tarea.

/svc

Enumera toda la información de servicios de cada proceso sin truncamiento. Es válido cuando el parámetro **/fo** se establece en **TABLE**.

/v

Especifica que en el resultado se mostrará la información detallada de tareas. Para ver la información detallada completa sin truncación, utilice este parámetro junto con **/svc**.

/fo{ **TABLE** | **LIST** | **CSV**}

Especifica el formato en el que se mostrará el resultado. Los valores válidos son **TABLE**, **LIST** y **CSV**. El formato de salida predeterminado es **TABLE**.

/nh

Elimina el encabezado de las columnas en el resultado. Es válido cuando el parámetro **/fo** se establece en **TABLE** o **CSV**.

/fi *filtro*

SISTEMAS OPERATIVOS – Administrador de Tareas

Especifica los tipos de procesos que se van a incluir o excluir de la consulta. La siguiente tabla muestra nombres de filtro, operadores y valores válidos.

Nombre	Operadores	Valor
Estado	eq, ne	RUNNING NOT RESPONDING UNKNOWN
Imagenname	eq, ne	Cualquier cadena válida.
PID	eq, ne, gt, lt, ge, le	Cualquier número entero positivo.
Session	eq, ne, gt, lt, ge, le	Cualquier número de sesión válido.
nombreSesión	eq, ne	Cualquier cadena válida.
CPUTime	eq, ne, gt, lt, ge, le	Tiempo válido en el formato <i>hh:mm:ss</i> . Los parámetros <i>mm</i> y <i>ss</i> deben estar entre 0 y 59, y <i>hh</i> puede ser cualquier valor numérico sin signo válido.
Memusage	eq, ne, gt, lt, ge, le	Cualquier entero válido.
Username	eq, ne	Cualquier nombre de usuario válido (<i>[dominio\]usuario</i>).
Services	eq, ne	Cualquier cadena válida.
Windowtitle	eq, ne	Cualquier cadena válida.

/?

Muestra Ayuda en el símbolo del sistema.

Notas

- Los filtros "WindowTitle" y "Status" no se admiten cuando se realiza una consulta en un sistema remoto.
- **Tasklist** sustituye a la herramienta **tlist**.

Taskkill

Finaliza una o más tareas o procesos. Los procesos se pueden suprimir mediante el Id. de proceso o el nombre de imagen.

Sintaxis

SISTEMAS OPERATIVOS – Administrador de Tareas

taskkill [/s *equipo* [/u *dominio\nombre de usuario* [/p *contraseña*]] {[**/fi** *Filter* [/fi *Filter* [...]]} [{ **/pid** *IdDeProceso* | **/im** *nombreDeImagen*}] | **/pid** *IdDeProceso* | **/im** *nombreDeImagen*} [**/f**] [**/t**]

Parámetros

/s *equipo*

Especifica el nombre o la dirección IP de un equipo remoto (no utilice barras diagonales inversas). El valor predeterminado es el equipo local.

/u *dominio\nombreDeUsuario*

Ejecuta el comando con los permisos de cuenta del usuario especificado por *nombreDeUsuario* o *dominio\nombreDeUsuario*. **/u** sólo se puede especificar cuando se especifica **/s**. El valor predeterminado son los permisos del usuario que inició la sesión actual en el equipo que emite el comando.

/p *contraseña*

Especifica la contraseña de la cuenta de usuario especificada en el parámetro **/u**.

/fi *Filtro*

Especifica los tipos de procesos que se van a incluir o excluir de la terminación. Se puede especificar más de un filtro. Utilice el carácter comodín (*) para especificar todas las tareas o todos los nombres de imagen. Son válidos los siguientes nombres de filtro, operadores y valores.

Nombre	Operadores	Valor
Estado	eq, ne	RUNNING NOT RESPONDING UNKNOWN
Imagename	eq, ne	Cualquier cadena válida.
PID	eg, ne, gt, lt, ge, le	Cualquier número entero positivo.
Session	eg, ne, gt, lt, ge, le	Cualquier número de sesión válido.
CPUTime	eq, ne, gt, lt, ge, le	Hora válida en el formato <i>HH:MM:SS</i> . Los parámetros <i>mm</i> y <i>ss</i> deben estar entre 0 y 59 y <i>hh</i> puede ser cualquier valor numérico sin asignar válido.
Memusage	eg, ne, gt, lt, ge, le	Cualquier entero válido.
Username	eq, ne	Cualquier nombre de usuario válido (<i>[dominio\]nombreDeUsuario</i>).
Services	eq, ne	Cualquier cadena válida.

SISTEMAS OPERATIVOS – Administrador de Tareas

Nombre	Operadores	Valor
Windowtitle	eq, ne	Cualquier cadena válida.
Modules	eq, ne	Cualquier cadena válida.

/pid *Id.Proceso*

Especifica el Id. de proceso del proceso que se va a terminar.

/im *nombreImagen*

Especifica el nombre de imagen del proceso que se va a terminar. Utilice el carácter comodín (*) para especificar todos los nombres de imagen.

/f

Especifica que los procesos serán terminados a la fuerza. Este parámetro se omite en procesos remotos; todos los procesos remotos se terminan a la fuerza.

/t

Finaliza el proceso especificado y todos los procesos secundarios iniciados por el mismo.

/?

Muestra Ayuda en el símbolo del sistema.

Notas

- Los filtros "WindowTitle" y "Status" no se admiten cuando se especifica un sistema remoto.
- El carácter comodín (*) sólo se acepta cuando se especifica junto con los filtros.
- La terminación de los procesos remotos siempre se realizará a la fuerza con independencia de que se especifique el parámetro **/f**.
- Al suministrar un nombre de equipo al filtro HOSTNAME se producirá un apagado y todos los procesos se detendrán.
- Utilice **tasklist** para determinar el Id. de proceso (PID) del proceso que se va a terminar.
- **Taskkill** sustituye a la herramienta **kill**.