

Subinac.exe

[Overview](#) | [Remarks](#) | [Syntax](#) | [Examples](#) | [Related Tools](#)

Overview

SubInACL is a command-line tool that enables administrators to obtain security information about files, registry keys, and services, and transfer this information from user to user, from local or global group to group, and from domain to domain.

For example, if a user has moved from one domain (DomainA) to another (DomainB), the administrator can replace DomainA\User with DomainB\User in the security information for the user's files. This gives the user access to the same files from the new domain.

SubInACL enables administrators to do the following:

- Display security information associated with files, registry keys, or services. This information includes owner, group, permission access control list (ACL), discretionary ACL (DACL), and system ACL (SACL).
- Change the owner of an object.
- Replace the security information for one identifier (account, group, well-known security identifier (SID)) with that of another identifier.
- Migrate security information about objects. This is useful if you have reorganized a network's domains and need to migrate the security information for files from one domain to another.

Corresponding Operating System Features

The operating system provides no GUI functionality that corresponds to this tool.

Concepts

For an introduction to security descriptors and the role they play in access control, see **Understanding access control** in Help and Support Center for Windows Server 2003.

System Requirements

The following are the system requirements for SubInACL:

- Windows XP Professional or Windows Server 2003 operating system

This tool is designed for use by administrators. Some actions may fail or generate error messages if the user does not have the following privileges:

- SeBackupPrivilege (Back Up Files and Directories)
- SeChangeNotifyPrivilege (Bypass Traverse Checking)
- SeRestorePrivilege (Restore Files and Directories)
- SeSecurityPrivilege (Manage Auditing and Security Log)
- SeTakeOwnershipPrivilege (Take Ownership of Files or Other Objects)
- SeTcbPrivilege (Act As Part of the Operating System)

File Required

- Subinac.exe

Remarks

Comparing SubInACL to the find Tool in UNIX

The syntax of SubInACL is analogous to that of the **find** tool in UNIX. For each object, SubInACL:

- Retrieves the security descriptor of the *ObjectName* object. For more information, see [Using SIDs in SubInACL](#).
- Applies one or more actions, which are executed in the order in which they appear on the command line.

If the security descriptor has been modified and the **/testmode** switch has not been specified, the changes are applied to the object. You can specify as many actions as you need. You must specify at least three characters for each action. The syntax is not case-sensitive.

Editing in SubInACL

SubInACL allows you to modify each part of a security descriptor:

- Owner
- Primary group
- System access control list (ACL) and access control entries (ACEs) (referred to by SubInACL as audit ACL and AACE, respectively)
- Discretionary ACL and ACEs (referred to by SubInACL as permission ACL and PACE, respectively)

Using SIDs in SubInACL

The security descriptor references a user group by using a security identifier (SID). An SID can be expressed in one of the following forms:

- DomainName\Account (for example, DOM\Administrators)
- StandaloneServer\Group
- Account
- s-1-x-x-x-x-x-x
Where x is expressed in decimal (for example, S-1-5-21-56248481-1302087933-1644394174-1001).

Caution

- No check is done to verify the existence of a given SID.

SubInACL maintains a local cache of SIDs to minimize "SID-to-human name" translation costs for the network.

Using PACEs in SubInACL

The following permission ACEs (PACEs) are used with the **/grant** and **/deny** parameters.

File PACEs

The following PACEs are valid for file objects:

PACE	Description
F	Full Control
C	Change
R	Read
P	Change Permissions
O	Take Ownership
X	eXecute
E	Read eXecute
W	Write
D	Delete

Cluster Share PACEs

The following PACEs are valid for cluster share objects:

PACE	Description
F	Full Control
R	Read
C	Change

Printer PACEs

The following PACEs are valid for printer objects:

PACE	Description
F	Full Control
M	Manage Documents
P	Print

Registry PACEs

The following PACEs are valid for registry key and registry subkey objects:

PACE	Description
F	Full Control
R	Read
A	ReAd Control
Q	Query Value
S	Set Value
C	Create SubKey
E	Enumerate Subkeys
Y	NotifY
L	Create Link
D	Delete
W	Write DAC
O	Write Owner

Services PACEs

The following PACEs are valid for services:

PACE	Description
F	Full Control
R	Generic Read
W	Generic Write

- X** Generic eXecute
- L** Read control
- Q** Query Service Configuration
- S** Query Service Status
- E** Enumerate Dependent Services
- C** Service Change Configuration
- T** Start Service
- O** Stop Service
- P** Pause/Continue Service
- I** Interrogate Service
- U** Service User-Defined Control Commands

Share PACEs

The following PACEs are valid for share objects:

PACE	Description
F	Full Control
R	Read
C	Change

Metabase PACEs

The following PACEs are valid for metabase objects:

PACE	Description
F	Full Control
R	Read - MD_ACR_READ
W	Write - MD_ACR_WRITE
I	Restricted Write - MD_ACR_RESTRICTED_WRITE
U	Unsecure Props Read - MD_ACR_UNSECURE_PROPS_READ
E	Enum Keys - MD_ACR_ENUM_KEYS
D	Write DAC - MD_ACR_WRITE_DAC

Process PACEs

The following PACEs are valid for process objects:

PACE	Description
F	Full Control
R	Read
W	Write
E	Execute

SAM Object PACEs

The following PACEs are valid for Security Accounts Manager (SAM) objects:

PACE	Description
F	Full Control
R	Read
W	Write
E	Execute

Minimizing Bandwidth Usage

- To minimize network bandwidth used when SubInACL resolves SIDs, place multiple commands that involve the same SIDs in the same command file. When SubInACL resolves a SID, it caches the result to improve its performance and to minimize network traffic. When a SubInACL command finishes, the cache is cleared. Therefore, if you issue four commands and each one requires SubInACL to resolve the same set of SIDs, SubInACL will resolve each of those SIDs four times. However, if you place those four commands in the same command file, SubInACL resolves each SID only once.

Syntax

The syntax descriptions below are grouped by how you use SubInACL: getting Help about its features, using it interactively in a console window, or using it within its own scripting environment.

Syntax for Getting Help

▸ **subinac** /help [/full | *Keyword*]

Parameters

/full

Displays all of the information about SubInACL.

Keyword

[/noverbose | /verbose | /verbose=1 | /verbose=2 | /testmode | /notestmode | /file | /subdirectories | /onlyfile | /share | /clustershare | /keyreg | /subkeyreg | /service | /printer | /kernelobject | /metabase | /display | /setowner | /replace | /changedomain | /migratetodomain | /findsid | /suppresssid | /confirm | /perm | /audit | /ifchangecontinue | /cleandeletedidsfrom | /accesscheck | /setprimarygroup | /grant | /deny | /revoke]

Displays information about the specified option, *object_type*, or action.

/option

Displays information about all SubInACL options.

/action

Displays information about all SubInACL actions.

/object_type

Displays information about all SubInACL *object_types*.

features

Displays information about the feature set.

usage

Displays a summary of SubInACL syntax.

syntax

Displays an conceptual overview of the SubInACL syntax.

sids

Displays information about how SIDs are expressed, and how SubInACL attempts to translate SIDs.

view_mode

Displays information about using SubInACL to view security information.

test_mode

Displays information about using a testing mode to ensure that a SubInACL command is correct.

object_type

Displays information about the types of object that SubInACL can work with.

domain_migration

Displays information about moving a user from one domain to another.

server_migration

Displays information about moving the file system of a server from one domain to another.

editing_features

Displays information about features of SubInACL that edit security descriptors.

For more information, see [/help](#) under Option Syntax Examples on the Examples page.

Syntax for Using SubInACL in a Console Window

► **subinac** [/Option] /object_type object_name [[/Action[=Parameter]..]

Parameters

/Option can be any of the following:

/outputlog=FileName

Redirects the output of the command to the specified file. The output will include errors unless the **/errorlog** option is used, in which case errors are sent to the error log file and all other output is sent to the output log file.

/errorlog=FileName

Redirects all errors to the specified file.

/alternatesamserver=ServerName

Specifies the server that SubInACL will use to look up SIDs, if its first attempt fails. This is useful during some server and domain migrations.

/offlinesam=FileName

Specifies a text file that matches user names to their SIDs, and directs SubInACL to look up SIDs in this file instead of on the server on which the object is located. This is useful if the domain is unaccessible or no longer exists.

/stringreplaceonoutput=String1=String2

Causes SubInACL to replace all occurrences of *String1* in its output with *String2*.

/expandenvironmentsymbols

Allows SubInACL to use environment variables, such as %username%. This is the default value, and the opposite of **/noexpandenvironmentvariables**.

/noexpandenvironmentsymbols

Prevents SubInACL from using environment variables. This is useful when SubInACL operates on command files.

/statistic

Displays statistics when processing is finished. This is the default value.

/nostatistic

Suppresses the display of statistics when processing is finished.

/dumpcachedsids=FileName

After you run SubInACL, you can dump the contents of the local cache SIDs to a file. This file can be used for future SubInACL execution (see **/offlinesam**) to speed up the SIDs resolution process.

/separator=character

Specifies a character for SubInACL to use in place of the equal sign (=) when it interprets a command. This allows you to specify a string that contains an equal sign within a SubInACL command.

/noverbose

Causes SubInACL to produce shortened output that is easier for people to read. The output of a SubInACL command in **/noverbose** mode can be saved in a command file and replayed later.

/verbose

Causes SubInACL to produce detailed output. This is the default level of detail.

/verbose=1

This display mode is identical to **/verbose** mode.

/verbose=2

This display mode is identical to **/verbose** mode.

/testmode

Runs SubInACL in testing mode so that changes will not be applied to the specified object's security descriptor.

/notestmode

Runs SubInACL in update mode, so that any changes defined by a SubInACL command will be applied. This is the default value.

/object_type can be any of the following:

/file [=directoriesonly | =filesonly]

Specifies that *object_name* is a file object. When the **/file** parameter is specified, *object_name* can identify files by using the Universal Naming Convention (UNC) format or by using a local drive letter and path. *object_name* can contain the * wildcard character.

Note

- SubInACL is not supported on distributed file system (DFS) volumes.

/subdirectories | /subdirec [=directoriesonly | =filesonly]

Specifies that *object_name* is a folder (directory) and that SubInACL will use all the files in it and in all its subfolders. When either the **/subdirectories** or **/subdirec** parameter is specified, *object_name* can identify files by using the UNC format or by using a local drive letter and path. *object_name* can include the * wildcard character.

/onlyfile

Opens a file without using the **FindFilexxx** mechanism. Valid values for *object_name* when the **/onlyfile** parameter is specified are named pipes or mailslots.

/samobject

Specifies that *object_name* is a Security Accounts Manager (SAM) object, such as a user, local group, or global group.

/share

Specifies that *object_name* is a network file share.

/clustershare

Specifies that *object_name* is a cluster file share.

/keyreg

Specifies that *object_name* is a registry key.

/subkeyreg

Specifies that *object_name* is a registry subkey.

/service

Specifies that *object_name* is a service.

/process

Specifies that *object_name* is a process.

/printer

Specifies that *object_name* is a printer.

/kernelobject

Specifies that *object_name* is a kernel object. Valid values for *object_name* can include mutexes, sections, or event objects.

/metabase

Specifies that *object_name* is an AdminACL metabase property of the Microsoft Internet Information Services (IIS) metabase.

Notes

- This *object_type* can be used only with the following metabase paths:
 - \LM\MSFTPSVC
 - \LM\MSFTPSVC/n

- \LM\W3SVC
- This *object_type* does not support enumeration

object_name

Specifies the name of the object. For examples, see specific *object_type* descriptions.

/Action can be any of the following:

/display [=dacl | =sac | =owner | =primarygroup | =sdsize | =sddl]

Displays the security descriptor for the specified object. This is the default action. The optional parameters allow you to specify which parts of the security descriptor SubInACL should search. When used in conjunction with **/noverbose**, **/display** reapplies the security descriptor to the specified object.

/setowner

Changes the owner of the object. Using **/owner=SID** or **/setowner=SID owner = DomainName\Administrators** will retrieve the Administrators SID on the server where the object is located.

/owner=Owner

Changes the owner of the specified object. *Owner* is a valid SID that can be expressed in four different formats. For more information, see [Using SIDs in SubInACL](#) on the Remarks page.

/replace=[DomainName\]OldAccount=[DomainName\]NewAccount

Replaces all access control entries (ACEs) (audit ACEs and permissions ACEs) in the specified object.

/accountmigration=DomainName\OldAccount=DomainName\NewAccount

Replaces the owner or primary group if one of them is *DomainName\OldAccount*. For example: */accountmigration=DOM_MARKETING\ChairMan=NEWDOM\NewChairMan* will duplicate all ACEs containing DOM_MARKETING\ChairMan with NewChairMan SID retrieves from NEWDOM domain. For more information, see the **/replace** action.

Caution

- If *DomainName\NewAccount* has an ACE already, ACE replacement is skipped.

/changedomain=OldDomainName=NewDomainName

Replaces all ACEs with an SID from *OldDomainName* with the equivalent SID found in *NewDomainName*.

/migratetodomain=SourceDomain=DestinationDomain

Adds ACEs found in *SourceDomain* for the specified object to *DestinationDomain*, while preserving the ACEs in *SourceDomain*.

/findsid=DomainName\Account[=stop | =continue]

Displays the *object_name* containing a reference to *DomainName\Account* in the security descriptor. If **=stop** is specified and the *Account* is found, the next parameters will be skipped and changes will not be applied. If **=stop** is specified and the *Account* is not found, the next parameters will be executed. If **=continue** is specified and the *Account* is found, the next parameters will be executed. If **=continue** is specified and the *Account* is not found, the next parameters will be skipped and changes will not be applied.

/suppresssid=[DomainName\]Account

Suppresses (deletes) all ACEs containing the *[DomainName\]Account*. If the object's owner is *[DomainName\]Account*, the owner is set to Everyone's SID.

/confirm

If placed inside a set of actions, prompts the user before processing the next action.

/perm

Suppresses all existing PACEs.

/audit

Suppresses all existing AACEs.

/ifchangecontinue

Continues to process the next actions only if changes have been made by the previous actions.

/cleandeletedsidsfrom=DomainName [=dacl | =sacl | =owner | =primarygroup | =sds size]

Deletes all ACEs containing deleted (not valid) SIDs from *DomainName*. The optional parameters allow you to specify certain parts of the security descriptor in which to search for invalid SIDs.

/testmode

Prevents changes from being applied to the object. This allows you to test the modifications that SubInACL will make.

/accesscheck=[DomainName\]UserName

Displays the access granted to the *[DomainName\]UserName*. This option requires the SeTcbName privilege (Act As Part of the Operating System), and cannot be used with remote objects.

/setprimarygroup=[DomainName\]Group

Changes the primary group.

/grant=[DomainName\]UserName [=Access]

Adds a PACE for *UserName*. Valid values for *Access* depend on the type of object specified in *object_name*. Valid PACEs are listed in [Using PACEs in SubInACL](#) on the Remarks page. If *Access* is not specified, Full Control access is granted.

/deny=[DomainName\]UserName [=Access]

Adds a denied PACE for the specified user or group. Valid values for *Access* depend on the type of object specified in *object_name*. Valid PACEs are listed in [Using PACEs in SubInACL](#) on the Remarks page. If *Access* is not specified, all accesses are denied.

/sgrant=[DomainName\]UserName [=Access]

Adds a successful AACE for the specified user. If *Access* is not specified, Full Control access is granted. Valid permission ACEs are listed in [Using PACEs in SubInACL](#) on the Remarks page.

/sdeny=[DomainName\]UserName [=Access]

Adds a failed AACE for the specified user. If *Access* is not specified, all accesses are denied. Valid PACEs are listed in [Using PACEs in SubInACL](#) on the Remarks page.

/revoke=[DomainName\]UserName

Denies all PACEs for the specified user or group.

/compactsecuritydescriptor

Compresses security descriptors by removing unused entries.

/pathexclude=Pattern

Excludes all containers matching the description of *Pattern*, and all the objects within those paths. The * wildcard character can be used within *Pattern* to represent any number of any characters.

/objectexclude=Pattern

Excludes all objects with names that match *Pattern*. The * wildcard character can be used within *Pattern* to represent any number of any characters.

Parameter

The parameter of */Action*, if required.

Syntax for Using SubInACL Within Its Own Scripting Environment

► **subinacl** [*/Option ..*] **/playfile** *FileName*

Parameters*/Option*

Any of the SubInACL options defined above.

FileName

The name of the SubInACL command file (script file). You can create the file manually, or by issuing a SubInACL command that uses the **/noverbose** and **/display** options.

The syntax of the **/playfile** command file is the same as the syntax of SubInACL when used in a console window, except that:

- */Option* is not used.
- Each */object_type* is preceded by a plus symbol (+) rather than a slash (/).
- Each */object_type* and *object_name* pair appear together, on the same line.
- Each action appears on its own line, followed by any applicable parameters.

For more information, see [/playfile](#) under Action Syntax Examples on the Examples page.

Examples

Scenario Examples

Scenario Example 1

The task in this example is to adjust the files on \\Server\Share after you move User1 from OldDomain to NewDomain. Type the following at the command line:

```
subinacl /subdirec \\server\share\*.*  
/replace=OLDDOMAIN\USER1=NEWDOMAIN\User1
```

Press ENTER.

Note

- The two domains must have a trust relationship.

Scenario Example 2

The task in this example is to migrate a backup domain controller (BDC) named MigrControl with all its files to NewDomain, and migrate users from OldDomain to NewDomain.

1. Reinstall MigrControl as a primary domain controller (PDC) of NewDomain, and do not erase the files.
2. Create the users on NewDomain.
3. Create a trust relationship with OldDomain.
4. To migrate the files, type the following at the command line:
**subinacl /noverbose /subdirectories x:*.*
/changedomain=OLDDOMAIN=NEWDOMAIN**
5. Press ENTER.
6. To verify the changes, type the following at the command line:
subinacl /noverbose /subdirectories x:*.*
7. Press ENTER.

Scenario Example 3

The task in this example is to move a stand-alone server and its users to NewDomain.

1. Move the server to NewDomain.
2. Create the users in NewDomain.
3. Type the following at the command line:
**subinacl /noverbose /subdirectories \\SERVER\SHARE
/changedomain=SERVER=NEWDOMAIN**

4. Press ENTER.

Scenario Example 4

The task in this example is to replace "Jim" with "Kim" in each .txt file in the C:\Temp folder, display the security descriptor for each such file, and apply any changes. Type the following at the command line:

subinacl /file c:\temp*.txt /replace=Jim=Kim/display

Press ENTER.

Option Syntax Examples

/help

- The task in this example is to display Help about the topic of domain migration. Type the following at the command line:

subinacl /help domain_migration

Press ENTER.

- The task in this example is to display Help about the **/setowner** action. Type the following at the command line:

subinacl /help /setowner

Press ENTER.

/outputlog

- The task in this example is to obtain security information about the file C:\Test.txt and record all output of the command (including errors) in the file C:\Alloutput.txt. Type the following at the command line:

subinacl /outputlog=C:\ALLOUTPUT.TXT /file C:\TEST.TXT /display

Press ENTER.

/errorlog

- The task in this example is to obtain security information about the file C:\Test.txt, record all errors generated by the command in the file C:\Errorlog.txt, and record all other output in the file C:\Nonerrors.txt. Type the following at the command line:

subinacl /outputlog=c:\NONERRORS.TXT /errorlog=C:\ERRORLOG.TXT /file C:\TEST.TXT /display

Press ENTER.

/alternatesamserver

- The task in this example is to display the security settings of the file C:\Test.txt and use the server \\Server1 to resolve SIDs if SubInACL is unable to resolve them on the server where the file is located. Type the following at the command line:

subinacl /alternatesamserver=\\server1 /file C:\TEST.TXT /display

Press ENTER.

/offlinesam

- The task in this example is to migrate the security settings of the files on a server from one domain to another. This example assumes that you have access to the source domain and know you will not have access to it during the migration.
 1. Store a record of user names and their corresponding SIDs from the source domain in a text file named C:\Samfile.txt. Use the following format:
 - `_cachefileonly_=s-1-9-cacheonly`
 - `[Domain\UserName | Server\UserName]=SID`
 2. Type the following at the command line:
subinacl /offlinesam=C:\SAMFILE.TXT /subdirect \\SERVER\SHARE*.* /migratedomain=SOURCEDOMAIN=DESTDOMAIN
 3. Press ENTER.

/stringreplaceonoutput

- The task in this example is to move the files from the E: drive of \\Server1 to the E: drive of \\Server2.
 1. To record the security settings of the files on the E: drive of \\Server1 in the file C:\Commandfile.txt, but replace references to \\Server1 with \\Server2, type the following at the command line:
subinacl /outputlog=c:\commandfile.txt /stringreplaceonoutput=\\server1=\\server2 /subdirectories E:*.* /noverbose /display
 2. Press ENTER.
 3. Copy all files from the E: drive of \\Server1 to the E: drive of \\Server2.
 4. Copy Commandfile.txt to the C: drive of \\Server2.
 5. To reapply the security settings to the files on the E: drive of \\Server2, type the following at the command line:
subinacl /playfile c:\commandfile.txt
 6. Press ENTER.

/noexpandenvironmentsymbols

- The task in this example is to prevent SubInACL from interpreting any strings as environment variables. Type the following at the command line:

subinacl /noexpandenvironmentsymbols /object_type object_name /action

Press ENTER.

/separator

- The task in this example is to temporarily define the tilde (~) as the separator character so that options such as **/stringreplaceonoutput** can manipulate strings that contain the default separator character (=). Type the following at the command line:

subinacl /separator=~ /stringreplaceonoutput~=europe\~=southerneurope /file *.* /noverbose /display

Press ENTER.

/noverbose

- The task in this example is to display a summary of the security settings of the file C:\Test.txt. Type the following at the command line:

subinacl /noverbose /file c:\test.txt

Press ENTER.

- The task in this example is to save the security settings of all files on the C: drive to the file D:\Filesettings.txt, so that they can be reapplied if necessary by using the **/playfile** and **/display** actions. Type the following at the command line:

**subinac /noverbose /outputlog=D:\FILESETTINGS.TXT /subdirectories C:*.*
/display**

Press ENTER.

/verbose

- The task in this example is to display the full details of the security settings of the file C:\Test.txt. Type the following at the command line:

subinac /verbose /file C:\TEST.TXT

Press ENTER.

/testmode

- The task in this example is to test a command and verify that you have used the correct syntax, without applying changes. You want to change the name of the domain in all security descriptors of all files in the subdirectories of Share1 on \\Server1 from DomA to DomB; however, you want to test the command first. Type the following at the command line:

**subInac /subdirec \\SERVER1\SHARE1*.* /changedomain=DOMA=DOMB
/ifchangecontinue /noverbose /display /testmode**

Press ENTER.

Object Syntax Examples

/file

- The task in this example is to display the security settings of all .obj files in the current folder. Type the following at the command line:

subinac /file *.obj /display

Press ENTER.

- The task in this example is to display the security settings of all .obj files in the C:\Temp folder. Type the following at the command line:

subinac /file C:\TEMP*.obj /display

Press ENTER.

- The task in this example is to display the security settings of all .exe files in the folder that is shared as \\Server1\Share1. Type the following at the command line:

subinac /file \\server1\share1*.exe /display

Press ENTER.

- The task in this example is to display the security settings of the folder that is shared as \\Server1\Share1 (rather than acting on the files within that folder). Type the following at the command line:

subinacl /file=directoriesonly \\server1\share1 /display

Press ENTER.

- The task in this example is to display the security settings of all files in the folder that is shared as \\Server1\Share1, and not on folders or subfolders. Type the following at the command line:

subinacl /file=filesonly \\server1\share1 /display

Press ENTER.

/subdirectory

- The task in this example is to display the security settings of all .obj files in the C:\Temp folder and all its subfolders. Type the following at the command line:

subinacl /subdirectory C:\TEMP*.obj /display

Press ENTER.

- The task in this example is to display the security settings of all .obj files in the C:\Temp\Test folder and all its subfolders. Type the following at the command line:

subinacl /subdirectory C:\TEMP\TEST*.OBJ /display

Press ENTER.

- The task in this example is to display the security settings of folders only, and not files. Type the following at the command line:

subinacl /subdirectory=directoriesonly C:*.* /display

Press ENTER.

/onlyfile

- The task in this example is to display the security settings of the named pipe PipeName. Type the following at the command line:

subinacl /onlyfile \\.\pipe\PipeName /display

Press ENTER.

/samobject

- The task in this example is to display the security settings of the local group Group1 on the Server1 server. Type the following at the command line:

subinacl /samobject \\SERVER1\GROUP1 /display

Press ENTER.

- The task in this example is to display the security settings of local users defined on the Server1 server. Type the following at the command line:

subinacI /samobject \\SERVER1*users* /display

Press ENTER.

- The task in this example is to display the security settings of local groups defined on the Server1 server. Type the following at the command line:

subinacI /samobject \\SERVER1*groups* /display

Press ENTER.

- The task in this example is to grant the power user named Poweruser1 full control over the TestGroup local group, which was created by another power user. Type the following at the command line:

subinacI /samobject \\SERVER1\TESTGROUP /grant=poweruser1=f

Press ENTER.

/share

- The task in this example is to display the security settings of the network file share named \\Server1\Share1. Type the following at the command line:

subinacI /share \\SERVER1\SHARE1 /share

Press ENTER.

/clustershare

- The task in this example is to specify that SubInACL act on the cluster share named \\Cluster1\Share1. Type the following at the command line:

subinacI /clustershare \\CLUSTER1\SHARE1 /display

Press ENTER.

/keyreg

- The task in this example is to display the security settings of the registry keys located on the server \\Server1, at the location HKEY_LOCAL_MACHINE\SOFTWARE. Type the following at the command line:

subinacI /keyreg \\SERVER1\HKEY_LOCAL_MACHINE\SOFTWARE /display

Press ENTER.

/subkeyreg

- The task in this example is to display the security settings of the registry keys and subkeys located on the server \\Server1, at the location HKEY_LOCAL_MACHINE\SOFTWARE. Type the following at the command line:

subinacI /subkeyreg \\SERVER1\HKEY_LOCAL_MACHINE\SOFTWARE /display

Press ENTER.

/service

- The task in this example is to display the security settings of the Messenger service on the local computer. Type the following at the command line:

subinac /service Messenger /display

Press ENTER.

- The task in this example is to display the security settings of the Messenger service on \\Server1. Type the following at the command line:

subinac /service \\SERVER1\MESSENGER /display

Press ENTER.

/printer

- The task in this example is to display the security settings of the printer shared as \\Server1\Printer1. Type the following at the command line:

subinac /printer \\SERVER1\PRINTER1 /display

Press ENTER.

/kernelobject

- The task in this example is to display the security settings of the mutex named _outlook_mutex_. Type the following at the command line:

subinac /kernelobject _outlook_mutex_ /display

Press ENTER.

/process

- The task in this example is to display the security settings of Notepad. Type the following at the command line:

subinac /process notepad.* /display

Press ENTER.

- The task in this example is to display the security settings of the process that has process identifier (PID) 1234. Type the following at the command line:

subinac /process 1234 /display

Press ENTER.

/metabase

- The task in this example is to grant administrators full control over the properties at \\LM\W3SVC on the server \\Server1. Type the following at the command line:

subinac /metabase \\SERVER1\LM\W3SVC /grant=administrators=f

Press ENTER.

Action Syntax Examples

/display

- The task in this example is to display the security settings of the files on the C: drive. Type the following at the command line:

subinacl /file C:*.* /display

Press ENTER.

- The task in this example is to save the security settings of the files on the C: drive to the file D:\Securitysettings.txt. Type the following at the command line:

subinacl /file /outputlog=D:\SECURITYSETTINGS.TXT C:*.* /display /noverbose

Press ENTER.

/owner

- The task in this example is to set Domain1\User1 to be the owner of the file C:\Test.txt. Type the following at the command line:

subinacl /file C:\TEST.TXT /owner=DOMAIN1\USER1

Press ENTER.

/replace

- The task in this example is to replace Domain1\User1 with Domain2\User2 throughout the ACEs of all files on the C: drive. Type the following at the command line:

subinacl /file C:*.* /replace=DOMAIN1\USER1=DOMAIN2\USER2

Press ENTER.

/changedomain

- The task in this example is to replace all ACEs that have an SID from Domain1 with the SID of the same user from Domain2, for all files on the C: drive. Type the following at the command line:

subinacl /subdirectory C:*.* /changedomain=domain1=domain2

Press ENTER.

- The task in this example is to replace all ACEs that have the SID of User1 from Domain1 with the SID of User2 from Domain2, for all files on the C: drive. Use a mapping file.
 1. Create a mapping file containing only the line "USER1=USER2" and save this file as Mapfile.txt.
 2. Type the following at the command prompt:

**subinacl /subdirectory C:*.*
/changedomain=domain1=domain2=MAPFILE.TXT**

3. Press ENTER.

/migratetodomain

- The task in this example is to leave intact each ACE on every file on the C: drive that has

an SID from Domain1, and create a new ACE with the same user from Domain2. Type the following at the command line:

subinacl /subdirectory C:*.* /changedomain=domain1=domain2

Press ENTER.

- The task in this example is to create a new ACE with the SID of Domain2\User2 for each ACE on every file on the C: drive that has an SID from Domain1\User1. Use a mapping file:
 1. Create a mapping file containing only the line **USER1=USER2** and save this file as Mapfile.txt.
 2. Type the following at the command line:
subinacl /subdirectory C:*.* /changedomain=domain1=domain2=mapfile.txt
 3. Press ENTER.

/findsid

- The task in this example is to display the names of files on the C: drive that have security descriptors that reference the SID of Domain1\User1. Type the following at the command line:

subinacl /subdirectory C:*.* /findsid=DOMAIN1\USER1

Press ENTER.

- The task in this example is to display the names of files on the C: drive that have security descriptors that reference the SID of Domain1\User1, and—if any are found—not to execute any other parameters and not to apply changes. Type the following at the command line:

subinacl /subdirectory C:*.* /findsid=DOMAIN1\USER1=stop

Press ENTER.

/suppresssid

- The task in this example is to remove all ACEs that reference Domain1\User1 from the file C:\Test.txt. Type the following at the command line:

subinacl /file C:\TEST.TXT /suppresssid=DOMAIN1\USER1

Press ENTER.

/confirm

- The task in this example is to begin cleaning up deleted SIDs from Domain1, searching only the DACL and SACL parts of the security descriptors of each file, and prompting the user to continue after deleting the first ACE that contains an invalid SID. Type the following at the command line:

**subinacl /file *.* /cleandeletedidsfrom=domain1=dac
/cleandeletedidsfrom=domain1=sac /ifchangcontinue /confirm**

Press ENTER.

/perm

- The task in this example is to suppress all existing permission ACEs (PACEs) on the file C:\Test.txt. Type the following at the command line:

subinacl /file C:\TEST.TXT /perm

Press ENTER.

/audit

- The task in this example is to suppress all existing auditing ACEs (AACEs) on the file C:\Test.txt. Type the following at the command line:

subinacl /file C:\TEST.TXT /audit

Press ENTER.

/accesscheck

- The task in this example is to display the access granted to Domain1\User1 on the file C:\Test.txt. Type the following at the command line:

subinacl /file C:\TEST.TXT /accesscheck=domain1\user1

Press ENTER.

/setprimarygroup

- The task in this example is to set the primary group of C:\Test.txt to be Domain1\Group1. Type the following at the command line:

subinacl /file C:\TEST.TXT /setprimarygroup=domain1\group1

Press ENTER.

/grant

- The task in this example is to grant Domain1\User1 the PACE of Take Ownership on the file C:\Test.txt. Type the following at the command line:

subinacl /file C:\TEST.TXT /grant=domain1\user1=o

Press ENTER.

- The task in this example is to grant Domain1\User1 the PACEs of Execute and Take Ownership on the file C:\Test.txt. Type the following at the command line:

subinacl /file C:\TEST.TXT /grant=domain1\user1=xo

Press ENTER.

/deny

- The task in this example is to deny Domain1\User1 the PACE of Take Ownership on the file C:\Test.txt. Type the following at the command line:

subinacl /file C:\TEST.TXT /deny=domain1\user1=o

Press ENTER.

- The task in this example is to deny Domain1\User1 the PACEs of Execute and Take Ownership on the file C:\Test.txt. Type the following at the command line:

subinacl /file C:\TEST.TXT /deny=domain1\user1=xo

Press ENTER.

/revoke

- The task in this example is to revoke all PACEs for Domain1\User1 on the file C:\Test.txt. Type the following at the command line:

subinacl /file C:\TEST.TXT /revoke=domain1\user1

Press ENTER.

/compactsecuritydescriptor

- The task in this example is to compact the size of security descriptors created by a disk utility. You used the **/display=sdsize** action to examine the sizes of these security descriptors, and determined that the utility created large security descriptors that included very little data. You want to compact these security descriptors on disk. Type the following at the command line:

subinacl /subdirectories C:*.* /compactsecuritydescriptor

Press ENTER.

/pathexclude

- The task in this example is to prevent a SubInACL command from displaying information about any folder that has a name that begins with "TESTING". Type the following at the command line:

subinacl /file C:*.* /display /pathexclude=TESTING*

Press ENTER.

/objectexclude

- The task in this example is to prevent a SubInACL command from displaying information about any file with an .asp extension. Type the following at the command line:

subinacl /file *.* /display /objectexclude=*.asp

Press ENTER.

/playfile

- The task in this example is to grant everyone Read permission on the file C:\Test1.txt, and both Read and Write permission on the file C:\Test2.txt. You could type the following SubInACL commands at the command line:

subinacl /file C:\TEST1.TXT /grant=everyone=r /noverbose /display
subinacl /file C:\TEST2.TXT /grant=everyone=rw /noverbose /display

To perform the same action with a command file (a playfile), do the following:

1. Create a text file named Commandfile.txt that contains only these lines:

```
+file C:\TEST1.TXT
/grant=everyone=r
/noverbose
```

```
/display  
+file C:\TEST2.TXT  
/grant=everyone=rw  
/noverbose  
/display
```

2. Type the following at the command line:

```
subinacl /playfile COMMANDFILE.TXT
```

Press ENTER.

- The task in this example is to save the security settings of all files on the C: drive to the file D:\Subinaclsave.txt by using a format that the **/playfile** command can replay. Type the following at the command line:

```
subinacl /noverbose /outputlog=D:\subinaclsave.txt /subdirectories c:\*.*  
/display
```

Press ENTER.

To reapply the saved settings, type the following at the command line:

```
subinacl /playfile D:\subinaclsave.txt
```

Press ENTER.

Related Tools

Tools related to Subinacl.exe include:

- Permcopyp.exe: Share Permissions Copy
- Perms.exe: User File Permissiong
- ShowacIs.exe: Show ACLs