NAME

sharesec - Set or get share ACLs

SYNOPSIS

sharesec {sharename} [-r, --remove=ACL] [-m, --modify=ACL] [-a, --add=ACL]
[-R, --replace=ACLs] [-D, --delete] [-v, --view] [--view-all] [-M, --machine-sid] [-F, --force]
[-d, --debuglevel=DEBUGLEVEL] [-s, --configfile=CONFIGFILE]
[-l, --log-basename=LOGFILEBASE] [--version] [-?, --help] [--usage] [-S, --setsddl=STRING]
[-V, --viewsddl]

DESCRIPTION

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

The sharesec program manipulates share permissions on SMB file shares.

OPTIONS

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

-a|--add=ACL
: Add the ACEs specified to the ACL list.

-D|--delete
: Delete the entire security descriptor.

-F|--force
: Force storing the ACL.

-m|--modify=ACL
: Modify existing ACEs.

-M|--machine-sid
: Initialize the machine SID.

-r|--remove=ACL
: Remove ACEs.

-R|--replace=ACLS
: Overwrite an existing share permission ACL.

-v|--view
List a share acl

--view-all
List all share acls

-S|--setsddl=STRING
Set security descriptor by providing ACL in SDDL format.

-V|--viewsddl
List a share acl in SDDL format.

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

-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.

ACL FORMAT

The format of an ACL is one or more ACL 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. Share ACLs do not specify an owner or a group, so these fields are empty.

ACLs specify permissions granted to the SID. This SID 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 share ACLs.

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 sharesec 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, sharesec returns and exit status of 0. If sharesec 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.

EXAMPLES

Add full access for SID *S-1-5-21-1866488690-1365729215-3963860297-17724* on *share*:

```
host:~ # sharesec share -a S-1-5-21-1866488690-1365729215-3963860297-17724:ALLOWED/0/FULL
```

List all ACEs for *share*:

```
host:~ # sharesec share -v
```

REVISION:1
CONTROL:SR|DP
OWNER:
GROUP:
ACL:S-1-1-0:ALLOWED/0x0/FULL
ACL:S-1-5-21-1866488690-1365729215-3963860297-177

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.