http://www.teknodatips.com.ar

Teknoda - Notas técnicas – Tips de AS400 – iseries – System i

Tip en detalle Nro. 26

(Lo nuevo, lo escondido, o simplemente lo de siempre pero bien explicado)

---

*"Tips en breve/Tips en detalle" se envía con frecuencia variable y absolutamente **sin cargo** como un servicio a nuestros clientes AS/400. Contiene principalmente notas técnicas y no contiene mensajes publicitarios.*

Este mensaje se envía en concordancia con la nueva legislación sobre correo electrónico: Por sección 301,párrafo (a) (2) (c) de S.1618 bajo el decreto s.1618 titulo 3º aprobado por el 105 congreso base de las normativas internacionales sobre SPAM, este e-mail no podrá ser considerado SPAM mientras incluya una forma de ser removido

*Conteste este mail con asunto "REMOVER" si no desea recibir más esta publicación. Si desea suscribir otra dirección de e-mail para que comience a recibir los "Tips", envíe un mensaje **desde esa dirección** a letter400@teknoda.com, aclarando nombre, empresa y cargo del suscriptor.*

Cómo gestionar y controlar la seguridad a través del menú SECTOOLS – Parte I

Tema:	Seguridad, Administración.
Utilidad:	Administración de Seguridad
Nivel:	Intermedio/Avanzado.
Versión:	Todas.

Lista de Tips publicados hasta la fecha:

1. Modificación de los parámetros por default que rigen en los comandos del OS/400
2. Restricción de comandos pesados a modalidad batch
3. Cómo generar un entorno de prueba para año 2000
4. Cómo salvar y restaurar spool
5. Cómo agregar pantallas de confirmación/validación para comandos delicados
6. Defragmentación del espacio en disco no utilizado : STRDSKRGZ, ENDDSKRGZ
7. Manipulación de bases de datos desde programas CL, a través de Query/400
8. Generación de spool AS/400 en formato PDF (Adobe Acrobat Reader) para almacenar en CD´s
9. Cómo proteger columnas de un archivo físico o lógico

10. Cómo cambiar la pantalla de signon
11. Cómo automatizar transferencias de archivos con TCP/IP desde AS/400
12. Control de accesos sobre archivos de spool
13. Aproveche lo que ya tiene: FILE SERVING con NETSERVER/400
14. EMULACION 5250 vía Internet con lo que ya tiene instalado
15. Editor alternativo: Comando EDTF (Edit File)
16. Auditoría sobre objetos en AS/400
17. Cómo personalizar los comandos del menú de petición del sistema
18. Acceso a archivos multimiembros en un entorno cliente/servidor o SQL
19. Cómo agregar opciones de usuario al producto PDM
20. Auditoría sobre usuarios en AS/400
21. Cómo obtener línea de comandos en pantallas que no la tienen.
22. Cómo enviar por e-mail objetos de QSYS.LIB
23. Cómo transferir archivos de spool a la PC usando Operations Navigator
24. Qué es el IFS y cómo accederlo
25. Curiosidades de la programación CL – Parte I

Temas de próximos tips:

- **Cómo rutear usuarios a subsistemas según el nombre y no el dispositivo.**
- **Curiosidades de la programación CL – Parte II**

Resumen ejecutivo

El menú SECTOOLS es un conjunto de herramientas de seguridad provistas por OS/400 que permiten, entre otras tareas, analizar contraseñas por omisión, habilitar usuarios en determinados rangos horarios, inhabilitar perfiles que no se utilizaron más de un número especificado de días, trabajar con la activación y visualización de las anotaciones de auditoría y generar una gran cantidad de informes relacionados con la seguridad. En la primera parte del presente tip ampliaremos algunas de sus posibilidades. Para poder acceder a las opciones del menú, desde línea de comandos ingrese GO SECTOOLS.

Introducción

El menú SECTOOLS ofrece amplias opciones para gestionar y controlar aspectos de la seguridad del OS/400. Para acceder a este menú ingrese en la línea de comandos GO SECTOOLS. Aparece la siguiente pantalla:

```
SECTOOLS                  Herramientas de seguridad
                                                    Sistema:   S1025CFM
Seleccione una de las opciones siguientes:

  Trabajar con perfiles
     1. Analizar contraseñas por omisión

     2. Visualizar lista de perfiles activos
     3. Cambiar lista de perfiles activos
     4. Analizar actividad de perfiles

     5. Visualizar planificación de activación
     6. Cambiar entrada de planificación de activación

     7. Visualizar planificación de caducidad
     8. Cambiar entrada de planificación de caducidad

     9. Imprimir información interna de perfil
                                                                  Más...
Selección o mandato
===>
```

Las opciones que analizaremos en este tip son las marcadas en azul. Existen más herramientas en las pantallas siguientes de este menú que serán cubiertas en próximos tips.

Opción 1 : Analizar contraseñas por omisión

El comando **ANZDFTPWD** permite acceder a una lista de perfiles de usuarios cuya contraseña es igual al nombre del perfil. Los usuarios con esta característica pueden representar un riesgo para la seguridad del sistema. **Esto puede ocurrir porque en el momento de crear un perfil de usuario con el comando CRTUSRPRF se utilizaron dos defaults que deberían haberse cambiado:** el valor para el parámetro "Contraseña de usuario" (palabra clave PASSWORD) en *USRPRF y el parámetro "Contraseña caducada" (palabra clave PWDEXP) en *NO. La ejecución del mandato ANZDFTPWD ofrece la posibilidad directa de determinar estas situaciones, dejando como resultado un archivo de spool de nombre QPSECPWD con los nombres de los usuarios que se encuentran en esta situación. Es importante observar, en el prompt del comando, que es posible seleccionar una acción a tomar para los perfiles en cuestión. La siguiente pantalla muestra las opciones disponibles:

```
                    Analizar contraseñas p/omisión (ANZDFTPWD)

Teclee elecciones, pulse Intro.

Acción realizada en perfiles . .   *NONE       *NONE, *DISABLE, *PWDEXP
                                   _________

                                                                    Final
```

- ***NONE**: no se toma ninguna acción sobre los perfiles.
- ***DISABLE**: todos los perfiles incluidos en el listado serán puestos en estado *DISABLED (parámetro "Estado" con palabra clave STATUS) en el momento de ejecutar el comando. Los perfiles en este estado no pueden iniciar trabajos interactivos.
- ***PWDEXP**: para todos los perfiles incluidos en el listado, el parámetro "Contraseña caducada" (palabra clave PWDEXP) será establecido a *YES. En el próximo inicio de sesión que se realice con estos perfiles, deberá cambiarse la contraseña.

Observar que pueden seleccionarse *DISABLE y *PWDEXP simultáneamente.

La primer ejecución de ANZDFTPWD genera un objeto de tipo *FILE PF-DTA , de nombre QASECPWD en la biblioteca QUSRSYS, con propietario QSYS y autorización *PUBLIC *EXCLUDE. Este archivo puede ser explotado desde cualquier aplicación, por ejemplo con QUERY/400 (RUNQRY QRY(*NONE) QRYFILE(QUSRSYS/QASECPWD)).

Opciones 2, 3 y 4: Gestión de perfiles de usuario activos

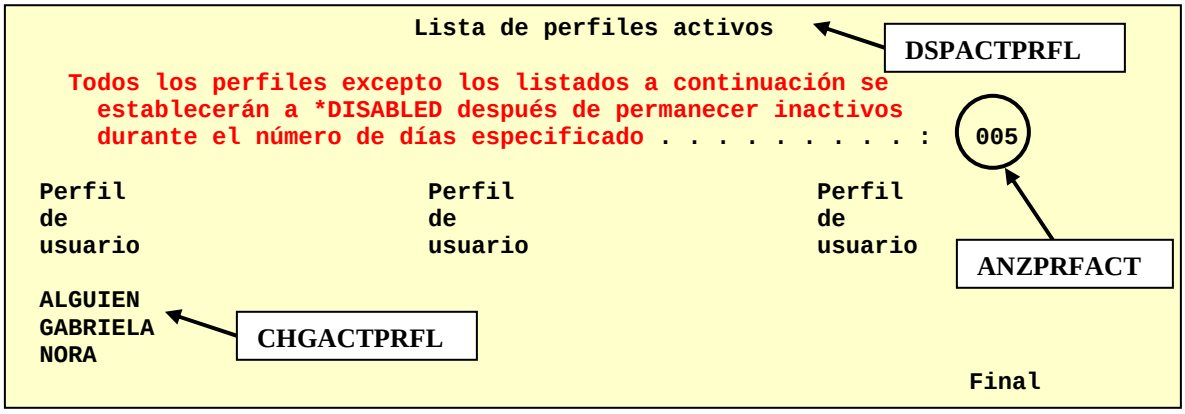
A través de las opciones 2, 3 y 4 se puede planificar que los perfiles de usuario que no hayan iniciado sesión después de un número de días especificado, sean automáticamente pasados a estado *DISABLED. Para habilitar esta función es necesario realizar las siguientes tareas:

1. **Establecer el número de días máximo de inactividad aceptado**: la opción 4 “Analizar actividad de perfil”, comando **ANZPRFACT**, permite especificar la cantidad de días tolerados de inactividad de usuarios.

2. **Cambiar lista de perfiles activos**: la opción 3, comando **CHGACTPRFL**, con el parámetro “Acción” (palabra clave ACTION) en *ADD (es el valor por default) permite agregar a la lista los nombres de los perfiles de usuario que **no serán vigilados en cuanto a su tiempo de inactividad**. **En este caso los usuarios agregados nunca se van a considerar inactivos**. Si en el parámetro “Acción” (palabra clave ACTION) se especifica *REMOVE, el perfil de usuario indicado se eliminará de la lista y se considerará inactivo una vez transcurrido el número máximo de días especificado (especificada con el comando ANZPRFACT).

3. **Visualizar lista de perfiles activos**: la opción 2, comando **DSPACTPRFL**, permite visualizar la lista de perfiles de usuario activos. Estos perfiles de usuario no se van a inhabilitar como resultado de ejecutar el comando ANZPRFACT. La información visualizada depende de lo que se haya especificado en el comando CHGACTPRFL ejecutado previamente.

La siguiente pantalla muestra la ejecución de la opción 2 “Visualizar lista de perfiles activos”:



Considerar lo siguiente:

- Es aconsejable añadir a la lista de la pantalla anterior todos los perfiles que se hayan creado para poseer objetos de aplicación y que no se utilizan para iniciar sesiones. También conviene añadir a esta lista cualquier otro perfil IBM ("Q") que no se desee inhabilitar. En la ayuda de los comandos CHGACTPRFL y ANZPRFACT figura la lista de los perfiles que nunca se considerarán inactivos, entre ellos QSECOFR, QSYS y QTCP.
- La utilización de esta herramienta genera una entrada planificada de nombre QSECIDL1. Para visualizarla utilizar el comando WRKJOBSCDE.
- Si se desea desactivar esta herramienta ejecutar ANZPRFACT INACDAYS(*NOMAX). La entrada planificada será inmediatamente eliminada del WRKJOBSCDE.
- **La ejecución de CHGACTPRFL y ANZPRFACT modifican el contenido de un *FILE PF-DTA existente con propietario QSYS en QUSRSYS de nombre QASECIDL, y autorización *PUBLIC *EXCLUDE.** Este archivo puede ser explotado desde cualquier aplicación, por ejemplo con QUERY/400 (RUNQRY QRY(*NONE) QRYFILE(QUSRSYS/QASECIDL)).

Para tener en cuenta...

- Una forma práctica de evitar usuarios que posean contraseñas igual al nombre del perfil es cambiar el default del parámetro “Contraseña caducada” (palabra clave PWDEXP) del comando CRTUSRPRF. Esto se puede realizar emitiendo el comando: CHGCMDDFT CMD(CRTUSRPRF) NEWDFT(‘PWDEXP(*YES)’) desde una sesión abierta con un perfil con autorización especial *ALLOBJ. Puede referirse al Tip nro 1: “Modificación de los valores por default que rigen en los comandos del OS/400”.
- Para poder ejecutar ANZDFTPWD es necesario tener autorización especial *ALLOBJ y *SECADM.
- Para ejecutar los comandos ANZPRFACT, CHGACTPRFL y DSPACTPRFL se necesita la autorización especial *ALLOBJ. El mandato ANZPRFACT también requiere *SECADM y *JOBCTL.

Copyright Agosto 2001 Teknoda S.A. - AS/400 y OS/400 son marcas registradas de IBM.

Dudas o consultas a nsalmun@teknoda.com.