NAME

smbcacls - Set or get ACLs on an NT file or directory names

SYNOPSIS

smbcacls {//server/share} {/filename} [-D|--delete acl] [-M|--modify acl] [-a|--add acl] [-S|--set acl] [-C|--chown name] [-G|--chgrp name] [-I allow|remove|copy] [--numeric] [-t] [-U username] [-d] [-e] [-m|--max-protocol LEVEL] [--query-security-info FLAGS] [--set-security-info FLAGS] [--sddl] [--domain-sid SID] [-x|--maximum-access]

DESCRIPTION

This tool is part of the **samba**(7) suite.

The smbcacls program manipulates NT Access Control Lists (ACLs) on SMB file shares. An ACL is comprised zero or more Access Control Entries (ACEs), which define access restrictions for a specific user or group.

OPTIONS

The following options are available to the smbcacls program. The format of ACLs is described in the section ACL FORMAT

-a|--add acl

Add the entries specified to the ACL. Existing access control entries are unchanged.

-M|--modify acl

Modify the mask value (permissions) for the ACEs specified on the command line. An error will be printed for each ACE specified that was not already present in the object's ACL.

-D|--delete acl

Delete any ACEs specified on the command line. An error will be printed for each ACE specified that was not already present in the object's ACL.

-S|--set acl

This command sets the ACL on the object with only what is specified on the command line. Any existing ACL is erased. Note that the ACL specified must contain at least a revision, type, owner and group for the call to succeed.

-C|--chown name

The owner of a file or directory can be changed to the name given using the *-C* option. The name can be a sid in the form S-1-x-y-z or a name resolved against the server specified in the first argument.

This command is a shortcut for -M OWNER:name.

-G|--chgrp name
The group owner of a file or directory can be changed to the name given using the *-G* option. The name can be a sid in the form S-1-x-y-z or a name resolved against the server specified n the first argument.

This command is a shortcut for -M GROUP:name.

-I|--inherit allow|remove|copy
Set or unset the windows "Allow inheritable permissions" check box using the *-I* option. To set the check box pass allow. To unset the check box pass either remove or copy. Remove will remove all inherited acls. Copy will copy all the inherited acls.

--numeric
This option displays all ACL information in numeric format. The default is to convert SIDs to names and ACE types and masks to a readable string format.

-m|--max-protocol PROTOCOL_NAME
This allows the user to select the highest SMB protocol level that smbcacls will use to connect to the server. By default this is set to NT1, which is the highest available SMB1 protocol. To connect using SMB2 or SMB3 protocol, use the strings SMB2 or SMB3 respectively. Note that to connect to a Windows 2012 server with encrypted transport selecting a max-protocol of SMB3 is required.

-t|--test-args
Don’t actually do anything, only validate the correctness of the arguments.

--query-security-info FLAGS
The security-info flags for queries.

--set-security-info FLAGS
The security-info flags for queries.

--sddl
Output and input acls in sddl format.

--domain-sid SID
SID used for sddl processing.

-x|--maximum-access

When displaying an ACL additionally query the server for effective maximum permissions. Note that this is only supported with SMB protocol version 2 or higher.

-d|--debuglevel=level
level is an integer from 0 to 10. The default value if this parameter is not specified is 0.

The higher this value, the more detail will be logged to the log files about the activities of the server. At level 0, only critical errors and serious warnings will be logged. Level 1 is a reasonable level for day-to-day running - it generates a small amount of information about operations carried out.

Levels above 1 will generate considerable amounts of log data, and should only be used when investigating a problem. Levels above 3 are designed for use only by developers and generate HUGE amounts of log data, most of which is extremely cryptic.

Note that specifying this parameter here will override the **log level** parameter in the smb.conf file.

-V|--version
Prints the program version number.

-s|--configfile=<configuration file>
The file specified contains the configuration details required by the server. The information in this file includes server-specific information such as what printcap file to use, as well as descriptions of all the services that the server is to provide. See smb.conf for more information. The default configuration file name is determined at compile time.

-l|--log-basename=logdirectory
Base directory name for log/debug files. The extension **".progname"** will be appended (e.g. log.smbclient, log.smbd, etc...). The log file is never removed by the client.

--option=<name>=<value>
Set the **smb.conf**(5) option "<name>" to value "<value>" from the command line. This overrides compiled-in defaults and options read from the configuration file.

-N|--no-pass
If specified, this parameter suppresses the normal password prompt from the client to the user. This is useful when accessing a service that does not require a password.

Unless a password is specified on the command line or this parameter is specified, the client will request a password.

If a password is specified on the command line and this option is also defined the password on the command line will be silently ignored and no password will be used.

-k|--kerberos
Try to authenticate with kerberos. Only useful in an Active Directory environment.

-C|--use-ccache
Try to use the credentials cached by winbind.

-A|--authentication-file=filename
This option allows you to specify a file from which to read the username and password used in the connection. The format of the file is

username = <value>
password = <value>
domain = <value>

Make certain that the permissions on the file restrict access from unwanted users.

-U|--user=username[%password]
Sets the SMB username or username and password.

If %password is not specified, the user will be prompted. The client will first check the **USER** environment variable, then the **LOGNAME** variable and if either exists, the string is uppercased. If these environmental variables are not found, the username **GUEST** is used.

A third option is to use a credentials file which contains the plaintext of the username and password. This option is mainly provided for scripts where the admin does not wish to pass the credentials on the command line or via environment variables. If this method is used, make certain that the permissions on the file restrict access from unwanted users. See the *-A* for more details.

Be cautious about including passwords in scripts. Also, on many systems the command line of a running process may be seen via the ps command. To be safe always allow rpcclient to prompt for a password and type it in directly.

-S|--signing on|off|required
Set the client signing state.

-P|--machine-pass
Use stored machine account password.

-e|--encrypt
: This command line parameter requires the remote server support the UNIX extensions or that the SMB3 protocol has been selected. Requests that the connection be encrypted. Negotiates SMB encryption using either SMB3 or POSIX extensions via GSSAPI. Uses the given credentials for the encryption negotiation (either kerberos or NTLMv1/v2 if given domain/username/password triple. Fails the connection if encryption cannot be negotiated.

--pw-nt-hash
: The supplied password is the NT hash.

-n|--netbiosname <primary NetBIOS name>
: This option allows you to override the NetBIOS name that Samba uses for itself. This is identical to setting the **netbios name** parameter in the smb.conf file. However, a command line setting will take precedence over settings in smb.conf.

-i|--scope <scope>
: This specifies a NetBIOS scope that nmblookup will use to communicate with when generating NetBIOS names. For details on the use of NetBIOS scopes, see rfc1001.txt and rfc1002.txt. NetBIOS scopes are *very* rarely used, only set this parameter if you are the system administrator in charge of all the NetBIOS systems you communicate with.

-W|--workgroup=domain
: Set the SMB domain of the username. This overrides the default domain which is the domain defined in smb.conf. If the domain specified is the same as the servers NetBIOS name, it causes the client to log on using the servers local SAM (as opposed to the Domain SAM).

-O|--socket-options socket options
: TCP socket options to set on the client socket. See the socket options parameter in the smb.conf manual page for the list of valid options.

-?|--help
: Print a summary of command line options.

--usage
: Display brief usage message.

ACL FORMAT

The format of an ACL is one or more entries separated by either commas or newlines. An ACL entry is one of the following:

REVISION:<revision number>
OWNER:<sid or name>
GROUP:<sid or name>
ACL:<sid or name>:<type>/<flags>/<mask>

The revision of the ACL specifies the internal Windows NT ACL revision for the security descriptor. If not specified it defaults to 1. Using values other than 1 may cause strange behaviour.

The owner and group specify the owner and group sids for the object. If a SID in the format S-1-x-y-z is specified this is used, otherwise the name specified is resolved using the server on which the file or directory resides.

ACEs are specified with an "ACL:" prefix, and define permissions granted to an SID. The SID again can be specified in S-1-x-y-z format or as a name in which case it is resolved against the server on which the file or directory resides. The type, flags and mask values determine the type of access granted to the SID.

The type can be either ALLOWED or DENIED to allow/deny access to the SID. The flags values are generally zero for file ACEs and either 9 or 2 for directory ACEs. Some common flags are:

- **SEC_ACE_FLAG_OBJECT_INHERIT 0x1**
- **SEC_ACE_FLAG_CONTAINER_INHERIT 0x2**
- **SEC_ACE_FLAG_NO_PROPAGATE_INHERIT 0x4**
- **SEC_ACE_FLAG_INHERIT_ONLY 0x8**

At present, flags can only be specified as decimal or hexadecimal values.

The mask is a value which expresses the access right granted to the SID. It can be given as a decimal or hexadecimal value, or by using one of the following text strings which map to the NT file permissions of the same name.

-

- Allow read access

- Allow write access

- Execute permission on the object

- Delete the object

- Change permissions

- Take ownership

The following combined permissions can be specified:

- Equivalent to ’RX’ permissions

- Equivalent to ’RXWD’ permissions

- Equivalent to ’RWXDPO’ permissions

EXIT STATUS

The smbcacls program sets the exit status depending on the success or otherwise of the operations performed. The exit status may be one of the following values.

If the operation succeeded, smbcacls returns and exit status of 0. If smbcacls couldn’t connect to the specified server, or there was an error getting or setting the ACLs, an exit status of 1 is returned. If there was an error parsing any command line arguments, an exit status of 2 is returned.

VERSION

This man page is part of version 4.13.17 of the Samba suite.

AUTHOR

The original Samba software and related utilities were created by Andrew Tridgell. Samba is now developed by the Samba Team as an Open Source project similar to the way the Linux kernel is developed.

smbcacls was written by Andrew Tridgell and Tim Potter.

The conversion to DocBook for Samba 2.2 was done by Gerald Carter. The conversion to DocBook XML 4.2 for Samba 3.0 was done by Alexander Bokovoy.