Services

Drivers.exe (texte)

Intérêt

Affiche la liste des drivers chargés

Syntaxe

drivers | more

La commande affiche les informations sur 5 colonnes.

ModuleName	Code Data	Bss	Paged	Init	LinkDate
Nom du driver	Nom de l'exécutable	???	Taille en mémoire	Taille sur disque	Date du lien

Autoexnt.exe (texte)

Intérêt

AutoExNT est un service qui vous permet d'exécuter un fichier batch sans être logué à la machine.

AutoExNT inclut une option **/interactive** option (identique à celle de la command AT) qui vous permet de voir l'écho de La commande à l'écran. En mode interactif, l'utilisateur connecté est capable d'arrêter le fichier batch.

Fichiers requis

- Autoexnt.exe

- Autoexnt.doc

- Servmess.dll

- Instexnt.exe

Installer AutoExNT

Pour installer le service AutoExNT :
1. Copier Autoexnt.exe et Servmess.dll files dans %*Systemroot*%\System32
2. Créez un fichier batch en l'appelant Autoexnt.bat dans ce même répertoire
4. Tapez à partir de la ligne de commande : **instexnt install ou instexnt install /interactive**

Delsrv.exe (texte)

Intérêt

Permet d'effacer un service installé.

Fichiers requis

- Delsrv.exe

Srvany.exe (texte)

Intérêt

Avec cet utilitaire, vous pouvez configure rune application windows en tant que service. Il est beaucoup plus fonctionnel de l'utiliser avec des applications Win32.

Installation

Tapez à partir de la ligne de commande **instsrv** *NomDuService Chemin***srvany.exe**
Vous pouvez utiliser aussi Srvinstw pour mettre en place le service.

Lancer une application en tant que service

Avec l'éditeur de register, accédez à la clé créée au niveau de l'étape précédente :
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NomDuService\
Dans la sous-clé Parameters, ajoutez la valeur :
Application (REG_SZ)=CheminCompletVersApplication
Si vous entrez les paramètres au niveau de la valeur, utilisez les doubles anti-slashes pour spécifier le chemin complet.
Pour spécifier des paramètres, ajoutez la valeur :
AppParameters(REG_SZ)=Paramètres de la commande
Setting Environment Variables
Spécifiez le repertoire de travail par la valeur :
AppDirectory (REG_SZ)=Répertoire
Vous pouvez aussi au niveau de la valeur application taper :
/D chemin\\Commande RépertoireDeTravail

Fichier(s) requis

- Srvany.exe

Instsrv.exe (texte)

Intérêt

Il installe le service de votre choix.

Syntaxe

instsrv *service-name exe-location*

service-name	exe-location
nom du service (à votre discretion)	Nom de l'exécutable

Désinstaller un service

Pour désinstaller un service, tapez : instsrv service-name remove

Fichier requis

- Instsrv.exe

Sclist.exe (Texte)

Intérêt

Affiche la liste des services et leur état

Fichier requis

sclist.exe

Srvinst.exe(graphique)

Intérêt

Equivaut à la commande instsrv.exe

Fichier requis

srvinst.exe

Svcmon.exe (graphique)

Intérêt

Identique à sclist.exe

Installation et configuration

Pour procéder à l'installation, copiez Svcmon.exe dans %SystemRoot%\System32.
Tapez à l'invite smconfig. Laissez vous guider par l'assistant.

Bogues du Services Monitoring Tools

Pour activer le fichier de logues, créez les entrées suivantes dans la clé :
HKEY_LOCAL_MACHINE\Software\Microsoft\ResKit\Service Monitoring Tool\Logging
Enabled   T (pour Vrai)| F (pour Faux)
LogFile Svcmon.lg (Par défaut)
LogLevel   1 (pas de log) à 7 (le plus haut niveau)

Fichiers requis

- Smconfig.exe - Service Monitoring Tool Configuration Wizard.

- Svcmon.exe - Service Monitoring Tool

Information

Ctrlist.exe (texte)

Intérêt

Donne la liste de tous les objets et compteurs installés dans le langage défini par language ID.

Syntaxe

ctrlist [/c] [LangID] [\\computer] > filename

/c	Crée un fichier CSV
LangID	009 = Anglais(default)
	007 = Allemand
	00A = Espagnol
	00C = Français
\\computer	Nom de la machine distante.
> filename	nom du fichier CSV

Fichiers requis

- Ctrlist.exe

Srvinfo.exe (texte)

Intérêts

Donne les services et les périphériques d'un ordinateur distant

Syntaxe

srvinfo [**-s**] [**-d**] [**-od**] [*computer_name*] [**-?**]

-ns	aucune information sur les services
-d	Visualise les péripéhriques et services
-od	Visualise le disque
\\computer_name	Nom de la machine distante

Fichier requis

srvinfo.exe

Administration : gestion des utilisateurs

Usrtogrp.exe (texte)

Intérêt en fr

Ajoute des utilisateurs existant à un groupe. Le groupe est créé au cas où celui-ic n'existe pas

Intérêt en en

The UsrToGrp tool adds users to a local or global group according to information in a user-specified input text file.

The UsrToGrp tool creates the specified group if it does not already exist. Then, for each user name specified in the file, it searches the specified computer or [domain](#) for the user account. If you are adding users to a local group, the tool also searches trusted domains for the user account. If you are adding users to a global group, the tool only searches the specified domain, not any trusted domains. Once the account is found, UsrToGrp adds the account to the group. Note that if the user name exists in multiple domains, only the first instance of that user name that UsrToGrp finds is added to the group.

UsrToGrp does not create user accounts. Each user specified in the text file you create must have an existing account. For global groups, users must have an account in the specified domain. For local groups, users must have an account on the local computer, the specified domain, or in a trusted domain. Only accounts that exist on your local computer will be used if your Windows NT Workstation computer is a member of a workgroup rather than a domain.

This tool is most beneficial when used in a trusted domain structure. It is useful for granting large numbers of users (1000 max per iteration) membership in a group, especially if you don't know in which trusted domain the user accounts are contained. The tool works on all Windows NT computers.

Note You must be a member of the Administrators or Account Operators group in the specified computer or domain.

Syntaxe

Create a text file with the following format:
domain: domainname
localgroup(or globalgroup): groupname
user1
user2
user3
(etc…)
At the command prompt, type:
usrtogrp *filename*
Where:
filename
is the text file you created in Step 1. If the file is not in the current folder, type the full path to the file.
For example:
c:\reskit> usrtogrp c:\public\tools\file.txt

Exemple

A text file for adding users to a group on the local computer:
domain: localmachine
globalgroup: sms users
user1
user2
user3

Note If you are manipulating a local group, UsrToGrp will also search trusted domains, so user accounts should be specified as "UserName", not "DomainName\UserName".
A text file for adding users to a group on the **maindomain** domain:
domain: maindomain
localgroup: second level administrators
user1
user2
user3
user4

Fichier(s) requis

usrtogrp.exe

Addusers.exe (texte)

Intérêt (fr)

Cette commande permet de créer, supprimer à partir d'un fichier texte. Elle permet aussi de sauvegarder les utilisateurs et les groupes d'un domaine.

Intérêt (en)

This 32-bit administrative tool uses a comma-delimited file to create, write, and delete user accounts. The easiest way to maintain such files is in a spreadsheet, such as Microsoft Excel, that can work with comma-delimited files.
The format for the comma-delimited file requires headings for users [User], global groups [Global], and local groups [Local]. Before you use the **/c** option to create user accounts, it is recommended that you first execute AddUsers with the **/d** switch, the dump accounts option, which writes the headings, user accounts, local groups, and global groups to a file. Viewing this file gives a clearer picture of the structure and headings of the comma-delimited file.
You must be a member of the Administrators group on the target computer to add accounts and a member of the Users group to write accounts.
AddUsers is 100 percent Unicode. The switch **/p:**, followed by **l**, **c**, **e**, **d**, or any combination of the four enables you to specify the four account-creation options available in User Manager: UserMustChangePasswordAtNextLogon, UserCannotChangePassword, PasswordNeverExpires, and AccountDisabled.

Syntaxe
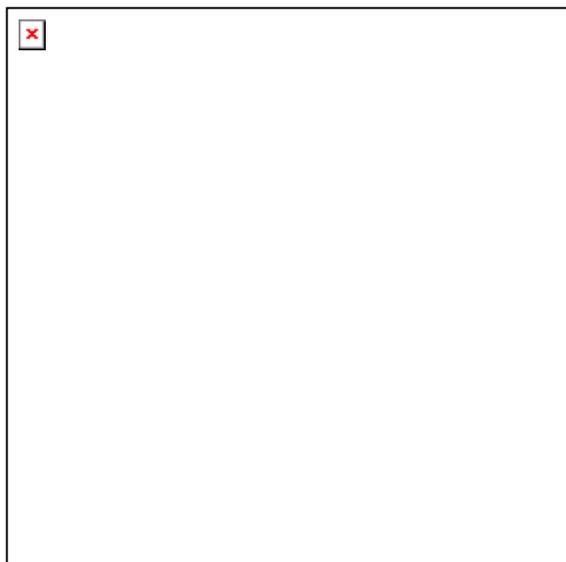
addusers [*computername*] { **/c** [**/p:**{**l** | **c** | **e** | **d**}] | **/d** | **/e** } *filename* [**/s:***x*] [**/?**]

Where: *computername*

is the computer on which you want to create user accounts or from which you want to write user accounts. if you do not specify a computer name, addusers will use the local computer by default. **/c**

creates user accounts, local groups, and global groups as specified by *filename*. **/p:**

followed by **l**, **c**, **e**, or **d**, or any combination of the four, sets the following account-creation options (must be used in conjuction with **/c**):

- **l**
  users do not have to change passwords at next logon.

- **c**
  users cannot change passwords.

- **e**
  passwords never expire (implies **l** option).

- **d**
  accounts are disabled.

if you do not specify this option, all accounts will be created with the usermgr.exe defaults. **/d**

dumps (writes) user accounts, local groups, and global groups to *filename*.
note that choosing to dump current user accounts does not save the account's passwords or any security information for the accounts. to back up security information for accounts, a tape backup should be used.
also, note that since password information is not saved in a user account dump, using the same file to create accounts will cause all passwords of newly created accounts to be empty. all created users will be required to change their password at logon by default. **/e**

deletes user accounts as specified by *filename*.
Caution Be careful when erasing user accounts, as it is not possible to recreate the user account with the same SID. This option, however, cannot erase built-in default accounts.
Also, be aware that when a local or global group is included in the text file, the **/e** switch does not just remove the user from the group, but also eliminates the entire group. *filename*

is the comma-delimited input/output file that addusers will use for data. **/s:***x*

changes the character used for separating fields in the file. the *x* should be replaced with the new character to be used for separating fields. for example, **/s:~** would make the "~" (tilde) the field-separation character.
if this option is not specified, the default separator, a comma (","), is used. **/?**

displays a usage screen with this syntax

Structure du fichier

AddUsers requires that each section in the comma-delimited input/output file have a heading to denote what type of information follows. These headings are [User], [Global], and [Local]. Use the dump users (**/d**) option to create a file that will demonstrate the use of these headings.

Syntax is section-specific for each entry (line) in the different sections, as follows:

[User]

<User Name>,<Full Name>,<Password>,<Home Drive>,<Home Path>,<Profile>,<Script>

[Global]

<Global Group Name>,<Comment>,<UserName>, …

[Local]

<Local Group Name>,<Comment>,<UserName>, …

The entries (lines) in the [Local] and [Global] group sections can have 0 or more <UserName> entries after the comment field. Each user name will be added to that group. Lines must end with a comma (or the appropriate separator character).

Note

- To change the separator character from the default comma, use the **/s:***x* command-line switch.

Exemple

Please note that the blank lines between the sections are not required. If blank lines are used, they must be completely empty (no spaces or tabs, only the return character).

[User]

jimmy,James Edward Phillip II,,,,,,

alex,Alex Denuur,,,E:\,E:\users\alex,,

ron,Ron Jarook,,hello,E:\,E:\users\ron,,

sarah,Sarah Selly,,,,,,

mike,Mike Olarte,,,,,,

[Global]

TestTeam,Regression,ron,alex,

DevTeam,Conversion to Sources,mike,sarah,jimmy,

[Local]

UsersAM,Users A through M,alex,jimmy,mike,

UsersNZ,Users N through Z,ron,sarah,

Fichier requis
addusers.exe
Global.exe (texte)

Intérêt

This command-line tool displays members of global groups on remote servers or domains.

Fichier(s) requis
Global.exe

Local.exe (texte)

Intérêt

This command-line tool displays members of local groups on remote servers or domains.
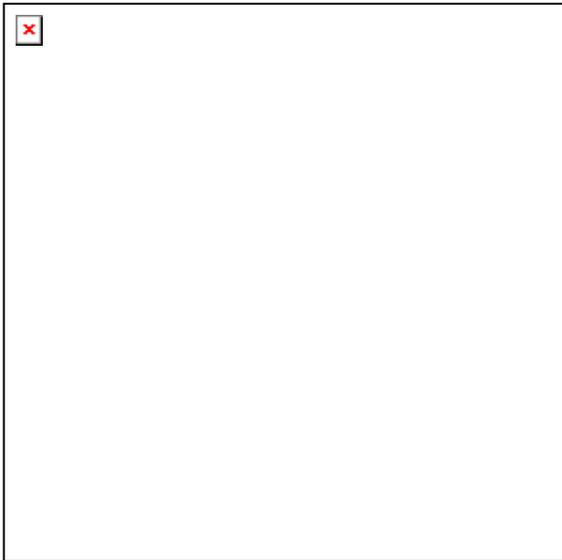
local *groupname* [*domainname* | *****server*]

Where

groupname

is the name of the local group for which to display members.
If groupname is multi-word (containing spaces), it must be enclosed in double quotation marks, for example, "server operators".

domainname

is the name of a network domain.

server

is the name of a network server.

local, run without parameters, displays this usage screen.

Example

local "server operators" nt_domain

[Related Topics](#)

Fichier(s) requis

Local.exe

Showgrps.exe (texte)

Intérêt

This command-line tool shows the groups to which a given user belongs, optionally within a given network [domain](#).

Fichier(s) requis

Showgrps.exe

Showmbrs.exe (texte)

Intérêt

This command-line tool shows the usernames of members of a given group, optionally within a given network [domain](#).

Fichier(s) requis

Showmbrs.exe

Grpcopy.exe (graphique)

Intérêt

Grpcpy is a graphical program that runs only under Windows NT®. It allows users to copy user names from an existing group to another group, in the same domain or in another domain, or on a computer running Windows NT. To use Grpcpy, you must have at least account operator privileges in the affected domains.

Fichier(s) requis

Grpcpy.exe
Grpcpy.doc

Delprof.exe

Intérêt

This tool deletes user profiles on computers running Windows NT.

In Windows NT, user profiles can grow quite large (easily over a megabyte each), which takes up considerable disk space when several people are using one computer. With this tool, administrators can free up disk space taken up by user profiles of users who are no longer working on the computer.

User Profile Deletion Utility can run on a local or remote computer running any version of Windows NT (but not Windows 95/98, as the tool is [Unicode](#)-based).

Caution
This tool deletes everything in a user's profile, including settings, colors, and documents.

Syntaxe

delprof [**/q**] [**/i**] [**/p**] [**/c:***computername*] [**/d:***days*] [**/?**]

Where:

/q
   runs User Profile Deletion Utility in quiet mode, with no confirmation for each profile to be deleted.
/i
   indicates that User Profile Deletion Utility should ignore errors and continue deleting.
/p
   prompts for confirmation before deleting each profile.
/c:*computername*
   specifies a remote computer name on which to run User Profile Deletion Utility.
/d:*days*
   specifies the number of days of inactivity (*days* is an integer). profiles with longer inactivity will be deleted.
/?

displays command-line syntax

Fichiers requis

- Delprof.exe

Creatals.exe (texte)

Intérêt

This command-line utility modifies the DOMAIN_CREATE_ALIAS right on a domain so that only domain administrators can create domain local groups.

The default Windows NT user rights allow non-administrative users to create domain local groups. Domain local groups reside only on domain controllers that share a single security account manager (SAM).

A non-administrative user could potentially abuse the ability to create aliases on a domain by creating a large number of domain local groups and causing the size of the account database to grow without restrictions. Unlimited local group creation could cause the domain controller to crash and create excessive network traffic because of the replication of local group information to backup domain controllers.

This tool must be run by the Domain Administrator on the Primary Domain Controller.

CreatAls runs on Windows NT 4.0 and previous versions on Windows NT.

Syntaxe

creatals [**-d**_account_] [**-g**_account_] [**-a**] [**-r**] [**-?**]

Where:

-d_account_
      denies CreateAlias access to the specified account.
      Note   CreateAlias cannot be denied to Administrators.
-g_account_
      grants CreateAlias access to the specified account.
-a
      restricts access to Administrators/AccountOps only.
-r
      resets the ACL to the Windows NT 4.0 default.
-?
      displays command-line syntax (as does **creatals** without arguments).

You can use any number of arguments. CreatAls, however, doesn't check for consistency in the arguments: it simply processes the arguments one at a time. This means that you should carefully determine the required accesses. For most purposes, you should use the **-a** or the **-r** option. The **-d** and **-g** options allow for greater control, but require more diligence in determining the correct settings.

Fichiers requis

- Creatals.exe

For more information

See Microsoft Knowledge Base Article Q169556 at Microsoft Support Online: http://support.microsoft.com/support

Registre

Associate.exe (texte)

Intérêt

This command-line tool enables you to register or unregister a file name extension with the registry. "File extension, executable program" associations enable the Windows NT shell to launch the correct executable program when a file with the associated extension is opened from the command prompt, from Windows Explorer, or from File Manager.

For example, if you use a lot of files with the extension ".abc" and have an application Abcrun.exe that operates on them, you could associate the extension and application by running:

associate .abc abcrun.exe

Then, whenever a file with the .abc extension is started from the command prompt or from Windows Explorer, Abcrun.exe would be run.

Syntaxe
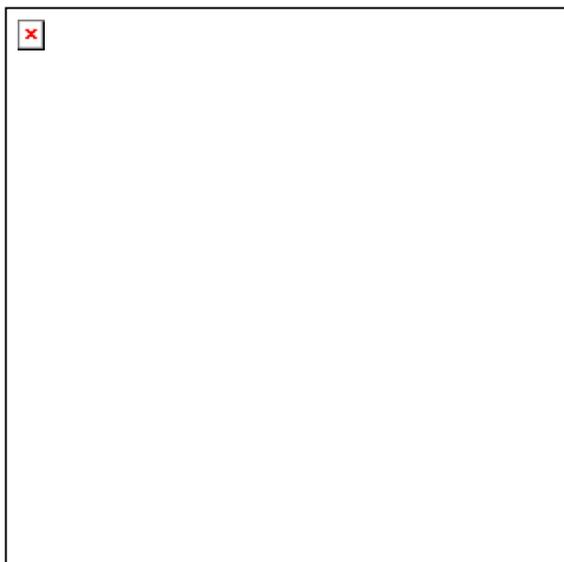
associate *.ext filename* [**/q**] [**/d**] [**/f**] [**/?**]

Where:

.ext

indicates the extension to be associated. *filename*

indicates the executable program to associate *.ext* with. **/q**

(quiet) suppresses all interactive prompts. **/d**

deletes the association if it exists. **/f**

forces an overwrite or delete of the existing entry without questions. **/?**

displays a usage screen.

Return Value

A return value of zero indicates success. Any other value indicates failure.

Exemples

associate .lst notepad.exe

adds the association of .lst with Notepad.exe.

associate .lst notepad.exe /d

removes the association of .lst with Notepad.exe.

associate .lst

returns the name of the associated executable for .lst, if it exists

Fichiers requis

* Associate.exe

Compreg.exe (texte)

Intérêt

This Win32 character-based/command-line "Registry DIFF" enables you to compare any two local or remote registry keys in Windows NT and Windows 95/98.

Syntaxe
compreg *key1 key2* [**-v**] [**-r**] [**-e**] [**-d**] [**-q**] [**-n**] [**-h**] [**-?**]

where

Option	Meaning
key1 key2	Local or remote Registry keys to compare (default: HKEY_CURRENT_USER) (example: \\HOTDOG\HKEY_LOCAL_MACHINE\Software) The Registry subtrees can be abbreviated as follows:
	HKEY_CURRENT_USER cu
	HKEY_CLASSES_ROOT cr
	HKEY_USERS us
	If *key2* is the name of a computer, the key name specified in *key1* is appended automatically.
-v	Verbose. Prints both differences and matches.
r	Recurse into subkeys that only exist in one key.
e	Sets the error level to the error code that was in effect the last time the utility was run. By default, the error level is set to the number of differences that were found.
d	Prints only the value entry names, not the actual values.
-q	Quiet. Prints only the number of differences.
-n	No color in output. By default, color is used.
-h	Displays additional help.
-?	Displays this screen.

Exemples

The following are examples of Compreg usage:
compreg "\lm\system\currentcontrolset\control\session manager" \\MOON

compreg HKEY_CURRENT_USER\Cheech HKEY_CURRENT_USER\Chong

The following are examples of possible output:
1 \Environment!Cpu REG_SZ,[i386]
1 \Memory Management!PagingFiles REG_MULTI_SZ,[C:\pagefile.sys 20|]
2 \Memory Management!PagingFiles REG_MULTI_SZ,[D:\pagefile.sys 43|]
X \AnyKey!AnyValue REG_DWORD,[4]
End of search: 3 differences found.

Fichiers requis

- Compreg.exe

- Compreg.doc

Regdmp.exe (texte)

Intérêt

RegDmp is a command-line tool that writes all or part of the Windows NT registry to the standard output (STDOUT). The output format is suitable for input to Regini.exe.

To access parts of the registry, you must be a member of the Administrators group.

Fichiers requis

- Regdmp.exe

Regfind.exe (texte)

Intérêt

RegFind is a command-line tool with which you can search the registry for arbitrary data, key names, or value names and optionally replace any of these with new values. RegFind has a special flag for finding malformed REG_SZ strings in the registry.

To access parts of the registry, you must be a member of the Administrators group.

Fichiers requis

- Regfind.exe

Regini.exe:

Intérêt

This tool uses character-based batch files to add keys to the registry by specifying a registry script.

You can use a registry editor (RegEdit or RegEdt32) to perform similar tasks as an interactive process, but RegIni supports a wider range of data types than the Registry editors do. RegIni also provides a quick way to add or modify drivers in the registry.

Caution   To add or modify a registry value entry, use administrative tools such as Control Panel or System Policy Editor whenever possible. Using a registry editor (RegEdit or RegEdt32) to change a value can have unforeseen effects, including changes that can prevent you from starting your system.

Syntaxe

To run Regini, at the command prompt, type:

regini *ScriptFile* **[***ScriptFile***…]**

where *ScriptFile* is the filename (and optionally the full path) of a script file used to modify the Windows NT Registry. For example:

regini \\myserver\public\myfolder\srv.**ini**

runs Regini, and directs it to run a script file named Srv.ini from the shared folder \\Myserver\Public\Myfolder.

Creating a Regini Script File

Script File Syntax

In a Regini script file specifying Registry changes, you must locate the subkey containing the value entry to be added or changed on the first line, followed by the intended value of that value entry on the second line, using the following format:

\Registry*Key* [*ACL*]*ValueEntryName* = *DataType Value*

where:

Key	is the name of the key or subkey containing the value entry you
	wish to add or change
ValueEntryName	is the name of the value entry whose value is to be modified
DataType	is the data type used by the value entry
Value	is the intended result
ACL	is an access control list you can choose to include.

The elements of this syntax are explained in more detail below.

If a line contains an equal sign (=), then Regini interprets that line as specifying the value of a Registry value entry.

If a line does not contain an equal sign (=), Regini interprets that line as specifying the name of a Registry key or subkey.

Note Make sure the text editor you use to create the script file inserts a carriage return at the end of each line. Missing carriage returns can cause unpredictable results.

For example, a Regini script file named Srv.ini, in the shared directory \\Myserver\Public\Myfolder, contains the following text:

\Registry\Machine\System\CurrentControlSet\Services\Lanmanserver
    \ParametersDiskSpaceThreshhold = REG_DWORD 0x00000000

The following, typed at the command prompt, adds the **DiskSpaceThreshhold** value entry to the Registry or changes the value that is already there:

regini \\myserver\public\myfolder\srv.**ini**

Note Script files can have any extension. They must be saved in ANSI format, but are converted to Unicode when read from the disk. Currently, there is no way to specify a Unicode text file as the script file.

Line Formatting

The format of the script file is line-based. If you are unable to fit all the information for a Registry subkey name or value entry on one line, use the backslash character (\) as a line-continuation character.

For example:

123456

**1234 **

12

is treated as single line containing:
1234561234 12

Registry Key Names

Key Name Syntax

If a line does not contain an equal sign (=), then the line specifies the name of a Registry key or subkey. In a Regini script file, the subkey name consists of all text from the first non-blank character to the end of the line, including spaces, on any line that does not contain an equal sign.

Leading spaces are significant. If there are no leading spaces, then the named subkey is an absolute path in the Registry.

For example:

\Registry\Machine\Software

–or–

USER:**Control Panel**

In the second example, *USER*: is replaced by the full path to the root of the currently logged-on user's profile (for example, \Registry\Users\S-x-x-xxxx…).

If a line in the script file does not contain an equal sign, and there are one or more spaces at the beginning of that line, then the subkey name on that line is defined in relation to the subkey preceding it in the Registry hierarchy. If the number of leading spaces is the same as in the preceding subkey, then Regini locates the subkey at the same level. If the number of leading spaces is lower, Regini locates the subkey one level higher; if the number is higher, Regini locates the subkey one level lower.

For example:

\Registry\Machine\Software

  Level1a

    Level2a

    Level2b

      Level3a

  Level1b

Kernel and User Key Names

Note that Regini works with Kernel Registry strings. When you access the Registry in User mode to modify the HKEY_LOCAL_MACHINE, HKEY_CURRENT_USER, or HKEY_CURRENT_USER keys, the string is converted to the following in Kernel mode:

- HKEY_LOCAL_MACHINE is converted to \Registry\Machine.

- HKEY_USERS is converted to \Registry\User.

- HKEY_CURRENT_USER is converted to \Registry\User*User_SID*, where *User_SID* is the current user's security identifier (SID).

ACL

After the subkey name, you can optionally specify an access control list (ACL). The ACL is a list of decimal numbers separated by spaces within square brackets. The decimal numbers represent the following user rights:

1. Administrator Full

2. Administrator R

3. Administrator RW

4. Administrator RWD

5. Creator Full

6. Creator RW

7. World Full
8. World R
9. World RW
10. World RWD
11. Power Users Full
12. Power Users RW
13. Power Users RWD
14. System OpFull
15. System OpRW
16. System OpRWD
17. System Full
18. System RW
19. System R
20. Administrator RWX

Value Entries

If a line in a script file contains an equal sign (=), then that line specifies a value for a Registry value entry. The text to the left of the equal sign, if any, is the name of the value entry. The text to the right of the equal sign specifies the data type and value of the value entry. Syntax for specifying a value is as follows:

ValueEntryName = DataType Value

where:

ValueEntryName   is the name of the value entry.

DataType   is the data type.

Value   is the value of the entry.

The value entry name consists of all characters from the first non-blank character on the line to the last non-blank character before the equal sign. The value consists of the first non-blank character after the data type to the end of the line.

Eight data type keywords are supported by Regini. If none is specified, the default data type, REG_SZ, is used. The data types and the format of the values for each are:

Data Type	Value Data	Sets the Registry data type to	Notes
REG_SZ	A string	REG_SZ	REG_SZ is the defaut data type.
REG_EXPAND_SZ	A string	REG_EXPAND_SZ	
REG_MULTI_SZ	One or more strings, each within quotes	REG_MULTI_SZ	
REG_MULTISZFILE	A path to a file	REG_MULTI_SZ	The file is opened and each quoted string is added to the value.
REG_DWORD	A decimal number	REG_DWORD	Use 0x to specify a hexadecimal value, 0o to specify an octal value, and 0b to specify a binary value.

			You can use the strings **On**, **Yes**, or **True**, which are converted to 0x00000001, and the strings **Off**, **No**, or **False**, which are converted to 0x00000000.
REG_BINARY	Two or more decimal numbers	REG_BINARY	The first decimal number must be the number of bytes of data that follow. The remaining numbers are converted into 32-bit numbers. The value length is always a multiple of 4 bytes.
REG_BINARYFILE	A path to a file	REG_BINARY	The named file is opened and its contents stored in the Registry as the value. The length of the value is the length of the file.
DELETE	[No value data]	[No data type]	If this keyword is specified as the data type, the value entry name is deleted.

Fichiers requis

- Regini.exe

- Regini.doc

- User-defined script file

Exemples de scripts

The sample Regini script files included in this section show how to:
- Store a user name to use for automatic logon

- Add a value for the current user in the Exchange client subkey

- Modify several Registry keys at the same time

Storing a user name for automatic administrative logon

This example shows how to use a Regini script to set a user name for an administrative account that can log on automatically to Windows NT.
Start the computer, and press CTRL+ALT+DEL to log on to Windows NT. In the **Logon Information** dialog box, type a user

name and password. The user name you type is stored in the **DefaultUserName** value entry in the Winlogon subkey of the Registry.

To ensure that the value of **DefaultUserName** never changes, create a script file containing the following text:

```
\Registry\Machine
      Software
            Microsoft
                  Windows NT
                        CurrentVersion
                              Winlogon
                                    DefaultUserName = REG_SZ USERNAME
```

where DefaultUserName is the value name, REG_SZ is the data type and *USERNAME* is the desired result or value.

Note To log on automatically to Windows NT, you must supply the password associated with the user name. The password is stored in the **DefaultPassword** value entry in the Winlogon subkey of the Registry. If no password was entered in the **Logon Information** dialog box, you do not need to supply a password in the script file.

To reference the script file, create a batch file containing the following command:

c:**reskit\regini c**:*username*.**ini**

where the name of the script file saved is *Username*.ini.

To ensure that the **DefaultUserName** will not change, however many users log on, place this batch file in the *Systemroot*\Profiles\All Users\Start Menu\Programs\Startup directory.

Adding a value for the current user in the Exchange client subkey

These examples show how to add a value entry for the current user in the Exchange subkey.

You can change the value of Exchange client options in either HKEY_USERS or HKEY_CURRENT_USER.

The following two sample scripts show how to use this information with Regini when you want to add or modify multiple Registry keys.

Example 1

```
\registry\user\software\microsoft\exchange\client\options
      DictionaryLangId = REG_SZ 1033
      PickLogonProfile = REG_SZ 0
```

Example 2

```
\registry\user\S-1-5-21-2185238159-1414228629-1939875897-1000\software\microsoft\exchange\client\options
      DictionaryLangId = REG_SZ 1033
      PickLogonProfile = REG_SZ 0
```

Setting the default user name

This example shows how to use Regini to set the default user name in the **Logon Information** dialog box. This script modifies HKEY_LOCAL_MACHINE.

```
\Registry\Machine
      Software
            Microsoft
                  Windows NT
                        CurrentVersion
                              Winlogon
                                    DefaultUserName = REG_SZ bmiller
```

Exemple complexe

The following scripts were obtained by running the Regdmp utility.

```
\Registry\Machine\Software
   Classes
      AudioCD [10 1 17 5]
         EditFlags = REG_BINARY 0x00000004 0x00000002
         DefaultIcon
            = REG_EXPAND_SZ %SystemRoot%\system32\shell32.dll,40
```

```
      shell
        = play
        play
          = &Play
          command
            = REG_EXPAND_SZ %SystemRoot%\system32\cdplayer.exe \
                        /play %1
Microsoft
  Rpc
      DCOM Protocols = REG_MULTI_SZ  "ncadg_ip_udp" \
                                "ncadg_ipx"    \
                                "ncacn_ip_tcp" \
                                "ncacn_spx" \
                                "ncacn_nb_nb" \
                                "ncacn_nb_ipx"
      NameService
        Protocol=ncacn_np
        NetworkAddress=\\.
        ServerNetworkAddress=\\.
        Endpoint=\pipe\locator
        DefaultSyntax=3
      NetBios
      ServerProtocols
        ncacn_np=rpclts1.dll
        ncalrpc=ncalrpc
        ncacn_vns=rpclts8.dll
      ClientProtocols
        ncacn_np=rpcltc1.dll
        ncalrpc=ncalrpc
        ncacn_vns=rpcltc8.dll
  NetDDE [17 1]
      DDE Shares
        SerialNumber = REG_BINARY 8 0x09000005 0x01000000
        CLPBK$
          fuCmdShow = REG_DWORD 0x7
          ItemList = REG_MULTI_SZ
          NewStyleLink = REG_SZ
          NumItems = REG_DWORD 0x0
          OldStyleLink = REG_SZ
          Revision = REG_DWORD 0x1
          SecurityDescriptor = REG_BINARY 0x6C \
            0x80040001 \
            0x0000004C \
            0x0000005C \
            0x00000000 \
            0x00000014 \
            0x00380002 \
            0x00000002 \
            0x00180200 \
            0x000F03FF \
            0x00000201 \
            0x05000000 \
            0x00000020 \
            0x00000220 \
            0x00180200 \
            0x000002BD \
            0x00000101 \
            0x01000000 \
            0x00000000 \
            0x00000220 \
            0x00000201 \
```

```
                     0x05000000 \
                     0x00000020 \
                     0x00000220 \
                     0x00000201 \
                     0x05000000 \
                     0x00000020 \
                     0x00000220
              SerialNumber = REG_BINARY 8 0x09000005 0x01000000
              Service = REG_DWORD 0x1
              SharedFlag = REG_DWORD 0x1
              ShareName = REG_SZ CLPBK$
              ShareType = REG_DWORD 0x4
              StartAppFlag = REG_DWORD 0x0
              StaticDataLink = REG_SZ ClipSrv|System
```

Regkey.exe (graphique)

Intérêt

RegKey is a GUI tool that can be used to set several registry settings without actually editing the registry.

Use RegKey to set the options for the following:

- Display Shutdown button in Logon dialog.

- Display last user in Logon dialog.

- Parse Autoexec.bat for SET and PATH commands.

- Number of user profiles to cache.

- Default background wallpaper.

- Allow long filenames in FAT.

Fichiers requis

- Regkey.exe

Scanreg.exe (texte)

Intérêt

This Win32 command-line "registry GREP" enables you to search for any string in keynames, valuenames, and/or valuedata in local or remote registry keys in Windows NT and Windows 95/98.

Syntaxe
scanreg [**-s**] *searchstring* [**-k**] [**-v**] [**-d**] [[**-r**]*rootkey*] [**-c**] [**-e**] [**-n**]

where

Option	Meaning
-s	The string to search for
-r	The Registry subtree from which to start searching (default: HKEY_CURRENT_USER).
	Rootkey can be abbreviated as follows:
	HKEY_LOCAL_MACHINE lm
	HKEY_CURRENT_USER cu

| | HKEY_CLASSES_ROOT | cr |
| | HKEY_USERS | us |

-k   Search keynames (Note: You must specify either **-k -v** or **-d**, and you may specify any combination of the three.)

-v   Search value names

-d   Search data

-c   Search case sensitive (default: not case sensitive)

-e   Returns only an exact match (default: returns all matches)

-n   Disables use of color in output (default: keys red, values green, data yellow)

Exemples

Valid examples of Scanreg usage include:

SCANREG -sWindows -k
SCANREG -s:Windows -v
SCANREG -s=Windows -kvc
SCANREG -s Windows -k -ve
SCANREG -s Windows -k -v -dn
SCANREG -s Windows -kvd
SCANREG /s Windows -kvd
SCANREG /s Windows -kvd -rlm
SCANREG /s Windows -kvd -r\software
SCANREG /s Windows -kvd -r\\HOTDOG\lm\system
SCANREG /s Windows -kvd -
   r\\HOTDOG\HKEY_LOCAL_MACHINE\system
SCANREG Windows \lm -kvd
SCANREG Windows -kvd
SCANREG Windows HKEY_CURRENT_USER\software -kvd

Fichiers requis

- Scanreg.exe

- Scanreg.doc

Administration : stratégies et sécurité

Auditpol.exe (texte)

Intérêt

AuditPol is a command-line tool that enables the user to modify the audit policy of the local computer or of any remote computer. To run AuditPol, the user must have administrator privileges on the target computer.

Syntaxe

auditpol [*computer*] [**/enable** | **/disable**] [**/help** | **/?**] [**/**category:*type*] [**/**category:*type*] …

Where:

computer is the name of a remote computer. if no computer name is specified, the operation takes place on the local computer.
/enable enables audit (default).
/disable disables audit.
/category**:**type
    specifies what kind of events to audit
    category can be:

- **system**: system events

- **logon**: logon/logoff events

- **object**: object access

- **privilege**: use of privileges

- **policy**: security policy changes

- **sam**: sam changes

    type can be:

- **success**: audit success events.

- **failure**: audit failure events.

- **all**: audit success and failure events.

- **none**: do not audit these events.

Exemples

Display the audit policy

C:> Auditpol.exe \\computer

Running …

(X) Audit Enabled

AuditCategorySystem = Success and Failure

AuditCategoryLogon = Failure

AuditCategoryObjectAccess = Failure

AuditCategoryPrivilegeUse = No

AuditCategoryDetailedTracking = No

AuditCategoryPolicyChange = No

AuditCategoryAccountManagement = Success and Failure

Enable audit for process category

C:> Auditpol.exe \\computer /process:all

Running …

Audit information changed successfully on \\computer …

New audit policy on \\computer …

(X) Audit Enabled

AuditCategorySystem = Success and Failure

AuditCategoryLogon = Failure

AuditCategoryObjectAccess = Failure

AuditCategoryPrivilegeUse = No

AuditCategoryDetailedTracking = Success and Failure

AuditCategoryPolicyChange = No

AuditCategoryAccountManagement = Success and Failure

Enable/disable audit

C:> Auditpol.exe \\computer /disable

Running …

Audit information changed successfully on \\computer…

New audit policy on \\computer…

(0) Audit Disabled

AuditCategorySystem = Success and Failure

AuditCategoryLogon = Failure

AuditCategoryObjectAccess = Failure

AuditCategoryPrivilegeUse = No

AuditCategoryDetailedTracking = Success and Failure

AuditCategoryPolicyChange = No

AuditCategoryAccountManagement = Success and Failure

C:> Auditpol.exe \\computer /enable

Running …

Audit information changed successfully on \\computer …

New audit policy on \\computer…

(X) Audit Enabled

AuditCategorySystem = Success and Failure

AuditCategoryLogon = Failure

AuditCategoryObjectAccess = Failure

AuditCategoryPrivilegeUse = No

AuditCategoryDetailedTracking = Success and Failure

AuditCategoryPolicyChange = No

AuditCategoryAccountManagement = Success and Failure

Fichiers requis

Auditpol.exe

Windows NT C2 Configuration Manager, can be used to compare the current security configuration on your Windows NT Workstation with C2-level security requirements of the United States government's National Computer Security Center. You can then configure the workstation to conform up to the C2 level.

C2Config.exe (graphique)

Intérêt

C2Config displays the Windows NT parameters that the C2 evaluators felt were critical, along with their current configuration. Selecting one of these items displays more information on the configuration of that item and allows you to change the configuration.

C2Config comes with a .h file that lets users write their own extensions to the application by calling DLLs. C2dll.txt is the text file that explains how this is done.

Fichiers requis

- C2acls.dll
- C2config.exe
- C2config.hlp
- C2config.inf
- C2dll.h
- C2dll.txt

- C2funcs.dll

- C2ntfacl.inf

- C2regacl.inf

Rshxmenu.exe

Intérêt

This shell extension makes it easy to edit security on objects by adding a **Security** menu to the context menu for files which are right-clicked in Windows Explorer.

Instalaltion

To install RshxMenu, right-click Rshxmenu.inf in Windows Explorer, then click **Install** on the popup menu.

RshxMenu is one of the [Power Toys](#).

Fichiers requis

- Rshxmenu.exe (installed)

- Rshxmenu.inf

- Rshxmenu.axp or .x86 (depending on platform)

Installation

Setupmgr.exe(Graphique)

Intérêt

Setup Manager is an administrative tool that enables system administrators to install or upgrade Windows NT on several computers without having to monitor the installations or upgrades.

With Setup Manager, you can create answer files that are used by Windows NT Setup to perform unattended installations or upgrades of Windows NT. Answer files contain the information that Setup would normally prompt users for while it is installing or upgrading Windows NT.

Note that answer files do not automatically eliminate the need for user input when Setup runs. The parameters in answer files must be set so that user interaction is not required.

If you are upgrading an existing Windows NT installation, Setup will use the parameters of the existing installation and ignore parameters specified in the answer file.

Using Setup Manager

You can run Setup Manager from the Tools Management Console, from the command prompt, or by clicking the "Run Setup Manager now" link at the top of this page.

To run Setup Manager from the command prompt, type:

setupmgr

Fichiers requis

- Setupmgr.cnt
- Setupmgr.exe
- Setupmgr.dll
- Setupmgr.hlp
- Setupmgr.inf

Sysdiff.exe (graphique)

Intérêt

Using this tool, you can pre-install applications as part of an automated setup, including applications that do not support scripted installation.

Using SysDiff is a three step process:

1. Create a "snapshot" of Windows NT Workstation after it has been installed on a reference computer. This is the SNAP mode (/snap option).

2. Install the applications you want on the reference computer and create a difference file with information on the these applications. Sysdiff enables you to view this difference file in a readable format. This is the DIFF mode (/diff option).

3. Apply the difference file to new installations on other computers, as part of an unattended setup or at any time after initial installation is complete. This is the INF mode (/inf option).

If many applications must be installed, the difference file can become unmanageably large, as it contains the files and settings for all these applications. In this case, SysDiff enables you to create from the difference file an information (.inf) file containing only [registry](#) and initialization (.ini) file directives. You can then use this information file to install the applications.

To create this separate .inf file, run SysDiff using the **/inf** switch.

Sysdiff.inf is a model information file used to customize SysDiff while the tool is running. Do not use Sysdiff.inf as a model for the kind of .inf file used to apply only registry changes and .ini file changes.

Bogues

How to Troubleshoot SysDiff Error Messages

SysDiff uses the Windows error numbering system to report problems. To determine the meaning of a SysDiff error message, that is, to translate the error number into a message, switch to an MS-DOS prompt and type the following

NET HELPMSG <number>

where <number> is the number of the SysDiff error message.

For example, SysDiff stops responding and the following error message appears:

ERROR MESSAGE: SYSTEM ERROR 5

When you type

NET HELPMSG 5

at an MS-DOS prompt, the meaning of "System Error 5" appears:

Access is denied.

When you use this same method to decode the error message "SYSTEM ERROR 32," the following information appears:

The process cannot access the file because it is being used by another
process.

In this way, you can decode the meaning of the error numbers.

How to Troubleshoot "Installation Failed" Applying .inf

There are many causes for this error message. It is not the purpose of this article to try to catalog all of them. This article shows you how to determine exactly where the apply command is failing and explains some general reasons for such failures.

The .inf file is created by the sysdiff /inf /m command and is automatically placed in the OEM directory. This file contains changes that are to be made to the registry. It also tells you the version of SysDiff that was used to create it, the system root directory and the total diff count.

The .inf file is executed sequentially, from the bottom up. To determine where it has failed, it is necessary to open the file in a text editor (like Notepad) beside the Registry Editor. Each line of the file, following the [AddReg] section heading, represents a single change to the registry. These are abbreviated; HKCR stands for HKEY_CLASSES_ROOT, HKLM stands for HKEY_LOCAL_MACHINE, and so on.

Instead of starting at the bottom and working your way up, it might be better to start at the middle and work your way out. Look at the line in the .inf file and check the registry to see if that line was written. If it was, move to the

halfway mark between there and the end of the file until you find a line that was not written. From there, locate the last line that was written; this will show you the last thing Sysdiff successfully wrote to the registry.

When SysDiff encounters an entry that it cannot write, it stops writing from that point forward and reports the error message "installation failed." SysDiff will then prompt you to continue. SysDiff will continue, but all entries from that point forward are not written. Changes that are made to .ini files are included in the [updateinis] section near the end of the .inf file. If you suspect the problem is in updating .ini files, comment out this section and see if SysDiff will continue.

Debugging .inf files can be a time-consuming process. It is not, however, necessary to do a full SysDiff /apply command to test it each time you comment something out. Because all the Cmdlines.txt is doing is reading the .inf file and writing each entry, you can configure it to do only that:

Copy Cmdlines.txt and the .inf file from the oem directory to the local Windows NT installation.

Copy Cmdlines.txt to a *.bat file (like GO.BAT).

Open the *.bat file in a text editor (like Notepad), delete the [Commands] heading and remove the quotation marks and save the changes.

Carry out the go.bat.

The above procedure is much faster than doing a full SysDiff /apply to debug an error in the .inf file.

Note Make certain that the \%WinDir%\System32 is in the environment path.

Note Make certain that you do this to a computer that has already failed in the installation. The main reason for verifying that this is done to a failed installation as opposed to a clean install is that if the application directories and .ini files do not exist, SysDiff will always return an error when it tries to write to files that are not there.

Behavior You Can Expect if the Problem Is a Bad .inf File

- When you double-click on an application, it starts, and then an hourglass appears and then goes away.

- When you double-click on files in Windows Explorer, you get a message stating that there is no application associated with this file (even though you know that a .xls file belongs to Microsoft Excel, for example).

- Programs do not appear in the Start menu but do appear on the hard disk drive. (This can also be due to forgetting the /m parameter on the SysDiff /inf command line).

Things that cause an .inf file to fail include:

- An attempt to write to a key that the current user no longer has access to or that SysDiff cannot, by its nature, write to. An example of this is a failure to write to changes in the Boot.ini. SysDiff cannot write to a read only file.

- An attempt to write to a key that no longer exists.

- Corrupted diff file (see below).

What to Do if You Suspect a Corrupted Diff File

One of the problems with creating the snapshot, diff, and .inf file over the network is network problems/bottlenecks. The diff file contains an image of all of the files that have been added since the image file was created. Creating this large a file over a network connection can leave you wide open for data corruption.

A corrupted diff file may be the cause when you do everything right, and you verify the integrity of the .inf file (using the Go.bat procedure outlined above) but the apply still fails. Diff files are huge. If there are any network bottlenecks at all, it is easy for these files to become corrupted. To resolve this, try

1. Create the snapshot, diff, and .inf files locally.

2. Manually copy the oem file to the I386 share, then run the unattended installation.

Files Required

- Sysdiff.cnt

- Sysdiff.exe

- Sysdiff.hlp

Mac

Atanlyzr.exe (graphique)

Nettime.exe (texte)

Files Required

Fichiers requis

Nettime.doc - documentation
Nettime.exe - executable file for x86-based computers
Nettime.hqx - self-extracting archive file in BinHex 4.0 format for Macintosh computers
Rtzone.exe - executable file for x86-based computers

Breakftm.exe (texte)

Intérêt

This command-line tool was designed to be used with Windows NT Server 4.0 Unattended Upgrade.

Computers running Windows NT that have the system drive mirrored cannot be upgraded, as a mirrored system drive will cause the Unattended Upgrade to fail. The mirror must therefore be broken before upgrading.

BreakFTM breaks the system mirror before the Windows NT Server 4.0 upgrade, and then recreates the mirror once the upgrade is finished. The tool has no effect on computers that do not have a system mirror.

Use BreakFTM only with Windows NT Server 4.0 Unattended Upgrade. To break or create a mirror manually, use Disk Administrator in Administration Tools (Windows NT Server only).

BreakFTM can be run either through SMS or directly from the command prompt.

Note   BreakFTM can only be used to recover mirrors that were broken by the tool. This tool cannot recover mirrors that were broken manually.

How to use this utility with SMS ***************************************
There are two setup variations for breakftm, that can be found the in the breakftm.pdf. Break System Mirror and Recover System Mirror. Break System Mirror should be scheduled immediately before the NT40 Server Upgrade. Recover System Mirror should be scheduled immediately after the NT 40 Server Upgrade. Breakftm will have no effect on non-mirrored systems so it can be safely used with any NT 40 Upgrade.

How to use this utility from the command line ***************************
Breakftm can also be used directly from the command line. Calling "breakftm /b" from the command line will examine the system drive and break it if it is a mirror. It will then cause a reboot. Calling "breakftm /r" from the command line will try to recover the system mirror (if it was originally a mirror) and reboot.

For advanced command line options type "breakftm /?"
Some Important Information About the Mirror Break/Restore Utility ******
You should not have Disk Administrator running when using the breaftm
utility.
Breakftm can only be used to recover mirror that were broken by the utility. Breakftm cannot recover mirrors that were broken manually.
Breakftm creates a hidden file called mirrorbk.dat in the Windows NT
system directory. This file contains the original mirror information need to recover the mirror. If this file is removed the mirror cannot be restored.
After the mirror is broken and the system has rebooted, the system drive will appear as a normal partition. The shadow will have no drive letter assigned to it, but will still be visible from the Disk Administrator. If an error occurs while recovering the mirror. The mirror can be re-
established manually through the Disk Administrator. To recreate the mirror manually, delete the shadow partition (the partition with no drive letter assigned) and use the free space to recreate the mirror. See Disk Administrator help for more information.

Description of the Success and Error output ****************************
Success No Mirror to Break - The system partition is not a mirror, therefore it does not need to be broken
Success Mirror Broken - The system mirror has been broken successfully

---

Success Mirror Recovered - The system mirror was recovered successfully

Success There Was No Mirror To Recovered - The system partition was not a mirror originally, therefore it does not need to be recovered.

Usage error in calling breakftm.exe - Usage error in calling breakftm from the command line. See breakftm /? For usage.

Error occurred while parsing the Registry - Could not get the disk information out of the registry key. The disk key in the registry may be corrupt, or missing. Mirror not broken/recovered. Break/recover mirror manually.

Error occurred while parsing the Partition Table - The information in the partition table was not what was expected. Mirror not broken/recovered. Break/recover mirror manually.

Drive Letter <> was invalid - The drive letter specified is not valid, or the system drive letter is incorrect. Mirror not broken. Make sure Drive Letter is a valid system partition and retry.

Unknown Registry Version - The disk registry key, is of a version not recognized by this utility. Break mirror manually.

Drive Letter <> was not a Mirror or Simple Partition - Breakftm can only be used to break mirrors. Verify that Drive Letter is a valid Mirror or Simple Partition and retry.

Mirror was Initializing -- The Mirror could not be broken because it was initializing. Wait for the initialization to complete and retry.

Mirror is Unhealthy -- The Mirror could not be broken because it was unhealthy. Please see Disk Administrator Help for more information about Mirror status.

Could not read Mirror data from file mirrorbk.dat - The hidden file mirrorbk.dat is corrupt or missing. Mirror not recovered. Recover mirror manually.

Drive Letter <> does not match Drive Letter of Broken Mirror - The system drive letter has changed. It is unsafe to recover the mirror using this utility. Recover the mirror manually.

Current Partition Table does not match stored mirror data - The partition information on the drives has changed after breaking the mirror. It is unsafe to recover the mirror using this utility. Recover the mirror manually.

Current Registry does not match stored mirror data - The partition information in the registry has changed after breaking the mirror or is missing. It is unsafe to recover the mirror using this utility. Recover the mirror manually.

Unexpected Win32 Error Code # -- An unexpected Win32 error occurred. Mirror not broken/recovered. You may retry, or break/recover the mirror manually.

Unknown Error Occurred - An unknown error and the mirror was not broken/recovered. You may retry, or break/recover the mirror manually.

Fichiers requis

- Breakftm.exe

- Breakftm.pdf

- Breakftm.txt

Showdisk.exe (texte)

Intérêt

This command-line tool reads and displays the registry subkey HKEY_LOCAL_MACHINE\SYSTEM\DISK.

This subkey contains information about each of the primary partitions and logical drives defined on the computer. It also identifies which of the primary partitions and logical drives are members of volume sets, stripe sets, mirror sets, and stripe sets with parity.

Exemple

Opening \SYSTEM\DISK successful
Disk Registry Information Size........ 168
Operating System Version.............. 3
Checksum.............................. 0x140300
Dirty Shutdown?....................... 114

```
......................... 0x0
......................... 0x6d
......................... 0x0
Disk Info Offset..................... 0x2c
Disk Info Size...................... 124
FT Info Offset...................... 0xa8
FT Info Size........................ 0
FT Stripe Width..................... -553123840
FT Pool Size........................ 1311456
Name Offset ......... 0x1402e0
Name Size .......... 5505107
General Disk Information:
Number of Disks..................... 2
........................... 0
Disk #0:
        Number Of Partitions.......... 1
        .................... 0x0
        Signature.................... 0x351d0ce2
        Partition #1:
                FT Type.............. Not a Fault Tolerance Partition
                FT State............. Healthy
                Starting Offset....... 0x4600
                Length............... 212011520
                FtLength............. 0
                ......... 0x0
                ......... 0x0
                Drive Letter.........
                Assign Drive Letter?.. Yes
                Logical Number........ 1
                Ft Group............. Not an FT Partition
                Modified?............ Yes
                ..... 0x0
                ..... 0x0
                ..... 0x0
Disk #1:
        Number Of Partitions.......... 1
        .................... 0x0
        Signature.................... 0xdefa0a19
        Partition #1:
                FT Type.............. Not a Fault Tolerance Partition
                FT State............. Healthy
                Starting Offset....... 0x7e00
                Length............... 527933952
                FtLength............. 0
                ......... 0x0
                ......... 0x0
                Drive Letter.........
                Assign Drive Letter?.. Yes
                Logical Number........ 1
                Ft Group............. Not an FT Partition
                Modified?............ Yes
                ..... 0x0
                ..... 0x0
                ..... 0x0
```

Fichiers requis

- Showdisk.exe

Diskmap.exe (texte)

Intérêt

This command-line tool produces a detailed report on the configuration of the hard disk that you specify. It provides information from the registry about disk characteristics and geometry, and reads and displays data about all of the partitions and logical drives defined on the disk.

A good way to use this tool is to run it for each disk in your computer, print out the configuration report for each disk, and save the hardcopy with the other configuration information that you maintain for your computer. In case of some kinds of disk problems, this information can then be used to reconstruct the hard-disk structure.

Syntaxe

diskmap /d<*drive#*> [**/h**]

Where:

/d<*drive#*>

specifies the number *<drive#>* of the physical disk for which you want a map.

/h

specifies hexadecimal output. The default is decimal output. Some fields are always decimal or always hexadecimal regardless of the value of this parameter. These fields are described in the Disks chapter of the *Microsoft® Windows® NT Workstation and Server Fundamentals* book of the *Microsoft® Windows® NT Resource Kit 4.0.*

Fichiers requis

- Diskmap.exe

Diskuse.exe (texte)

Intérêt

DiskUse is a command-line tool that scans directories on a hard disk and reports on space used by each user.

This tool can scan a single directory, a directory tree, or an entire drive and can extract information on one user or all users. Reports can be displayed on-screen or output to a file, in table or text format. DiskUse can also list all the files owned by a user or users, filtered in a variety of ways.

Syntaxe

/f:<file>   =   Store Results in <file>
Store the output in a file instead of displaying it on the screen. The file name can be a full name, relative name, or UNC. If Table Mode (described below) is specified, the file will be comma delimited. If you specify Table Mode and end the file with a '.csv' extension (Comma Separated Values), it can be directly loaded into Excel.
Examples: /F:OUTPUT.TXT /F:C:\SCAN.DAT /F:\\SERVER\SHARE\DATA.CSV
/e:<file>   =   Store Errors in <file>
Store all error and warning messages in a file instead of displaying them on the screen. The file name can be a full name, relative name, or UNC.
Examples: /E:ERROR.LOG /E:C:\DISKUSE.ERR /E:\\SERVER\SHARE\LOG.ERR

/u:<user>   =   Only Search for <user>
Only scan for and report information about a specific user. The user name should be in the format
DOMAIN\USERNAME. If no domain is specified, it will use the first instance of the user it can find.
Examples: /U:DOMAIN\USERNAME   /U:USERNAME
/s   =   Include Subdirectories
Scan all subdirectories of the path specified.
/t   =   Table Format
Output will be in a table format. If the output is going to a file, the table will be comma delimited. If the output is
going to the screen, the table will be space delimited.
/w   =   Unicode Output (Wide Characters)
By default all output will be in ANSI characters. Use this switch if you have Unicode file names on your server and
wish to have them reported in Unicode format. Unicode will still be read, even if this switch is not present. This
switch only effects the output.
NOTE: Most command windows cannot display Unicode characters, so the output may not be displayed correctly. If
you are sending the output to a file, make sure that the program you are using to read the file supports Unicode as
well (e.g. Notepad).
/q   =   Quiet Mode
No information will be displayed on the screen. If this is used without the /F switch, the program is basically useless.
If this is used without the /E switch, you will not get a report of any errors or warnings.
/? | h   =   Help Screen
Display a brief summary of usage and switches.
/r:<file>   =   Restriction are stored in <file>
Specify a file to read restrictions from. If you want to limit the amount of space a user can use, create a file listing
the user and his/her limit in bytes in the following format:
DOMAIN\USERNAME   <limit>. For example:
ACCOUNTING\FRED   2000000
MARKETING\JUDY   4000000
List one user per line in the file. A line starting with a semi-colon (;) will be considered a remark. Anything after the
limit but before the next line will be considered a remark. All remarks are ignored.
NOTE: This will not stop the user from using more than his/her limit. It will, however, flag that user in the report
and tell you how much over the limit he/she is.
Examples: /R:RESTRICT.TXT   /R:C:\LIMIT.DAT /R:\\SERVER\SHARE\MAX.SIZ
/o   =   Show Only Users Over Limit
Only report information on users that are over their limit. This switch only works if the /R switch is also used. If you
specify /O without /R it will have no affect.
/v   =   Verbose Mode
List all of the files that each user owns. This switch can make the report very large. After listing a user, it will also
list all of the files that user owns, the dates of the files, and the sizes of the files. The format of the output is as
follows:
SIZE : DATE : FILENAME
The only exception is if you are saving the output to disk (/F) and you are using Table Mode (/T), then the output is in
the following format:
SIZE,DATE,FILENAME
/d:a|c|w   =   Date to Display   Access | Create | Write
Specify the date to be display in a verbose output. This has no affect if /V is not specified. The choices are Last
Accessed Date, Date Created, or Last Written To Date.
/n:<number>   =   Display <number> Largest Files Per User
This will list only the <number> largest files for each user. This has no affect if /V is not specified.
/x:<number>   =   Display Files of <number> Bytes or Larger
This will list only files that are <number> bytes or larger. This has no affect if /V is not specified.

        Exemple

diskuse c:\ /s
Displays how much space each user has used on drive c.

diskuse c:\ /s /v /n:5 /x:2000000 /f:c_drive.txt
Stores in the file c_drive.txt how much space each user has used on drive c, and lists under each user the five largest files that are over 2 megs in size.
diskuse c:\ /s /v /o /r:restrict.txt
Displays all of the users that have exceeded there quota on drive c. The quotas are listed in a file called restrict.txt that must be
created before the program is run.
diskuse c:\ /s /u:SALES\GENNY
Displays how much space user SALES\GENNY has used on drive c.
diskuse \\server\share /s /t /f:usage.csv
Stores how much space each user has used on the share \\server\share in the file usage.csv. This file is in table format and can be loaded directly into Excel.
diskuse c:\ /f:c_drive.txt /e:error.log /s /q /r:restrict.txt /v /d:a /n:10
Stores how much space each user has used on drive c in a file c_drive.txt. It also stores the ten largest files each user owns. The date stored with the file will be the last time it was accessed. It will flag any user that is over his/her limit (specified in restrict.txt) and show how many bytes over the limit he/she is. It will store all errors and warnings in a file error.log. No output will be displayed on the screen at all.

Sortie de la commande

E:\diskuse>diskuse e:\ /s
DiskUse   Version 1.2
Scanning Path e:\……………………………………………………………
……………………………………………………………………………………
Resolving Names..
Sorting..
User: BUILTIN\Administrators
Space Used: 517693705
User: ACCOUNTING\bobsmith
Space Used: 688475

Fichiers requis

- Diskuse.exe

- Diskuse.txt

Diskprobe.exe (graphique)

DiskProbe is a sector editor for Windows NT. It allows a user with local Administrator rights to directly edit, save and copy data on the physical hard drive that is not accessible in any other way.

Intérêt

You can use DiskProbe to replace the Master Boot Record, repair damaged partition table information and to repair or replace damaged Partition Boot Sectors or other file system data. The toolcan also save Master Boot Records and Partition Boot Sectors as files. They can then be replaced if the sectors become damaged at a later time. These on-disk data structures are not accessible through the file system, and so are not saved by any backup programs currently available.

Restrictions

- Only users with local Administrator rights can use DiskProbe to access the physical disk. Other users can run DiskProbe, but in the **Open Physical Drive** dialog box, no physical drives will be listed.

- DiskProbe runs under Windows 95, but no physical drives are available. Windows 95 still uses BIOS Interrupt 13 calls for disk access, and does not support the Kernel mode calls necessary to access large physical drives. But under Windows 95 you can still open, edit, and save files as raw hex data.

Utilisation

Although it is a GUI tool, DiskProbe can also be run from the command prompt. Only the path and filename are supported as arguments, for example:

dskprobe c:\mydir\sector00.dsk

This example runs DiskProbe and opens Sector00.dsk in the C:\MYDIR folder.

After the program has been run, double-clicking a file with the .dsk extension will start DiskProbe and load the file.

Caution Because any sector editor allows direct access to a physical drive, it is possible to damage or permanently overwrite critical on-disk data structures. Backup all critical data before using any low-level tool such as DiskProbe. Misuse of low-level tools such as DiskProbe may make all data on a drive or volume permanently inaccessible.

Note These DLLs may be used by other Resource Kit tools.

DiskProbe uses no configuration files. The only change it makes to the registry is to register the shell type and default file extension (.dsk).

Fichiers requis

- Dskprobe.exe

- Dskprobe.hlp

- Mfc40.dll

- Msvcrt40.dll

Scripts

Sleep.exe (texte)

Intérêt

Sleep causes the computer to wait for a specified amount of time. Sleep is useful in batch files and may be more convenient to use than the **at** command in certain cases.

Syntaxe

Add a line in a batch file in the format:
sleep *time*

Where

time

is the number of seconds to pause.

For example:

sleep 3600

will pause for an hour before running the next command in a batch file.

sleep 10

waits 10 seconds.

Fichiers requis

sleep.exe

Soon.exe (texte)

Intérêt

For brief usage details, at the command prompt, type: **soon**. To view Soon's default settings, run **soon /d**.

Soon schedules commands and programs to run in the near future on either the local or a remote computer, by generating and executing an appropriate AT command (part of the Windows NT operating system).

The Soon command closely resembles the AT command because Soon simply generates and executes a suitable AT command. The Schedule service must be running to use the Soon command.

Soon schedules jobs to run at a time relative to the current time (a number of seconds from "now"). Rescheduling a job with Soon therefore requires no editing of the Soon command. Soon can also be used to schedule jobs to run cyclically at intervals of less than one day. You encapsulate the job to be scheduled in a command file, along with a suitable Soon command, then schedule the command file rather than the actual job it encapsulates.

Syntaxe (programmation d'une tâche)

The Soon scheduling command takes the following form:

soon [*computername*] [*delay*] [**/interactive**] "*command*"

Where:

\\computername

Specifies a remote computer on which the command is to be scheduled. If this argument is omitted, the command is scheduled on the local computer.

delay

Specifies when the command is to run, expressed as a number of seconds from now. If this argument is omitted, Soon will use one of its default delay settings, as follows:

- If the job is to be run on the **local** computer, Soon uses its LocalDelay.

- If the job is to be run on a **remote** compute, Soon uses its RemoteDelay.

/interactive

Allows the job to interact with the desktop of the logged on user when the job runs. If this argument is omitted, Soon uses its current InteractiveAlways (**/i**—see Configuration) setting, as follows:

- If InteractiveAlways is **on**, the job will interact with the desktop.

- If InteractiveAlways is **off**, the job will NOT interact with the desktop.

command

Specifies the command to be scheduled (enclosed in double quotation marks).

Syntaxe (configuration)

The Soon configuration command takes the following form:

soon /d [**/l:**n] [**/r:**n] [**/i:**{**on** | **off**}]

Where:

/d

Instructs Soon to modify or display its default settings.

- If **/d** is omitted, Soon assumes that this is a Scheduling command

- If **/d** is specified on its own, Soon displays its current default settings.

- If **/d** is specified with other arguments, Soon modifies its default settings accordingly.

/l:n

Sets the value of LocalDelay—default delay for Local jobs—initially 5 seconds. Specify a positive decimal integer for this value.

/r:n

Sets the value of RemoteDelay—default delay for Remote jobs—initially 15 seconds. Specify a positive decimal integer for this value.

/i:[**on**|**off**]

Sets the value of InteractiveAlways—initially **off**.

Fichiers requis

- Soon.exe

- At.exe (standard Windows NT tool) must be on your path.

- Schedule service (standard Windows NT service) must be running on the target computer.

Timeout.exe (texte)

Intérêt

Timeout is a command-line tool that causes the command processor to pause execution for the number of seconds specified by the time (#) parameter, after which it continues without requiring a user keystroke. A user keystroke, however, will cause execution to resume immediately even if the timeout period has not expired.

The functioning of Timeout is similar to that of the MS-DOS **pause** command merged with Sleep.exe. Timeout is typically used in batch files.

Fichiers requis

- Timeout.exe

Waitfor.exe (texte)

Intérêt

WaitFor is a command-line tool that waits until a signal is given across the network, then carries out a job. Multiple computers can wait for the same signal.

In testing builds of a piece of software, for example, the build computer could send out a signal to several computers running WaitFor once the build has completed successfully. On receipt of the signal, the batch file including WaitFor could instruct the computers to immediately start running tests on the build.

The names of the signals that WaitFor uses are are file-like, independent, and not sensitive to case. Multiple instances of WaitFor can run on a single computer, but each must be waiting for a different signal. A signal can be triggered by using the **-s** option.

WaitFor runs on any version of Windows NT and on Windows 95. On Windows NT, the computer receiving the signal must be in the same domain as the sending computer. On Windows 95, signal names longer than the 8.3 file name format (*xxxxxxx.xxx*) will be truncated, so use of signal names that comply with the 8.3 standard is advised.

WaitFor command-line switches enable you to specify the number of seconds to wait and the name of the signal for which to wait or which to send.

Syntaxe

waitfor [**-t** *timeout*] [**-s**] *signalname* [**-?**]

Where

-t *timeout*

specifies the number of seconds to wait. Default is forever.

-s

sends signalname instead of waiting for it.

signalname

      specifies the signal for which WaitFor waits or which it sends. Signalname is not case-sensitive.

-?

      displays a usage message (as does any error in parsing the command line).

Note   Only one instance of WaitFor can wait for a given signal on a given computer.

Exemples

waitfor -t 10 espresso\build007
waits 10 seconds or until the "espresso\build007" signal is triggered.

waitfor espresso\build007
waits forever (the default) or until the "espresso\build007" signal is triggered.

waitfor -s espresso\build007
triggers the "espresso\build007" signal.

Fichiers requis

- Waitfor.exe

Winat.exe (graphique)

Intérêt

Command Scheduler can be used to schedule commands on a local or remote computer to occur once or regularly in the future. The Workstation service must be started to use this application. This tool is similar to the UNIX CRON tool.

Note   While working in Command Scheduler, press F1 for online Help.

The current AT commands for the local computer are displayed by default when Command Scheduler is started. The list of AT commands is automatically refreshed, so the display is always current. AT commands are displayed in a format similar to that of the command-line AT command.

You can run Command Scheduler from within Windows NT or from the command line.

Note

- For Command Scheduler to work consistently, the Schedule service must be configured for Automatic startup in the Services option of Control Panel. This service is part of the Windows NT operating system, not part of the Resource Kit. For more information click the Help button in the Services option of Control Panel.

- For a full description of the AT command with notes and examples, see the Command Reference in Windows NT Help.

Fichiers requis

- Winat.cnt

- Winat.exe

- Winat.hlp

Choice.exe (texte)

Intérêt

Choice prompts the user to make a choice in a batch program by displaying a prompt and pausing for the user to choose from among a set of keys. You can use this command only in batch programs.

Syntaxe

choice [/**c**[:]*choices*] [**/n**] [**/s**] [**/t**[:]*c*,*nn*] [*text*]
Where:
/c[:]*choices*
specifies allowable keys in the prompt. When displayed, the keys will be separated by commas, will appear in brackets ([]), and will be followed by a question mark. If you don't specify the **/c** switch, Choice uses YN as the default (which displays as [Y, N]). The colon (:) is optional.
/n
causes Choice not to display the prompt. The text before the prompt is still displayed, however. If you specify the **/n** switch, the specified keys are still valid.
/s
causes Choice to be case-sensitive. If the **/s** switch is not specified, Choice will accept either uppercase or lowercase for any of the keys that the user specifies.
/t[:]*c*,*nn*
causes Choice to pause for a specified number of seconds before defaulting to a specified key. The values for the **/t** switch are as follows:
c = the character to default to after *nn* seconds. The character must be in the set of choices specified in the **/c** switch.
nn = the number of seconds to pause. Acceptable values are from 0 to 99. If 0 is specified, there will be no pause before defaulting.
text
specifies text you want to be displayed before the prompt. Quotation marks are necessary only if you include a switch character (/) as part of the text before the prompt. If you don't specify text, Choice displays only a prompt.

Exemples

When you use the following syntax in a batch file:

  choice /c:ync

causes the following to display when Choice is started:

  [Y,N,C]?

Adding text to the syntax:

  choice /c:ync Yes, No, or Continue

causes the following to display when Choice is started:

  Yes, No, or Continue [Y,N,C]?

Using the **/n** switch to leave out the prompt in a batch program:

  choice /n Yes, No, or Continue?

means the user sees only the text you specified when CHOICE is started:

  Yes, No, or Continue?

Using the following syntax in a batch program:

choice /c:ync /t:n,5

means the user sees the following when CHOICE is started:

[Y,N,C]?

If the user doesn't press a key within 5 seconds, CHOICE selects N and returns an ERRORLEVEL value of 2. Otherwise, CHOICE returns the value corresponding to the user's choice.

Notes

ERRORLEVEL is set to the offset of the key that the user presses in choices.

The first key you assign returns a value of 1, the second a value of 2, the third a value of 3, and so on. If the user presses a key that is not among the keys you assigned, CHOICE sounds a warning beep (that is, it sends a BEL, or 07h, character to the console).

If CHOICE detects an error condition, it returns an ERRORLEVEL value of 255.

If the user presses CTRL+BREAK or CTRL+C, CHOICE returns an ERRORLEVEL value of 0.

When you use ERRORLEVEL parameters in a batch program, list them in decreasing order.

Fichiers requis

- Choice.exe

Compress.exe (texte)

Intérêt

This command-line tool can compress one or more files. These compressed files can be expanded with Expand.exe: File Expansion Utility

Syntaxe

compress [**-r**] [**-d**] *source* [*destination*] [**-?**]

Where:

-r
    renames compressed files.
-d
    updates compressed files only if out of date.
source
    specifies the source file. The "*" and "?" wildcards can be used.
destination
    specifies the destination file or path. The *destination* can be a folder. If *source* specifies multiple files and **-r** is not specified, then *destination* must be a folder.
-?
    shows command-line help.

Fichiers requis

- Compress.exe

Applications

Apimon.exe (graphique)

Winalign.exe (graphique)

Depends.exe

Intérêt

Dependency Walker is a graphical Win32 development tool that scans any Win32 module (.exe, .dll, .ocx, .cpl, .scr, and .sys, among others) and builds a hierarchical tree diagram of all dependent modules. For each module found, this tool lists all the functions that are exported by that module, and which of those functions are actually being called by other modules. Another view displays the minimum set of required files, along with detailed information about each file including a full path to the file, base address, version numbers, machine type, debug information, and more.

Dependency Walker can help troubleshoot system errors related to module load problems. During the module scan, Dependency Walker detects dozens of common application problems such as missing modules, invalid modules, import/export mismatches, circular dependency errors, and mismatched machine types of modules.

Dependency Walker is useful for developers, testers, system administrators, creators of setup scripts, and anyone else who needs to examine what dependencies are required to make a specific module load successfully.

You can use Dependency Walker to:

- Find out the minimum set of files required to load a particular application.

- Determine what functions are exported by a particular module (use Dependency Walker instead of LINK /DUMP or DUMPBIN).

- Determine what functions a particular module actually uses in other modules.

- Remove a module as a dependency of your application.

- List the full path, version, base address, or machine type of all modules for a given application.

- Troubleshoot a module load error.

Fichiers requis

- Depends.exe

- Depends.hlp

- Depends.cnt

Internet

Browmon.exe (graphique)

Intérêt

Browser Monitor is a GUI tool that monitors the status of browsers on selected domains. Browsers are shown on a per-domain and per-transport basis.

Fichiers requis

- Browmon.exe

- Browmon.hlp

Réseaux

Browstat.exe (texte)

Intérêt

BrowStat is a general purpose, character-based [browser](#) diagnostic tool. Use BrowStat to find out whether a browser is running and to find active Microsoft Windows for Workgroups (WFW) browsers in Windows NT [domains](#). This tool also provides information about the state of the browser in a workgroup, including the name of the master browser.

You can find out which [transports](#) are on a computer by using the **net config rdr** command and examining the result. In this discussion, "transport" refers to the Windows NT device name (case-insensitive) for the specified transport, in one of the following formats:

\device*transport* (For example: **\device\Nbf_elnk1601**)

transport

transport

Syntaxe

browstat *options*

browstat options

Where:

options

is the whole word or abbreviation from the following list:

ELECT (EL) — Forces a master browser election on the domain that uses the transport specified.

Usage:

browstat elect *transport domain*

GETBLIST (GB) — Retrieves a list of the backup browsers on the domain with the specified transport.

Usage:

browstat getblist *transport* [[*domain*] **refresh**]

GETMASTER (GM) — Uses [NetBIOS](#) to retrieve the name of the browser master for a transport for a workgroup.

Usage:

browstat getmaster *transport domain*

GETPDC (GP) — Uses NetBIOS to retrieve the name of the primary domain controller for a transport for a workgroup.

Usage:

browstat getpdc *transport domain*

LISTWFW (WFW) — Finds Windows for Workgroups computers that are currently running the browser.

If you have a mixed workgroup-and-domain network, you can disable the browser in Windows for Workgroups.

Usage:

browstat listwfw *domain*

STATS (STS) — Dumps various useful browser statistics.

The *****server* switch allows it to be pointed to a specific server.

Usage:

browstat stats [*****server*] [**clear**]

See STATS Example

STATUS (STA) — Dumps browser status for the specified workgroup on all local transports.

It also includes the build number of the browser master and how many servers are in the workgroup.

Usage:

browstat status [**-v**] *workgroup*

See STATUS Example

TICKLE (TIC) — Stops the browser master for the specified workgroup on the specified transport.

It can be used to reset a computer that has been determined to be "bad."

Usage:

browstat tickle *transport domain*

VIEW (VW) — Retrieves the list of servers or domains for a specified server for a specified transport or workgroup.

Usage:

browstat view *transport*

browstat view *transport domain | server* [*/DOMAIN*]

browstat view *transport server /DOMAIN domain*

Valeurs retournées

AFP = AFP Server	PBR = Potential Browser
BBR = Backup Browser	PDC = Primary Domain Controller
BDC = Backup Domain Controller	
DFS = Distributed File System	PQ = Print Server
	S = Server
DL = Dial-in Server	
	SQL = SQL Server

DMB = Domain Master Browser	SS = Windows NT Member Server
MBR = Master Browser	TS = Time Source
MDC = Member Domain Controller	VMS = Vax VMS Server
MFPN = Microsoft File and Print for Netware	W = Workstation
NT = Windows NT	W95 = Windows 95
NV = Novell	WFW = Windows for Workgroups
OSF = OSF Server	XN = Xenix

Exemples

```
C>BROWSTAT STATS
Browser statistics since 20:40:54.705 on 6/9/1993    Time statistics were last cleared
NumberOfServerEnumerations:    237
NumberOfDomainEnumerations:    235
NumberOfOtherEnumerations:    6
NumberOfMailslotWrites:    1974
NumberOfServerAnnouncements:    0
NumberOfDomainAnnouncements:    0
NumberOfElectionPackets:    27425
NumberOfGetBrowserServerListRequests:    0
NumberOfMissedGetBrowserServerListRequests:    0
NumberOfDroppedServerAnnouncements:    0
NumberOfDroppedMailslotDatagrams:    0
NumberOfFailedMailslotReceives:    0
NumberOfMasterAnnouncements:    0
NumberOfIllegalDatagrams:    0
```

Meaning:

NumberOfServerEnumerations: = Number of browse requests for servers

NumberOfDomainEnumerations: = Number of browse requests for domains

NumberOfOtherEnumerations: = Number of "other" browse requests

NumberOfMailslotWrites: = Number of mailslot writes received

NumberOfServerAnnouncements: = Number of server announcements received

NumberOfDomainAnnouncements: = Number of domain (workgroup) announcements received

NumberOfElectionPackets: = Number of browser election packets received

NumberOfGetBrowserServerListRequests: = Number of GetBrowserServerList requests received

NumberOfMissedGetBrowserServerListRequests: = Number of GetBrowserServerList requests missed

NumberOfDroppedServerAnnouncements: = Number of server announcements dropped

NumberOfDroppedMailslotDatagrams: = Number of mailslot writes dropped due to memory

NumberOfFailedMailslotReceives: = Number of mailslot writes dropped due to transport

NumberOfMasterAnnouncements: = Number of WAN master browser announcements

NumberOfIllegalDatagrams: = Number of illegal datagrams received

```
C>BROWSTAT STATUS NTLAN
Status for domain ntlan on transport \Device\Nbf_Lance01
    Master browser name is: MSTRBROWSER1
        Master browser is running build 1.511.1
    3 backup servers retrieved from master MSTRBROWSER1
        \\MYPC
        \\MSTRBROWSER1
        \\BACKUPSVR1
    There are 20 servers in domain ntlan on transport \Device\Nbf_Lance01
    There are 1074 domains in domain ntlan on transport \Device\Nbf_Lance01
Status for domain ntlan on transport \Device\Streams\NWNBLINK
    Master browser name is: MSTRBROWSER1
        Master browser is running build 1.511.1
    3 backup servers retrieved from master MSTRBROWSER1
        \\BACKUPSVR1
        \\MSTRBROWSER1
        \\MYPC DEBUG
    There are 8 servers in domain ntlan on transport \Device\Streams\NWNBLINK
    There are 36 domains in domain ntlan on transport \Device\Streams\NWNBLINK
Status for domain ntlan on transport \Device\Streams\NBT
    Master browser name is: MSTRBROWSER1
        Master browser is running build 1.511.1
    3 backup servers retrieved from master MSTRBROWSER1
        \\MSTRBROWSER1
        \\BACKUPSVR1
        \\MYPC
    There are 11 servers in domain ntlan on transport \Device\Streams\NBT
    There are 101 domains in domain ntlan on transport \Device\Streams\NBT
```

Fichiers requis

- Browstat.exe

Impression

chgprint.exe

Intérêt

This tool assists networkadministrators in managing printer shares.
When an administrator adds or removes a print server, changes a print server's name, or consolidates print queus, the printer connections must be changed manually on every affected desktop.
With Change Printer Utility installed on those desktops, the administrator can simply instruct users to run the tool after changes in print servers. Change Printer changes, adds or removes printer connections. If a replaced printer had been the default printer on a particular computer, the tool makes the replacement printer the default printer.
Change Printer Utility runs only on Windows NT.

Syntaxe

Change Printer Utility also offers command-line usage information. At the command prompt, type:
chgprint /?

Fichiers requis

Chgprint.exe
Chgprint.cnt
Chgprint.hlp

Printmig.exe (graphique)

Intérêt

This printer configuration tool allows you to back up or migrate any print server on which you have administrative rights.

Printer Migrator backs up print server's registry entries and printer drivers into a .cab file. You can then use the tool and the .cab file to restore the printer configuration on the same or any remote Windows NT print server on which you have administrative rights.

This tool can help automate a vital part of enterprise-level deployment: entire print server configurations can be backed up for fault tolerance and replicated to other servers in a fraction of the time that it would take to propagate them manually.

Printer Migrator does not install monitor services because their installation is not standardized among third-party vendors. If a particular monitor needs to be installed, however, the tool prompts the user to do this.

For each platform supported by Windows NT, Printer Migrator includes a separate executable. To backup or restore a configuration to or from a remote computer running Windows NT, the source and target version of the tool do not have to be for the same platform. However, once the backup CAB file has been created, it must be restored to the same platform onto which it was backed up. For example, a .cab file that has been created using an x86-based computer as the source and an Alpha-based computer as the target can only be used to restore the print server configuration onto an Alpha-based computer.

Printer Migrator runs on both Windows NT Workstation and Windows NT Server, and can back up and restore printer configurations between computers running one and computers running the other.

Note

- Printer Migrator replaces rather than merging with an existing printer configuration. So if you restore a printer configuration to a computer, the previous configuration is wiped out. However, you can first use

Printer Migrator to back up the print server, then overwrite it with the new configuration. This leaves the option of restoring the initial setup later.

- To perform Printer Migrator operations, you must have administrative privileges for the computers on which the operations are performed.

Fichiers requis

- Printmig.cnt

- Printmig.exe

- Printmig.hlp

Defptr.exe

Intérêt

For syntax details, at the command prompt, type: **defptr /? or defptr -?**

Using this tool you can easily change your default printer, switching between available network or local printers.

Network printers tend to get busy at erratic intervals, which can require periodically switching the default to avoid "traffic jams." Default Printer allows you to toggle among available printers, local and network. The tool can be used for other purposes as well: for example, to switch printers while working in applications that support only the default printer.

Default Printer can be especially valuable for roaming users, allowing them to quickly select different default printers in different places for a docked notebook computer.

By default, Default Printer runs in tray icon mode. The icon is located next to the clock toward the right end of the Windows NT taskbar. To disable tray icon mode, run **defptr -i**.

Fichiers requis

- Defptr.exe

Environnement

ChkInks.exe (graphique)

Intérêt

Link Check Wizard scans all of the link (shortcut) files on your system, and checks to see if the shortcut points to an existing application or document. If the associated application or document is not found, the Wizard lists that file as a dead link, giving you the option to remove it.

- To find out more information about a particular link, right-click its entry in the list of dead links.

- To remove a link, check the box next to it.

- To remove all of the listed links, click Select All.

When you have selected all of the links you want to remove, click Finish.

Link Check Wizard requires Microsoft Internet Explorer 4.0 or later.

Fichiers requis

- ChkInks.exe

Cmdhere.exe (graphique)

Intérêt

Platform: CmdHere runs only on x86-based computers.

This shell extension adds a **CMD Prompt Here** command to the context menu of folder and drive objects which are right-clicked in Explorer. Selecting this option creates a new command-prompt session with the same path as that of the object.

Installation

To install CmdHere,

1. In Windows NT Explorer, navigate to <*Windows NT 4 Supplement 4 install dir*>\ntrk

2. Right-click **Cmdhere.inf**.

3. In the resulting popup menu, click **Install**.

CmdHere is one of the Power Toys.

Fichiers requis

- Cmdhere.exe (installed)

- Cmdhere.inf

- Cmdhere.x86

Quickres.exe (graphique)

Intérêt

This tool enables you to change your display's visible screen area, resolution (DPI), bit depth, and color palette settings from the taskbar, without restarting Windows NT.

QuickRes resides in the notification area at the right end of the taskbar. Single-click (left) the icon to dynamically select new display settings for your desktop. Double-click (left) to bring up the Display properties applet.

Note   If you select a mode that is incompatible with your video card, simply wait 15 seconds and then press the ESC key. This will return you to the previous resolution.

QuickRes is one of the [Power Toys](#).

Fichiers requis

- Quickres.exe

Runext.exe

Intérêt

Platform: Run Extension runs only on x86-based computers.

This shell extension adds a **Run** command to the context menu for files that are right-clicked in Windows Explorer. Selecting **Run** from the menu opens the **Run** dialog box with the file's path name set in the **Open** field. The cursor is set immediately after the filename to allow the quick entry of parameters for that application.

To install Run Extension, right-click Runext.inf in Windows Explorer, then click **Install** on the popup menu.

RunExt is one of the [Power Toys](#).

Fichiers requis

- Runext.exe (installed)

- Runext.inf

- Runext.x86

TweakUI

Intérêt

Platform: TweakUI runs only on x86-based computers.

This "Control Panel for Type A Personalities" extends your ability to adjust and customize your Windows user interface.

With TweakUI, you can change:

- Menu speed

- Mouse sensitivity

- Window animation and sound

- Shortcut appearance and default names

- Which icons appear on your desktop

- Startup parameters, including whether to start the graphic user interface

- Internet Explorer parameters

You can also create new templates.

The various tweaks are grouped under five tabs: General, Explorer, Desktop, Templates, and Boot.

TweakUI is one of the [Power Toys](#).

Installation

To install TweakUI, right-click Tweakui.inf in Windows Explorer, then click **Install** on the popup menu.

Fichiers requis

- Tweakui.cnt

- Tweakui.cpl

- Tweakui.hlp

- Tweakui.inf

Desktops.exe

Intérêt

Using this desktop-switching application for the Windows platform, you can customize desktop wallpaper and colors, and run programs in their own separate desktops.

DeskTops was formerly known as MultiDesk.

Note   DeskTops provides a similar type of desktop switching capability as workspaces in [CDE](#).

Fichiers requis

- Desktops.exe

Process, mémoire et gestion des tâches

Clearmem.exe (texte)

Intérêt

Clearmem is a command line tool used to force pages out of RAM. This utility attempts to allocate and commit more memory then is physically available, as well as flushing the file cache. In Windows NT, working sets are allowed to grow until memory pressure forces them to decline. Flushing the file cache is important because some pages in the process working set are part of the file cache (for example, code loaded from a file).

Running Clearmem twice will usually force most applications out of memory. Clearmem has to be run multiple times to present a real life memory load because the system does not immediately trim all possible pages in a process working set, but does so gradually over time. When Clearmem is run, the system will pause because of the flood of high priority activity.

To run Clearmem, the computer's paging file must be at least as large as its RAM. If you are running Windows NT Server configured for "Maximize Throughput for Network Applications," , you might have to run Clearmem more than twice to reduce application working sets to the minimum. Use Performance Monitor to check on progress.

Working sets
The working set is a set of memory pages. It is all the physical pages "owned" by a process. Each memory page can be:

- Shared - memory that is shared with some other process or processes. If these other processes are usually running (for example, services.exe or explorer.exe) then the effect of these pages can be ignored as removing them from the working set would not free any pages because they will still be in use.

- Shareable - memory that could potentially be shared with another process but is not. This memory is not shared because there is no demand for its content anywhere else.

- Private - memory which cannot be shared.

Fichiers requis

- Clearmem.exe

Vadump.exe

Intérêt

This command line tool shows the state and size of each segment of virtual address space. It shows the state and size of each segment of virtual address space and can be used to make sure virtual address space is not over-allocated.

VaDump serves as a hard copy of some of the information visible in Pview.

VaDump creates a listing that contains information about the memory usage of a specified process.

Syntaxe

The following is the command-line syntax for VaDump:

vadump -p *pid*

Where:

-p *pid*

specifies the process identifier of the process whose address space is to be listed, in decimal notation.

The list produced by VaDump includes the following:

- Each address, along with its size, state, protection, and type.

- Total committed memory for the image.

- Total committed memory for the .EXE file.

- Total committed memory for each .DLL file, including system .DLL files.

- Total mapped committed memory.

- Total private committed memory.

- Total reserved memory.

- Information about the working set.

- Information about paged and nonpaged pool usage.

Fichiers requis

- Vadump.exe

Tlist.exe (texte)

Intérêt

The Task List Viewer is a command-line tool that displays a list of tasks, or processes, currently running on the local computer. For each process, it shows the process ID number, process name, and, if the process has a window, the title of that window.

Syntaxe

tlist [**/t** | *pid* | *pattern*]

Where:

/t

specifies that the output is to be displayed based on which processes are children/parents of which other processes.

pid

is a process ID. Instructs TList to list module information for this task.

pattern

is a pattern to use (e.g., A*).The pattern can be a complete task name or a regular expression pattern to use as a match. TList matches the supplied pattern against the task names and the window titles.

Exemples

Example 1

Exemple1

The following is an example of output from running **tlist** without the **/t** option. For each process, the process ID, process name, and window title (if any) are shown.

0 System Process

15 System

29 Smss.exe

22 Csrss.exe

17 Winlogon.exe

42 Services.exe

40 Lsass.exe

57 Spoolss.exe

85 Tcpsvcs.exe

111 Locator.exe

102 Rpcss.exe

37 Nddeagnt.exe NetDDE Agent

78 progman.exe Task List

92 Cmd.exe Command Prompt - tlist

49 Ntvdm.exe Microsoft Word - Document2

115 Scm.exe

138 invwin32.exe

158 Tlist.exe

Example 2

The following is an example of output from running **tlist** with the **/t** option.

System Process (0)

System (2)

smss.exe (25)

csrss.exe (33)

Winlogon.exe (39)

Services.exe (45)

Spoolss.exe (74)

Rpcss.exe (88)

Msdtc.exe (98)

Inojobsv.exe (121)

Cisvc.exe (127)

Cidaemon.exe (247)

Inv32cli.exe (139)

Pstores.exe (150)

Rconsvc.exe (155)

Atsvc.exe (165)

wnvtmr32.exe (169)

Wuser32.exe (174)

Dns.exe (184)

Inetinfo.exe (193)

Wnvirq32.exe (201)

NETDDE.EXE (248)

Clipsrv.exe (258)

Isass.exe (48)

Nddeagnt.exe (256)

Explorer.exe (357) Program Manager

Newsalrt.exe (251)

Clipbrd.exe (276) ClipBook Viewer

Winhlp32.exe (323)

Systray.exe (257)

Loadwc.exe (49)

Mgaqdesk.exe (216)

Mgahook.exe (271)

Conf.exe (275)

Realmon.exe (281)

Netwatch.exe (265) Net Watch

Cmd.exe (308) Command Prompt - tlist /t

Tlist.exe (260)

Ddhelp.exe (307)

Climonnt.exe (334)

Example 3

The following is an example of output from running **tlist** with the *pid* option using the crss process with the process ID of 22.

tlist 22

Csrss.exe

WD: D:\BO40\system32\

mdLine: D:\BO40\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,3072,512 Windows

SubSystemType=Windows ServerDII=basesrv,1 ServerDII=winsrv:UserServerDIlInitialization,3 Server

winsrv:ConServerDIlInitialization,2 ProfileControl=Off MaxRequestThreads=16

irtualSize: 38924 KB PeakVirtualSize: 43152 KB

orkingSetSize: 1220 KB PeakWorkingSetSize: 2544 KB

umberOfThreads: 10

34 Win32StartAddr:0x00000000 LastErr:0x00000000 State:Waiting

35 Win32StartAddr:0x00000000 LastErr:0x00000057 State:Waiting

36 Win32StartAddr:0x00000000 LastErr:0x00000000 State:Waiting

37 Win32StartAddr:0x00000000 LastErr:0x00000000 State:Waiting

40 Win32StartAddr:0x00000000 LastErr:0x00000057 State:Waiting

84 Win32StartAddr:0x00000000 LastErr:0x00000057 State:Waiting

220 Win32StartAddr:0x00000000 LastErr:0x00000057 State:Waiting

222 Win32StartAddr:0x00000000 LastErr:0x00000000 State:Waiting

269 Win32StartAddr:0x00000000 LastErr:0x00000006 State:Waiting

299 Win32StartAddr:0x00000000 LastErr:0x00000000 State:Waiting

4.0.1371.1 shp 0x5ffe0000 Csrss.exe

4.0.1381.4 shp 0x77f60000 Ntdll.dll

4.0.1371.1 shp 0x5ff90000 Csrsrv.dll

4.0.1381.4 shp 0x5ffa0000 Basesrv.dll

4.0.1381.4 shp 0x5ffb0000 Winsrv.dll

4.0.1381.4 shp 0x77e70000 User32.dll

4.0.1381.4 shp 0x77f00000 Kernel32.dll

4.0.1381.4 shp 0x77ed0000 Gdi32.dll

4.0.1381.4 shp 0x77dc0000 Advapi32.dll

4.0.1381.4 shp 0x77e10000 Rpcrt4.dll

4.0.1371.1 shp 0x77fd0000 Winmm.dll

1.0.7.0 shp 0x10000000 Wnvwav32.dll

4.0.1381.4 shp 0x0ffb0000 Wow32.dll

4.0.1381.4 shp 0x77c40000 Shell32.dll

4.72.2106.4 shp 0x70ff0000 Comctl32.dll

4.0.1381.4 shp 0x0f000000 Ntvdm.exe

4.0.1381.4 shp 0x77d80000 Comdlg32.dll

4.0.1371.1 shp 0x77a90000 Version.dll

4.0.1371.1 shp 0x779c0000 Lz32.dll

4.0.1381.4 shp 0x5f810000 Rpcltc1.dll

4.0.0.1381 shp 0x74100000 Msacm32.drv

4.0.0.1371 shp 0x75d50000 Msacm32.dll

Fichiers requis

- Tlist.exe

Kill.exe

Intérêt

Use this command-line tool to end one or more tasks or processes. Processes can be killed by process ID number(PID) any part of its process name a window name, usually the applications main window title To find the PID, use PuList or TList, two tools included in the *Windows NT Resource Kit*.

With Kill, you can also specify how the process is to be stopped: you can have Kill send it a command telling it to halt itself, or have Kill force the process to end.

Syntaxe

kill [**/f**] {*process_id | pattern*}

Where:

/f

forces the process to terminate, rather than allowing it to halt itself.

process_id

specifies the ID number of the process to be ended.

pattern

can be either a complete process name, or an expression using wildcards that will be compared to the process names and window titles of all current processes. For example, typing **kill *help*** will end all processes with process names or window titles that contain "help".

Exemples

The first step is to get the process name or ID from Tlist as show below.

TList Sample Output

C:\NTRESKIT>tlist

```
   0 System Process
   2 System
  25 smss.exe
  33 csrss.exe
  39 WINLOGON.EXE
  45 SERVICES.EXE
  48 LSASS.EXE
  74 SPOOLSS.EXE
  88 RPCSS.EXE
 139 INV32CLI.EXE
 168 RCONSVC.EXE
 180 atsvc.exe
 193 WUSER32.EXE
 203 inetinfo.exe
 204 wnvirq32.exe
 245 cidaemon.exe
 259 NDDEAGNT.EXE
  69 EXPLORER.EXE     Program Manager
 275 systray.exe
```

Example: killing the wnvirq32 process by using the process id

C:\NTRESKIT>kill 204
process #204 killed

Example: killing the atsvc process by using the process name

C:\NTRESKIT>kill atsvc
process #180 [atsvc.exe] killed

Fichiers requis

- Kill.exe

Pulist.exe

Intérêt

For syntax details, at the command prompt, type: **pulist -?** or **pulist /?**

This command-line tool displays processes running on local or remote computers. PuList works much like TList, but can also list the user name associated with each process on a local computer.

Note The ability to obtain the username from each process is dependant on whether the caller has sufficient access to the access token in each process. For best results, run PuList from an Administrator account or from the Local System account (running under a service running as Local System).

PuList can be used by network administrators to determine what processes are running on servers and workstations on a network. Furthermore, batch-file developers can redirect the output of the tool to a file and leverage this information in useful ways.

If you know the name of the executeable you're looking for, the following will help narrow your results: pulist|grep notepad

A local computer is specified by running the tool with no commandline arguments. In this case, PuList also attempts to obtain the user name associated with each running process in the system. This is useful if multiple processes are running in the system in different security contexts—PuList provides a mechanism for differentiating such processes from other processes in the system.

Remote computers are targeted by specifying one or more computer names on the command line. PuList displays the computer name followed by a list of running processes. If an error occurred when querying process information on a given computer, the error string will be displayed instead of the process information.

Fichiers requis

- Pulist.exe

Pviewer.exe (graphique)

Intérêt

Process Viewer is a Windows-based tool that displays information about a running process and allows you to stop (kill) processes and change process priority.

Note Process Viewer is similar to Pview.exe, but also allows you to look at processes on remote computers.

Commandes disponibles

The **Process Viewer** dialog box contains the following elements:

Memory Detail
Click this button to see details about memory use for the selected process.

Kill Process
Click this button to stop the selected process.

Caution Do not attempt to kill processes required for running Windows NT. Make sure you understand which program owns a process before attempting to kill it.

Computer
Shows the name of the computer whose processes are currently displayed. Click the **Connect** button and complete the dialog box to view processes for a remote computer.

Process
The name of the process followed by the process ID number (in hexadecimal format) in parentheses.

Processor Time
Processor Time is expressed as a percentage of the elapsed time that a processor is busy executing a non-Idle thread. It can be viewed as the fraction of the time spent doing useful work. Each processor is assigned an Idle thread in the Idle process that consumes those unproductive processor cycles not used by any other threads.

Privileged Time
Privileged Time is the percentage of processor time spent in Privileged Mode in non-Idle threads. The Windows service layer, the Executive routines, and the Windows kernel execute in Privileged Mode. Device drivers for

most devices other than graphics adapters and printers also execute in Privileged Mode. Unlike some early operating systems, Windows NT uses process boundaries for subsystem protection in addition to the traditional protection of User and Privileged modes. These subsystem processes provide additional protection. Therefore, some work done by Windows NT on behalf of your application may appear in other subsystem processes in addition to the Privileged Time in your process.

User Time

User Time is the percentage of processor time spent in User Mode in non-Idle threads. All application code and subsystem code execute in User Mode. The graphics engine, graphics device drivers, printer device drivers, and the window manager also execute in User Mode. Code executing in User Mode cannot damage the integrity of the Windows Executive, kernel, and device drivers. Unlike some early operating systems, Windows NT uses process boundaries for subsystem protection in addition to the traditional protection of User and Privileged modes. These subsystem processes provide additional protection. Therefore, some work done by Windows NT on behalf of your application might appear in other subsystem processes in addition to the Privileged Time in your process.

Process Memory Used

The current number of bytes in the Working Set of this process. The Working Set is the set of memory pages touched recently by the threads in the process. If free memory in the computer is above a threshold, pages are left in the Working Set of a process even if they are not in use. When free memory falls below a threshold, pages are trimmed from Working Sets. If they are needed, they will then be soft-faulted back into the Working Set before they leave main memory.

Process Priority

The current base priority of this process. Threads within a process can raise and lower their own base priority relative to the process's base priority.

Threads

Thread State is the current state of the thread. It is 0 for Initialized, 1 for Ready, 2 for Running, 3 for Standby, 4 for Terminated, 5 for Wait, 6 for Transition, 7 for Unknown. A Running thread is using a processor; a Standby thread is about to use one. A Ready thread wants to use a processor but is waiting for a processor because none are free. A thread in Transition is waiting for a resource in order to execute, such as waiting for its execution stack to be paged in from disk. A Waiting thread has no use for the processor because it is waiting for a peripheral operation to complete or a resource to become free.

Thread Priority

The current base priority of this thread. The system might raise the thread's dynamic priority above the base priority if the thread is handling user input, or lower it towards the base priority if the thread becomes compute bound.

Thread Information

Context Switches/sec is the rate of switches from one thread to another. Thread switches can occur either inside of a single process or across processes. A thread switch can be caused either by one thread asking another for information, or by a thread being preempted by another, higher-priority thread becoming ready to run.

Dynamic Priority is the current dynamic priority of this thread. The system can raise the thread's dynamic priority above the base priority if the thread is handling user input, or lower it towards the base priority if the thread becomes compute bound.

Fichiers requis

- Piewer.exe

Wrkill.exe (graphique)

Intérêt

(You must first install the service before running the tool.)

This service (Rkillsrv.exe) with both GUI (Wrkill.exe) and command-line (Rkill.exe) clients allows a user to enumerate and kill processes on a remote computer. To kill a process remotely with this tool, you must be member of the Administrators group.

Remote Process Kill combines some of the functionality of Tlist.exe and Kill.exe.

The service can be installed with Instsrv.exe or Srvinstw.exe.

Remote Process Kill also includes the following features:

- An installation option to allow the client to automatically install and start the service on a remote system

- An uninstall option

Fichiers requis

- Rkill.exe (command-line version)

- Rkillsrv.exe (service)

- Wrkill.exe GUI version)

Pview.exe

Intérêt

This GUI tool monitors memory usage and threads of running processes. It also enables you to stop running processes.

Fichiers requis

- Pview.exe

Qslice.exe (graphique)

Intérêt

Quick Slice shows the percentage of total CPU usage for each process in the system. This tool is similar to Pstat.exe, but it presents the information in a graphical format.

The Quick Slice Window
Quick Slice displays, for active processes:
PID (Process ID)
The process ID number in hexadecimal format.
Image Name
Identifies the executable filename or process associated with a particular item.
% Process CPU Usage
Identifies the percentage of total CPU usage associated with a particular process.
In the Quick Slice window:
Red bar = Kernel time
Blue bar = user time
For the main window, the length of the bar represents (CPU usage for a single process) / (CPU usage for all processes currently running in the system) * 100.
For the secondary windows, the length of the bar represents (CPU usage for an individual thread) / (CPU usage for all the threads in this process) * 100.
You can specify the sampling interval for Quick Slice at the command prompt. The default is 500 milliseconds.

Fichiers requis

- Qslice.exe

Dotcrash.exe (texte)

Intérêt

Dotcrash is a command-line tool which creates a memory dump of hung or leaking user-mode processes. It is especially useful in production envronments where time limitations make it difficult for you to take a computer offline for debugging purposes. Dotcrash can help you debug the following type of problems:

- Memory leaks

- An application that stops responding at 0 percent (dead lock) CPU usage

- An application that stops responding at 100 percent (busy loop) CPU usage

When you run DotCrash, it produces an application exception that triggers the troubleshooting application Dr. Watson, which is a part of the Windows operating systems. DotCrash does not check to see if the files required to run Dr. Watson are installed in the system. To check this, run Drwtsn32 from the **Run** dialog box (click **Start** and then select **Run**). While Dr. Watson is working on the memory dump, it opens a dialog box: do not click the **Close** or **Cancel** button. Wait until the **OK** button is enabled and then click it.

The memory dump created by Dr. Watson can be loaded into WinDbg, a debugging utility.

Syntaxe

dotcrash [**-b**] *pid* | *process_EXE_name target_file_name*[**-?**]

Where:

-b

> breaks into process without configuring Dr. Watson. This is useful to initiate JIT Debugging or when breaking into a NTSD -D session.

pid

> is the process id in decimal or hex (preface the number with 0x for the latter).

process_exe_name

> is the name of the executable file that owns the process. if multiple .exe files with the same name are found, the errorlevel will be 1 and a list of process ids will be printed to stdout.

target_file_name

> is the name of the memory dump file. Make sure the account the process about to be crashed runs under has sufficient privilege to write to this location.

-?

> displays a syntax screen.

Errorlevel values

- 0 success, dumped a process.

- 1 multiple processes found for %s, use process id.

- 2 process %s not found.

- 3 invalid or out-of-range process id.

- 4 could not open process %s, error:

- 5 could not create thread to crash the process, error:

- 6 can't get debug privilege. aren't you administrator?

- 7 could not access registry to configure dr. watson. tried to fix it.

- 8 this application only runs on windows nt 3.51 or later.

- 9 can't kill process ids 0 and 2.

- 10 could not load psapi.dll. error:

- 11 target file name not allowed when using option -b.

Success message

Process *process_name* has terminated! you should find *process_name*.dmp in your windows directory.

Fichiers requis

- Dotcrash.exe

- Psapi.dll

Pstat.exe (texte)

Intérêt

PStat is a character-based tool that lists all running [processes](#) and [threads](#) and displays their status. This tool is similar to [Qslice.exe](#), but uses a command-line rather than a GUI interface.

The current version of PStat takes a system snapshot and shows [Pmon.exe](#) and old PStat-style data, aong with [Drivers.exe](#) output, in a single output stream. This output can be useful for trouble shooting.

Fichiers requis

- Pstat.exe

Pmon.exe

Intérêt

Process Resource Monitor is a command-line tool that monitors [process](#) resource usage, tracking CPU and memory usage.

Process Resource Monitor can be used to measure Paged and Nonpaged pool usage and can be helpful in identifying kernel mode memory leaks.

Process Resource Monitor also provides a keyboard interface. Use the up and down arrow keys to scroll up and down the list of currently running processes. Use ESC or q to exit Process Resource Monitor. Use any other key to have Process Resource Monitor refresh its display immediately.

Utilisation de la commande Pmon

To Run Process Resource Monitor, at the command prompt, type:

pmon

To Quit Process Resource Monitor, Press CTRL+C or click **Close** on the window menu of the command-prompt window.

Informations retournées

CPU	CpuTime	Mem Usage	Mem Diff	Page Faults	Flts Diff	Commit Charge	Usage NonP	Usage Page	Pri	Hnd Cnt	Thd Cnt	Image Name

CPU: CPU %

Identifies the percentage of total CPU usage associated with a particular process.

CpuTime

Expressed as a percentage of the elapsed time that a processor is busy executing a non-Idle thread. It can be viewed as the fraction of the time spent doing useful work. Each processor is assigned an Idle thread in the Idle process that consumes those unproductive processor cycles not used by any other threads.

MemUsage: Memory Usage

Identifies the total memory used.

Page Faults

Page faults/second is a count of the page faults in the processor. A page fault occurs when a process refers to a virtual memory page that is not in its working set in main memory. A page fault will not cause the page to be fetched from disk if that page is on the standby list, and hence already in main memory, or if it is in use by another process with which the page is shared.

Commit Charge

Displays the size of virtual memory (in bytes) that has been Committed (as opposed to simply reserved). Committed memory must have backing (that is, disk) storage available, or must be assured never to need disk storage (because main memory is large enough to hold it).

Usage NonP: Non-paged usage

The size of the Nonpaged Pool, which is a system memory area where space is acquired by operating system components as they accomplish their appointed tasks. Nonpaged Pool pages cannot be paged out to the paging file, but instead remain in main memory as long as they are allocated.

Usage Page: Page Usage

The amount of the Page File instance in use.

Thd Cnt: Thread Count

Identifies the number of threads for the particular process.

Image Name

Identifies the executable filename or process associated with a particular item.

Notes

The Process Resource Monitor output screen updates every few seconds. An easy way to monitor Process Resource Monitor over time is to copy the screen to a notepad file. Do this once an hour or so while you are running your test. This will make it easier to compare values.

Monitor the Commit numbers on the second row. Constantly increasing numbers over several hours will indicate a probable leak. Total Paged and Nonpaged bytes are the last two items on the second row. Also monitor the Commit Charge column. The process with the leak should have an increasing Commit Charge.

Output

Memory: 130484K Avail: 73872K PageFlts: 25 InRam Kernel: 5524K P:11448K

Commit: 87144K/ 53116K Limit: 250300K Peak: 113904K Pool N: 4352K P:15844K

CPU	Cpu Time	Mem Usage	Mem Diff	Page Faults	Flts Diff	Commit Charge	Usage	NonP	Pri Page	Hnd Cnt	Thd Cnt	Image Name
		19800	0	23075420								File Cache
97	279:00:57	16	0	1	0	0	0	0	0	0	2	Idle Process
0	0:02:42	200	0	3445	0	36	0	0	8	520	38	System
0	0:00:00	200	0	2257	0	164	1	0	11	30	6	smss.exe
1	0:00:05	1092	0	9287	0	1964	5	36	13	383	10	csrss.exe
0	0:00:02	1080	0	7397	0	2376	12	21	13	65	3	WINLOGON.EXE
0	0:00:24	3396	0	48089	2	1412	267	16	9	296	20	SERVICES.EXE
0	0:00:02	1812	0	6590	0	1056	28	10	9	111	13	LSASS.EXE
0	0:00:00	268	0	2457	0	2076	692	14	8	105	9	SPOOLSS.EXE

Fichiers requis

- Pmon.exe

Exctrlst.exe

Intérêt

This tool provides information on the Extensible Performance Counter DLLs that have been installed on a computer running Windows NT, listing the services and applications that provide performance information via the Windows NT registry. You can use these performance counters for optimizing and troubleshooting.

Windows NT Server and Windows NT Workstation are thoroughly instrumented to measure many aspects of performance and status. These measurements are collected in the Performance Registry and can be conveniently displayed using Performance Monitor (Perfmon.exe), a tool provided with Windows NT.

To enable device drivers, system services and applications to display performance data in Performance Monitor along with the standard system measurements, an interface is published to enable the developers of these programs to provide these data to the Performance Registry. Once the information can be read by the Performance Registry, it can be viewed in Performance Monitor. Extensible Performance Counter List reads the registry to find the programs and devices that have registered an Extensible Performance Counter library.

Note ExCtrLst does not test for the existence of the DLLs.

The following table contains descriptions for the different fields displayed in the ExCtrLst dialog box.

Field	Description
Machine name	The name of the machine from which the information is read. The default value is the local machine. However, you can use the name of any machine for which you have permission to read the registry.
Refresh	When you click this button, the utility updates the display with current information from the registry of the selected machine.
Sort Order	The sort order for the items displayed in the **Extensible Performance Counters** list box. The default sort order is **By Library Name**, which sorts the list in alphabetical order by the name of the DLL. If **By Service Name** is selected, the list is sorted by the name of the service entry in the registry.

Extensible Performance Counters	A list box that contains the names of the services that provide performance counters, and the DLL that provides this information. The order is determined by the **Sort Order** selection.
DLL Name	The entry found in the registry for the DLL that the operating system is to load for the performance data provided by this service. Either the file must be located in the system path, or you must provide the fully qualified path to the DLL. If the DLL is not found, the system logs an error in the Application event log.
Open Procedure	The name of the DLL function that initializes the performance functions for the service. This function must be exported by the DLL and must return success. If this function is not found in the DLL or if it returns an error, the system logs an error in the Application event log.
Collect Procedure	The name of the DLL function that collects the performance data for the service. This function is called each time an application, such as Performance Monitor, requests performance data. If this function is not found in the DLL or causes an error, the system logs an error in the Application event log.
Close Procedure	The name of the DLL function that performs any termination or cleanup when the application requesting performance data closes its interface to the performance registry. If this function is not found in the DLL, the system logs an error in the Application event log.
Counter ID Range	When the extensible performance counter DLL is installed, the system assigns a range of Index values to its object and counter name strings. The values assigned during installation are displayed here. If the service uses pre-assigned index values, this entry is not applicable, and the value of this field is **N/A**. If there is a problem with the entry for the service, its counters are not displayed, and this field is **Not Found**.
Help ID Range	When the extensible performance counter DLL is installed, the system assigns a range of index values to its object and counter descriptions. The indices used are the corresponding counter or object name string index + 1. The values assigned during installation are displayed here. If the service uses pre-assigned index values, this entry is not applicable, and the value of this field is **N/A**. If there is a problem with the entry for the service, its counters are not displayed, and this field is **Not Found**.

Note   The values for the **Counter ID Range** and **Help ID Range** fields must correspond to the entries found in the following registry key:
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Perflib*LangID*\Counter
where *LangID* corresponds to the specific entry for the default language on the machine (for example, 009 indicates that the language is English). If these values do not correspond, the counters and objects described for the service are not displayed correctly.

Fichiers requis

- Exctrlst.cnt

- Exctrlst.exe

- Exctrlst.hlp

Heapmon.exe

Intérêt

This command-line tool enables the user to view system heap information.

Syntaxe

heapmon [-?] [-1] [-p *id*] [-t | -a | -f | -d | [-u | -b]] [-(| -)] [-e] [-I]

Where:

-?

displays this message.

-1

specifies to monitor the Win32 subsystem

-p *id*

specifies the process *id* to monitor. Default is to monitor the Win32 subsystem.

-t

sorts output by tag name.

-a

sorts output by #allocations.

-f

sorts output by #frees.

-d

sort output by #allocations - #frees.

-u

sorts output by bytes used.

-b

sorts output by bytes used; same as -u.

-(

Changes #allocations and #frees above to be #bytes allocated and freed.

-)

Changes #allocations and #frees above to be #bytes allocated and freed; same as -(.

-e

enables display of total lines.

-I

enables highlighing of changed lines.

Changing output while HeapMon is running

While HeapMon is running, you can type any of the following switch characters to change the output:

t

sorts output by tag name

a

sorts output by #allocations

f

sorts output by #frees

d

sorts output by #allocations - #frees

u or **b**

specifies the sort output by bytes used

(or **)**

toggles interpretation of #allocations and #frees above to be #bytes allocated and freed.

e

toggles display of total lines.

l

      toggles highlighing of changed lines

? or **h**

      displays help text

q

      quits the program

Fichiers requis

- Heapmon.exe

Leakyapp.exe

Intérêt

This [GUI] testing tool appropriates system memory to see how other applications or the system as a whole runs in low-memory situations.

LeakyApp allocates all available memory to its own [process] and retains the memory until it is stopped or reset. When the tool stops, the memory it has allocated is released.

LeakyApp can show how the system responds to a process that is allocating a disproportionate share of memory. This demonstration can help administrators recognize real applications that behave like LeakyApp.

The **My Leaky App** dialog box displays a status bar representing current space used and space remaining in the paging files on the hard disks of the local computer. If the computer has more than one paging file, the status bar represents the total space in all paging files.

You can observe the effects of memory allocation by watching the LeakyApp paging-file status bar, or by using Task Manager or Performance Monitor, which are included with Windows NT.

Note LeakyApp makes your system run poorly because it restricts memory for all other processes. Run LeakyApp only for purposes of testing or experimentation.

Fichiers requis

- Leakyapp.exe

Perfmtr.exe

Intérêt

At the command prompt, type: **perfmtr**

This command-line tool displays text-based information on the performance of a computer running Windows NT.

Performance Meter can show:

- CPU usage

- file cache usage

- header

- I/O usage

- POOL usage

- Cache Manager reads and writes

- server statistics

- virtual memory usage

- x86 VDM (Virtual DOS Machine) usage

Utilisation

PerfMtr begins by displaying CPU usage. Use the following keystrokes to change the type of performance information displayed:

Key	Displays
c	CPU usage
v	VM usage
f	File Cache usage
r	Cache Manager read and write operations
p	Pool usage
i	I/O usage
x	x86 VDM stats
s	Server stats

The information is periodically updated, and will scroll off the screen.
Type **h** to repeat the header for the current information type.
Type **q** to quit.

Fichiers requis

- Perfmtr.exe

Cpustres.exe

Intérêt

CPU Stress is a command line testing tool consumes processor cycles continuously by executing an endless loop.

Using the CPU Stress Utility, you can:

- demonstrate the effects of priority levels on system performance

- load the processor, so you can test your application when the system is under a heavy load.

- measure the response of your configuration to high processor use

- simulate processor bottlenecks

Note   Runing CPUstress starts one thread for the UI, which is fairly static, and at least one other.

Using Cpustres, you can run a single-threaded or multithreaded process using processor time. You choose the number of threads and set the priorities of the process and its threads, the threads' activity level.

To use CPU Stress Utility, run cpustres.exe. The **CPU Stress** dialog box that appears contains the following fields.

Field	Description		
Process Priority Class			
	Select **Normal** or **High**.		
Access Shared Memory	Click the check box and specify the size of the shared memory, in kilobytes.		
ThreadX	The X is a value from 1 to 4. Each thread has the following properties:		
	Active		Mark the check box to activate the thread. To deactivate the thread, remove the mark.
	Thread Priority		Click **Idle**, **Lowest**, **Below Normal**, **Normal**, **Above Normal**, **Highest**, or **Time Critical**.
	Activity		Click **Low**, **Medium**, or **Busy**.

Fichiers requis

- Cpustres.exe

Dh.exe

Intérêt

Display Heap is a command-line tool to display information about heap usage for user-mode processes or pool usage in kernel-mode memory. It also enables you to lock heaps, tags, stacks, and objects. Display Heap accepts command-line switches to identify which process to display information for and what information to display, and writes formatted output to a text file.

One of Display Heap's most useful functions is to display a list of potential memory hogs and memory allocation calls which have allocated the most memory. However, to identify call sites symbolically the system needs the ability to capture a stack back trace at runtime. This is only supported on checked x86 builds.

Note   Symbols are removed from the standard Windows releases (also known as a retail or 'free' builds) to reduce file size, decrease file load time and increase system performance.

After you've configured your computer, the **-g** option of Display Heap displays a sorted list of call sites that have allocated the most memory. Each call site is identified by a symbolic stack back trace of up to 16 levels which uniquely identifies the code path that resulted in the memory allocations.

On regular builds of Windows, the **-p 0** option displays a list of all Windows kernel objects in the system, along with all handles to those objects for each process. If the **-p 0** option is specified, all references to "heap" in the usage text should be replaced by "pool", as Display Heap is really displaying system pool usage information. The same restrictions apply as on checked x86 builds, but you must enable the **Create Kernel mode stack trace DB** option with Gflags.exe and reboot before the **-g** option will display useful pool information.

Remarques

Before using Display Heap, the following configurations should be made to your system:

1. Back up your registry settings.

2. Start Registry Editor (Regedt32.exe)

Caution   Using Registry Editor incorrectly can cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk.

3. From the HKEY_LOCAL_MACHINE subtree, go to the following key:

4. SYSTEM\CurrentControlSet\Control\Session Manager

5. Change the value of the GlobalFlag entry to 23000. For example:

6. GlobalFlag:REG_DWORD:0X00023000

   Note By default, this value is ZERO or 0x00000000.

7. Ensure the following flags are enabled. Gflags.exe lets you easily change these flags.

   o Enable debugging of the WIN32 subsystem

   o Create user mode stack DB

   o Create kernel mode stack DB

   o Enable loading of kernel debugger symbols

   Note The enabled value of all flags is 00023000.

8. Click **OK** and quit the Registry Editor.

9. If you have a checked build of Windows, install the checked symbol table files into the %WinDir% directory.

   Note Symbol table files must match the version of the image from which they were made. Your Windows CD-ROM contains these files in the \support\debug *<platform>*\symbols directory. If you install a service pack, you must also install the updated symbol table files.

10. Shutdown and restart the computer.

11. After restarting, open a command prompt and type the following command to set the location of the symbol files:

    SET _NT_SYMBOL_PATH=C:\%WINDIR%

After this is completed, you can run Display Heap.

Commutateur -p 0

Use the **-p 0** option to display a list of all Windows kernel objects in the system along with all handles to those objects for each process.

Note Global flag settings still apply when using Display Heap on retail builds of Windows.

Syntaxe

dh {**-p** *n* | **-p -1** | **-p 0** [**-k**] [**-o**]} [**-l**] [**-m**] [**-s**] [**-g**] [**-h**] [**-t**] [**-b**] [**-i**] [**-f** *fileName*] [**--**] [**-?**]

Where:

-p *n*
   displays information about process with clientid of *n* in dh_*n*.dmp. default flags for **-p** *n* are **-s -g**.
-p -1
   displays information about win32 subsystem process in dh_win32.dmp.
-p 0
   displays information about kernel memory and objects in dh_sys.dmp. default flags for **-p 0** are **-m -s -g -t -k -o**.
- **-k**
- displays information about processes and threads (valid only with **-p 0**).

- **-o**
  - displays information about object handles (valid only with **-p 0**).
- **-l**
  - displays information about locks.
- **-m**
  - displays information about module table.
- **-s**
  - displays summary information about heaps.
- **-g**
  - displays information about memory hogs. this option displays a sorted list of call sites that have allocated the most memory. each call site is identified by a symbolic stack >back trace of up 16 levels that should uniquely identify the code path that resulted in the memory allocations.
- **-h**
  - displays information about heap entries for each heap.
- **-t**
  - displays information about heap tags for each heap.
- **-b**
  - displays information about stack back trace database.
- **-i**
  - ignore information about stack back trace database.

-f *filename*

      specifies the name of the file to write the dump to.

--

      specifies the dump output should be written to stdout.

-?

      displays this usage information.

Scénario d'utilisation

When setting up development practices for a new project, many developers like to use a common memory allocation routine, exposed as a macro, which can easily be switched to use a memory leak-tracking version. When the process ends, this memory leak-tracking version dumps any remaining allocated memory chunks, usually stored in a linked list, along with the file name and line-number information on where each allocation was made.

Older projects may not have planned for such memory leak-tracking features. In this case, you can use Display Heap to dump all memory allocations at a beginning point in the test program to a file (Dh_1.dmp, for example), run the stress application for some time, have the stress program pause in a state that should be identical to the first pause, then take another reading with Dh.exe (Dh_2.dmp).

With the two output files, Dh_1.dmp and Dh_2.dmp, you can then use Dhcmp.exe to compare them for any changes in memory usage. Dhcmp.exe will list any memory allocation differences in order of size and tells you a block number for each leak. For each block number, look in the file Dh_2.dmp and go to each allocation history to see a stack back-trace which tells you what chunks of memory are not being freed correctly.

Fichiers requis

- Dh.exe

Dhcmp.exe

Intérêt

This command-line tool compares two dumps of heap usage from Dh.exe, matching the backtraces from each file, to find leaks.

Fichiers requis

- Dhcmp.exe

Gflags.exe

Intérêt

GFlags is a GUI tool that enables a developer or system administrator to edit the NtGlobalFlag settings for Windows NT.

You can use GFlags to modify the current flags in use by the Kernel or the flags used when a particular image file is launched. If you have administrative privileges, you can also use GFlags to modify the global Registry settings that will be used the next time Windows NT starts.

The GlobalFlag registry entry consists of 32 bits that are used as switches to enable or disable several different advanced internal system diagnostics and troubleshooting tests. Only certain flags can be changed for each target. Changes to the Kernel Registry flags do not take effect until the next time Windows NT starts. GFlags only looks at global flags specific to a particular image file when you launch this tool under a debugger or by clicking the GFlags **Launch** button.

GFlags can also set the flag required for the Kernel feature of Oh.exe, a *Microsoft® Windows ® Resource Kit* tool which shows the handles of open windows.

Note   Running GFlags without arguments displays a dialog box that allows the user to modify the global flag settings.

Caution   You should use GFlags only in consultation with Microsoft Technical Support. It is an optional component provided solely for troubleshooting purposes. Incorrect use of this tool might cause system boot failure, or might adversely impact performance. This tool makes modifications to your registry. Changing the registry can have unforeseen effects that can prevent you from starting your computer.

Syntaxe

gflags [**-r** [*flags* [*maxdepth*]]] [**-k** [*flags*]] [**-i** *ImageFileName* [*flags*]] [**-l** *flags commandline*…]

Where:

-r
    operates on system registry settings.
-k
    operates on kernel settings of running system.
-i
    operates on settings for a specific image file.
    If **-i** switch is specified without flags, then current settings are displayed, not modified.
    If flags specified for the **-i** switch are FFFFFFFF, then the registry entry for that image is deleted.
-l
    launches a command line with a specific setting.
flags
    is one of the following:

- A single hex number that specifies all 32-bits of the GlobalFlags value (e.g., 0x1234578).

- One or more arguments beginning with a "+" or "-", where a + means to set the corresponding bit(s) in the GlobalFlags and a - means to clear the corresponding bit(s). The + or - character can be followed by a hex number or a three letter abbreviation for a GlobalFlag. Valid abbreviations are:

Valid Global Flag abbreviations

Abbreviation	Description
bmp	Stop on Hung GUI
d32	Enable debugging of Win32 Subsystem
dhc	Disable Heap Coalesce on Free
dic	Debug Initial Command
dps	Disable paging of kernel stacks
dwl	Debug WINLOGON
ece	Enable Close Exception
edt	Enable Object Dereference Tracking
eel	Enable Exception Logging
eot	Enable Object Handle Type Tagging
hat	Enable Heap API Call Tracing
hfc	Enable heap free checking
hpa	Place heap allocations at ends of pages
hpc	Enable heap parameter checking
htc	Enable heap tail checking
htd	Enable Heap Tagging By DLL
htg	Enable heap tagging
hvc	Enable heap validation on call
idp	Ignore debug priviledge
ksl	Enable loading of kernel debugger symbols
kst	Create kernel mode stack trace DB
otl	Maintain a list of objects for each type
pfc	Enable pool free checking
ptc	Enable pool tail checking
ptg	Enable pool tagging
sls	Show Loader Snaps
soe	Stop On Exception
ust	Create user mode stack trace DB

Note

If no arguments are specified to GFlags then it displays a dialog box that allows the user to modify the global flag settings.

Exemple

Note: Poolmon is located on the Windows NT CD-ROM in the Support directory. It is used to monitor memory tags. With Poolmon you can monitor total Paged and Nonpaged pool bytes. Unless specific global flags are enabled using GFlags, Poolmon will not execute and instead will fail with the following error: "Query pooltags Failed c0000002"

To troubleshoot a memory leak with Gflags and Poolmon

1. Place Gflags.exe and Poolmon.exe on the target system.

2. Run Gflags.Exe without arguments.

3. Select **System Registry** for the Destination

4. Select **Enable pool tagging** from the list of options

5. Click **Apply**.

6. Click **Okay**.

7. Shutdown and restart the computer.

8. Run Poolmon.exe with the following command:

    poolmon.exe -wpooldata.txt -s300 -p -b

Where -w specifies the output file, -s specifies the log interval in seconds; - p sorts tag list by Paged, Non-Paged, or mixed; -b sorts tags by max byte usage. If you change these values do not put a space between w/s and the new value.

Example Output

```
Memory: 16224K Avail: 4564K PageFlts: 31 InRam Krnl: 684K P: 680K
 Commit: 24140K Limit: 24952K Peak: 24932K  Pool N: 744K P: 2180K
 Tag Type    Allocs        Frees        Diff  Bytes      Per Alloc
 -------------------------------------------------------------------
 CM  Paged   1283 (  0)    1002 (  0)    281 1377312 (    0) 4901
Strg Paged  10385 ( 10)    6658 (  4)   3727 317952 (  512) 85
 Fat  Paged   6662 (  8)    4971 (  6)   1691 174560 (  128) 103
MmSt Paged    614 (  0)     441 (  0)    173  83456 (    0) 482
```

The columns show usage for each tag name. By monitoring periodically which tag's bytes are increasing in allocation without being freed up you may be able to identify a possible leakage.

Référence

The following are global tags for Windows NT:

Flag Name	32 Bit Hex Value
FLG_STOP_ON_EXCEPTION	0x00000001
FLG_SHOW_LDR_SNAPS	0x00000002
FLG_DEBUG_INITIAL_COMMAND	0x00000004
FLG_STOP_ON_HUNG_GUI	0x00000008
FLG_HEAP_ENABLE_TAIL_CHECK	0x00000010
FLG_HEAP_ENABLE_FREE_CHECK	0x00000020
FLG_HEAP_VALIDATE_PARAMETERS	0x00000040
FLG_HEAP_VALIDATE_ALL	0x00000080
FLG_POOL_ENABLE_TAIL_CHECK	0x00000100
FLG_POOL_ENABLE_FREE_CHECK	0x00000200
FLG_POOL_ENABLE_TAGGING	0x00000400
FLG_HEAP_ENABLE_TAGGING	0x00000800
FLG_USER_STACK_TRACE_DB	0x00001000
FLG_KERNEL_STACK_TRACE_DB	0x00002000

FLG_MAINTAIN_OBJECT_TYPELIST	0x00004000
FLG_HEAP_ENABLE_TAG_BY_DLL	0x00008000
FLG_IGNORE_DEBUG_PRIV	0x00010000
FLG_ENABLE_CSRDEBUG	0x00020000
FLG_ENABLE_KDEBUG_SYMBOL_LOAD	0x00040000
FLG_DISABLE_PAGE_KERNEL_STACKS	0x00080000
FLG_HEAP_ENABLE_CALL_TRACING	0x00100000
FLG_HEAP_DISABLE_COALESCING	0x00200000
FLG_ENABLE_CLOSE_EXCEPTIONS	0x00400000
FLG_ENABLE_EXCEPTION_LOGGING	0x00800000
FLG_ENABLE_HANDLE_TYPE_TAGGING	0x01000000
FLG_HEAP_PAGE_ALLOCS	0x02000000
FLG_DEBUG_INITIAL_COMMAND_EX	0x04000000
FLG_VALID_BITS	0x07FFFFFF

These values are stored in the registry in the the following location:

HKEY_LOCAL_MACHINE subtree in the following key:

\SYSTEM\CurrentControlSet\Control\Session Manager

GlobalFlag REG_DWORD

The default value for GlobalFlag is 0, so Windows NT does not expend extra overhead in gathering pooltag information. If set to 0, all system registry global flag settings are disabled. For more information, see the definition of Ntexapi.h FLG_ in the Win32 Software Development Kit.

Gflags can also set the flag required for the Kernel feature of Oh.exe, a *Microsoft® Windows NT® Resource Kit* tool that shows the handles of open windows.

Fichiers requis

- Gflags.exe

Oh.exe

Intérêt

This command-line tool shows the handles of all open windows. Alternatively, you can constrain the OH display to show only information relating to a particular process, object type, or object name. This feature is useful for finding which process has a file open when a sharing violation occurs.

To function properly, OH requires that an option internal to the kernel be enabled. This option maintains a linked list of all objects by object type. If OH detects that this option is not set, it sets it and sends a message that the user must reboot before the option will take effect. After rebooting, OH can give useful results.

This linked list uses 8 bytes of overhead per object. If desired, this option can later be disabled with Gflags.exe. To disable this option in Gflags.exe, clear the check box for "Maintain a list of objects for each type" in the Global Flags window, then restart the computer.

Fichiers requis

- Oh.exe

Presse-papiers

Clip.exe (texte)

Intérêt

For syntax details, at the command prompt, type: **clip /?** or **clip -?**

This command-line tool copies text from the STDIN stream to the Windows Clipboard. You can then paste the data directly into any application that can receive text from the Clipboard.

To use Clip

Run any program that prints text to STDOUT and pipe the results through Clip. Clip reads from STDIN and copies the text to the Clipboard. Then, using the **Paste** command, copy the text to any application that can receive text from the Clipboard.

Exemples

Example 1

dir | clip

copies a folder listing onto the Clipboard. Next, run Wordpad (or a similar text editor) and choose **Edit**, then **Paste** from the menu bar to paste the folder listing into Wordpad.

Example 2

clip < readme.txt

places a copy of the contents of Readme.txt onto the Clipboard.

Example 3

awk -f gencode.awk input.txt | clip

places the output of the AWK program Gencode.awk onto the Clipboard.

Fichiers requis

- Clip.exe

Clipstor.exe (graphique)

Intérêt

For help on using Clipstor, press F1 while the tool has focus.

This GUI tool manages multiple Clipboard text buffers. It allows you to retrieve text from the Clipboard and store it in one of its buffers, and paste any of its buffers to the Clipboard, with your mouse.

Utilisation

- To store text in a Clipstor buffer, simply copy the text as you normally would under Windows. Then right-click a pane in the Clipstor window to insert the text into that pane.

- To copy a text buffer from Clipstor to the clipboard, left-click the pane that contains the text you want to copy.

- To clear a Clipstor buffer, hold down the Shift key and right-click the pane you want to erase.

- To make Clipstor the top-most window, hold down the control key and left click on any pane.

- To change the number of panes in the WinMB window, pass a number on the command line to Clipstor, in the form **clipstor** *x*, where *x* is an integer. The default is 5 panes. For example, running **clipstor 10** would create 10 panes and make that the default by storing the value in the registry.

Fichiers requis

- Clipstor.exe

Cliptray.exe

Intérêt

This tool allows you to store and organize chunks of text and copy them into text-based files using the clipboard. It is useful for developers, authors, support personnel, Webmasters, or anyone who needs to use the same text multiple times.

When you start ClipTray, the ClipTray icon appears in the system tray. Right-clicking on this icon brings up the ClipTray menu, containing the titles of your current entries and options for adding more. Clicking on the ClipTray Entry you wish to use will place it into the Windows clipboard, ready for pasting into any program.

ClipTray also has the ability to use more than one ClipTray text file, allowing you to access your entries by project or to distribute entries to other members of your team.

Fichiers requis

- Cliptray.cnt

- Cliptray.exe

- Cliptray.hlp

- Comdlg32.ocx

- Msgblast.ocx

- Vb40032.dll

Netclip.exe (graphique)

Intérêt

NetClip is a GUI tool that enables you to view the contents of the Clipboard of another computer on the network, and to drag and drop (or cut and paste) any data, in any format, to and from the other computer. The same user must be logged into both computers when using NetClip.

To share the clipboard between the two computers, NetClip uses the Microsoft Component Object Model (COM). It fully supports Rich Text Format (RTF) as well as any custom data format supported by your applications.

To use this tool, simply run Netclip.exe. When it starts you'll be viewing your local clipboard. To connect to another computer, click the Connect button on the Toolbar and enter the computer name. You can enter a NetBIOS name (for

example, "mycomputer"), a [DNS](#) name (for example, "mycomputer.mysite.com"), or an [IP address](#) (for example, "127.0.0.1"). The Disconnect button terminates the connection with the remote computer.

You can also pass a computer name on the command line, allowing you to put a shortcut on your desktop for each of your computers.

NetClip requires Windows NT 4.0 to view and modify the clipboard on another computer. It also works on Windows 95 or Windows 98 as a local clipboard viewer only.

NetClip is one of the [Power Toys](#).

Note

- To allow clients access to a server's Clipboard via NetClip, you must grant the user launch and access permissions on the server computer. You can do this with either [Oleview.exe: OLE/COM Object Viewer](#) or Dcomcnfg.exe, a program located in the %System32% directory.

- If you receive an "Access denied" error when attempting to connect to a remote server's Clipboard, make sure that "Enable distributed COM on this computer" is checked on the Default Properties tab of Dcomcnfg.exe, a program located in the %System32% directory.

Fichiers requis

- Netclip.exe

- Netclipps.dll

Messagerie et téléphonie

Tlocmgr.exe

Intérêt

Telephony Location Manager was written for laptop computer users who use telephone applications, such as Dial-Up Networking, from several locations. It is useful for anyone who changes TAPI (Telephony API) locations—for example, taking a laptop from the office to home, where the computer no longer has to dial a "9" prefix. For a laptop user with a hot-docking setup, this utility will automatically change the TAPI location.

When you start Telephony Location Manager, an icon appears in your Taskbar notification area (near the clock).

A menu from this icon enables you to quickly:

- change your current TAPI location (click the icon with the left mouse button).

- bring up dialing properties (click with the right mouse button).

- run Phone Dialer (click with the right mouse button).

Telephony Location Manager is one of the Power Toys.

Fichiers requis

- Tlocmgr.exe

Clusters

Cluster Verification Utility

Intérêt

Platform: Cluster Verification Utility runs only on x86-based computers.

This tool verifies that two-node cluster systems are set up properly. The minimum requirements for a server cluster are (a) two servers connected by a network, (b) a method for each server to access the other's disk data, and (c) special cluster software like Microsoft® Cluster Server (MSCS), which is included in Windows NT Server, Enterprise Edition.

CVU includes two tests: Configuration Verification and Shared SCSI Drive Diagnostic Verification.

- Configuration Verification allows you to verify that the two cluster nodes are able to communicate with each other, and that both of them are able to access the same shared SCSI drive or drives.

- Shared SCSI Drive Diagnostic Verification tests a shared SCSI Bus for functionality that is required by by Microsoft Cluster Server systems.

  Caution   This test is destructive. It will destroy data on all disks on the shared bus.

Clustering technology enables you to connect a group of servers in order to enhance data availability, server manageability, and performance. Regardless of how many servers are connected in a cluster, a workstation will treat it as if the cluster were a single server. Cluster configurations are used to address availability, manageability, and scalability.

- Availability. When a system or application in the cluster fails, the cluster software respond by restarting the failed application or dispersing the work from the failed system to the remaining systems in the cluster.

- Manageability. Administrators use a graphical console to move applications and data within the cluster to different servers. This is used for manually balancing workloads and for unloading servers for planned maintenance without downtime.

- Scalability. When the overall load for a cluster-aware application exceeds the capabilities of the systems in the cluster, additional systems can be added to the cluster. Formerly, customers who desired future system expansion capability needed to make up-front commitments to expensive, high-end servers that provided space for additional CPUs, drives, and memory. With clustering and cluster-aware applications, customers will be able to add systems as needed to meet overall processing power requirements.

Fichiers requis

Cluster Verification Utility must be installed separately from the *Windows NT Resource Kit*, using Setup.exe.

- Setup.exe – An installation program which copies all the CVU files to a \CVU directory on the local hard drive.

- Wpcvp.exe – The main CVU executable, containing the Configuration Verification codes.

- Wpcvp.hlp – The CVU Help file.

- Clustsim.exe – The execution file for Shared SCSI Drive Diagnostic Verification.

- Ntlog.dll

- Readme.txt - The Clustsim documentation

Sites

For more information on clustering, see

- http://premium.microsoft.com/msdn/library/backgrnd/html/msdn_clustfaq.htm

- http://www.microsoft.com/ntserver/support/faqs/clustering_faq.asp

Aide

Regentry.hlp : toutes les entrées sur la base de registre

Counters.hlp

Auditcat.hlp

Profiles.doc

Utilitaires

Creatfil.exe (texte)

Intérêt

This command-line tool creates zero-filled files of a size you specify.

Create File must be run from the command prompt; it cannot be run from the **Run** command on the **Start** menu.

Syntaxe

creatfil *filename* [*filesize*]

Where:

filename
        is the name of the file to create.
filesize
        is the size of the file to create, in units of 1024 bytes. This argument is optional. The default is 1024 bytes.

Exemple

c:\>creatfil workfile.dat 100

creates a 102,400 byte (100K) file of zeros called workfile.dat.

Fichiers requis

- Creatfil.exe

Timezone.exe (texte)

Intérêt

This command-line tool updates the daylight savings information for a time zone in the registry. In some countries, the start and end of daylight savings time are changed every year, and there is no fixed start or end date.

This tool runs on Windows NT and Windows 95/98.

Fichiers requis

- Timezone.exe

Boot et débogage

Ntdetect.chk

Intérêt

Platform: NTDetect runs only on *x*86-based computers.

Installd.cmd installs Ntdetect.chk, the debug (or checked) version of Ntdetect.com, which is part of Windows NT.

On *x*86-based computers, NTDetect detects installed hardware components at startup time and displays the hardware information structures passed to the kernel. If the standard version of Ntdetect.com fails to detect all the hardware you think it should find, you can use the debug version, which provides more diagnostic information, to help isolate the problem. A mouse or a disk controller is the component that typically causes problems.

NTDetect displays information about the computer's system components, bus and adapter components, disk geometry, read-only memory (ROM) blocks, keyboard and communications (COM) port and parallel port components, mouse component, and floppy disk drive component. When detection is complete, you are prompted to press any key to display hardware information in the registry.

Installing NTDetect is a separate task you perform after you install the *Windows NT Resource Kit* Toolbox.

Caution   Under no circumstances should you delete Ntdetect.chk, which is a required program for a computer running Windows NT. The debug version installed by Installd.cmd is a special version that displays diagnostic information. If you have removed the standard version of Ntdetect.com and your system does not start correctly, use the Emergency Repair Disk to restore the original version. You can also use Installd.cmd to remove the special version of NTDetect.

Installation

1. At the command prompt, switch to the folder where the Resource Kit tools are installed, and type **installd**

   Installd:

   o   Renames the standard Ntdetect.com in the root directory of your system partition.

   o   Copies the debug version of Ntdetect.com from %NTResKit% to the root directory.

2. To see the results, shut down and restart the computer.

   NTDetect displays information about the computer's system components, bus and adapter components, disk geometry, read-only memory (ROM) blocks, keyboard and communications (COM) port and parallel port components, mouse component, and floppy disk drive component. When detection is complete, you are prompted to press any key to display hardware information.

3. To view more information, keep pressing any key. The information displayed is similar to what is stored under **HKEY_LOCAL_MACHINE\HARDWARE\Controller***x* in the registry.

   Example of NTDetect information for the system component

4. After all information for detected hardware is displayed, you can press SPACEBAR to use the LastKnownGood control set instead of the current control set to start the system.

   This allows a system experiencing problems to revert to the last configuration that started successfully.

Désinstallation

At the command prompt, type:
installd /not

Exemple

Current Node: 00050000

Type: MaximumType

Child: 00050045

Parent = 00000000

Sibling: 00000000

ConfigurationData = 00000000

IdentifierLength = 0000011

Identifier= AT/AT COMPATIBLE

ConfigdataLength = 00000044

Version = 0000, Revision = 0000

Count = 0002

Type = Device Data

Size = 0000000C

0080 0000 00DB 000 0000 0000 002 0000 000B 0000 0001 0000

Fichiers requis

- Installd.cmd

- Ntdetect.chk

Extensions du débogueur

Intérêt

This document provides extensive information on using these tools.

The Microsoft Windows NT 4.0 OEM Support Tools version 2.0 are troubleshooting tools for Windows NT Stop errors. Also included are development tools which extend the functionality of existing debugging tools, such as WinDbg, the Windows Debugger.

Note   These tools are for Microsoft Windows NT Server and Workstation, versions 3.51 and 4.0, including all Service Pack revisions.

When Windows NT encounters hardware problems, inconsistencies within data necessary for its operation, or other similar errors, the operating system may crash. This will produce a Stop error, which in turn displays a Stop message,

also known as a "blue screen." Debugging the system is typically necessary to discover the cause. In other cases, system performance may degrade for no apparent reason and kernel mode drivers are suspected. Again, debugging the system is often the best solution.

In these and other situations, kernel debugging is typically performed with Windbg.exe. However, the standard WinDbg extensions can examine only a limited number of data structures, often inadequately, leaving little recourse for the resolution of a critical problem.

The Kernel Debugger Extensions were developed to address some of these shortcomings. Their purpose is to facilitate examination and analysis of a wider range of kernel data structures than is conveniently possible today, especially when dealing with crash dumps. The extensions use the standard WinDbg kernel debugger extension interface, operate similarly to existing kernel debugger extensions, and are intended for Windows NT 3.51 and 4.0 (3.51 Alpha debuggees are not supported).

This toolset is divided into four groups:

1. New debugger extensions to facilitate examination and analysis of a wider range of kernel data structures than is conveniently possible today, especially when dealing with crash dumps. This set of tools will be referred to as the "Kernel Debugger Extensions."

2. Tools for memory pool caller-tracking/tail-checking, pool logging, pool free block pattern fill, and increasing available pool statistics. This set of tools will be referred to as the "Pool Enhancements."

3. A heuristics-based kernel memory crash dump analysis tool to aid in diagnosing memory corruption problems. This tool discovers and analyzes anomalies in the kernel memory space and will be referred to as the "Kernel Memory Space Analyzer."

4. A tool that allows users to create dump files from any Win32 process, such as Csrss.exe or Explorer.exe, that can be examined using Windows Debugger. The tool allows for manual creation of dump files via the command line or hot-key, or automatic creation when exceptions occur in monitored processes.

Fichiers requis

Files are located in the *<cdroot>**<platform>*\desktop\Debug\oemsupt directory on your Windows NT Resource Kit CD-ROM.

Outils de débogage

Intérêt

The Windows NT 4.0 Debugger Tools are a suite of debuggers and debugging-related tools. They are intended for use by users experienced in debugging such as application developers, driver developers, and administrators.

Caution   Incorrect debugging can crash processes as well as the operating system.

Installation

Run the self extracting file, *<cdrom drive>*:Apps\Debug\dbg.exe, from your Windows NT Resource Kit CD-ROM.

Windbg is the main debugger produced by the Windows NT Debugger development team. NTSD and KD are provided for those familiar with these debuggers, and in scenerios where Windbg may not support a particular operation. Included debuggers are:

- Windbg.exe - Windbg debugger

- Windbgrm.exe - Windbg Remote

- Dbgwiz.exe - Windbg Configuration Wizard

- Alphakd.exe - Kernel Debugger for Alpha systems

- I386kd.exe - Kernel Debugger for x86 systems

- Cdb.exe - CDB Debugger (a variant of NTSD)

- Ntsd.exe - NTSD Debugger

- Kd (i386kd, alphakd) is the kernel debugger which is run on a separate debug machine to find problems in the kernel and drivers on a test machine.

- Ntsd is a "software debugger" which is used to debug user mode processes on a test machine.

- WinDbg is a windows-based debugger which can be used to debug either kernel or user mode. It is larger and somewhat slower than its text counterparts, but it has additional features, including source-level debugging. Ntsd-and WinDbg when debugging user mode processes-use symbols in the %windir%\symbols directory. The dll and exe symbols are needed for debugging most user mode problems.

The following debugger-related tools are also included:

- gflags.exe - Global Flags tool

- dumpchk.exe - Dump Check tool

- breakin.exe - BreakIn tool

- remote.exe - Remote tool

- kill.exe - Process Kill tool

- list.exe - File List tool

  Note Another debugger related tool, Dr. Watson, ships with the operating system and is in %systemroot%\system32.

Fichiers requis

- dbg.exe (Windows NT 4.0 Debugger Tools installation file)