NAME

samba-tool - Main Samba administration tool.

SYNOPSIS

samba-tool [-h] [-W myworkgroup] [-U user] [-d debuglevel] [--v]

DESCRIPTION

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

OPTIONS

-h|--help
: Show this help message and exit

--realm=REALM
: Set the realm name

--simple-bind-dn=DN
: DN to use for a simple bind

--password=PASSWORD
: Password

-U USERNAME|--username=USERNAME
: Username

-W WORKGROUP|--workgroup=WORKGROUP
: Workgroup

-N|--no-pass
: Don’t ask for a password

-k KERBEROS|--kerberos=KERBEROS
: Use Kerberos

--ipaddress=IPADDRESS
: IP address of the server

-d|--debuglevel=level
: *level* is an integer from 0 to 10. The default value if this parameter is not specified is 1.

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.

COMMANDS

computer

Manage computer accounts.

computer create computername [options]

Create a new computer in the Active Directory Domain.

The new computer name specified on the command is the sAMAccountName, with or without the trailing dollar sign.

--computerou=COMPUTEROU
DN of alternative location (with or without domainDN counterpart) to default CN=Computers in

which new computer object will be created. E.g. ’OU=OUname’.

--description=DESCRIPTION
The new computers’s description.

--ip-address=IP_ADDRESS_LIST
IPv4 address for the computer’s A record, or IPv6 address for AAAA record, can be provided multiple times.

--service-principal-name=SERVICE_PRINCIPAL_NAME_LIST
Computer’s Service Principal Name, can be provided multiple times.

--prepare-oldjoin
Prepare enabled machine account for oldjoin mechanism.

computer delete computername [options]
Delete an existing computer account.

The computer name specified on the command is the sAMAccountName, with or without the trailing dollar sign.

computer edit computername
Edit a computer AD object.

The computer name specified on the command is the sAMAccountName, with or without the trailing dollar sign.

--editor=EDITOR
Specifies the editor to use instead of the system default, or ’vi’ if no system default is set.

computer list
List all computers.

computer move computername new_parent_dn [options]
This command moves a computer account into the specified organizational unit or container.

The computername specified on the command is the sAMAccountName, with or without the trailing dollar sign.

The name of the organizational unit or container can be specified as a full DN or without the

domainDN component.

computer show computername [options]
Display a computer AD object.

The computer name specified on the command is the sAMAccountName, with or without the trailing dollar sign.

--attributes=USER_ATTRS
Comma separated list of attributes, which will be printed.

contact
Manage contacts.

contact create [contactname] [options]
Create a new contact in the Active Directory Domain.

The name of the new contact can be specified by the first argument 'contactname' or the --given-name, --initial and --surname arguments. If no 'contactname' is given, contact's name will be made up of the given arguments by combining the given-name, initials and surname. Each argument is optional. A dot ('.') will be appended to the initials automatically.

--ou=OU
DN of alternative location (with or without domainDN counterpart) in which the new contact will be created. E.g. 'OU=OUname'. Default is the domain base.

--description=DESCRIPTION
The new contacts's description.

--surname=SURNAME
Contact's surname.

--given-name=GIVEN_NAME
Contact's given name.

--initials=INITIALS
Contact's initials.

--display-name=DISPLAY_NAME
Contact's display name.

--job-title=JOB_TITLE
Contact’s job title.

--department=DEPARTMENT
Contact’s department.

--company=COMPANY
Contact’s company.

--mail-address=MAIL_ADDRESS
Contact’s email address.

--internet-address=INTERNET_ADDRESS
Contact’s home page.

--telephone-number=TELEPHONE_NUMBER
Contact’s phone number.

--mobile-number=MOBILE_NUMBER
Contact’s mobile phone number.

--physical-delivery-office=PHYSICAL_DELIVERY_OFFICE
Contact’s office location.

contact delete contactname [options]
Delete an existing contact.

The contactname specified on the command is the common name or the distinguished name of the contact object. The distinguished name of the contact can be specified with or without the domainDN component.

contact edit contactname
Modify a contact AD object.

The contactname specified on the command is the common name or the distinguished name of the contact object. The distinguished name of the contact can be specified with or without the domainDN component.

--editor=EDITOR
Specifies the editor to use instead of the system default, or ’vi’ if no system default is set.

contact list [options]
List all contacts.

--full-dn
Display contact’s full DN instead of the name.

contact move contactname new_parent_dn [options]
This command moves a contact into the specified organizational unit or container.

The contactname specified on the command is the common name or the distinguished name of the contact object. The distinguished name of the contact can be specified with or without the domainDN component.

contact show contactname [options]
Display a contact AD object.

The contactname specified on the command is the common name or the distinguished name of the contact object. The distinguished name of the contact can be specified with or without the domainDN component.

--attributes=CONTACT_ATTRS
Comma separated list of attributes, which will be printed.

dbcheck
Check the local AD database for errors.

delegation
Manage Delegations.

delegation add-service accountname principal [options]
Add a service principal as msDS-AllowedToDelegateTo.

delegation del-service accountname principal [options]
Delete a service principal as msDS-AllowedToDelegateTo.

delegation for-any-protocol accountname [(on|off)] [options]
Set/unset UF_TRUSTED_TO_AUTHENTICATE_FOR_DELEGATION (S4U2Proxy) for an account.

delegation for-any-service accountname [(on|off)] [options]
Set/unset UF_TRUSTED_FOR_DELEGATION for an account.

delegation show accountname [options]
Show the delegation setting of an account.

dns
Manage Domain Name Service (DNS).

dns add server zone name A|AAAA|PTR|CNAME|NS|MX|SRV|TXT data
Add a DNS record.

dns delete server zone name A|AAAA|PTR|CNAME|NS|MX|SRV|TXT data
Delete a DNS record.

dns query server zone name A|AAAA|PTR|CNAME|NS|MX|SRV|TXT|ALL [options] data
Query a name.

dns roothints server [name] [options]
Query root hints.

dns serverinfo server [options]
Query server information.

dns update server zone name A|AAAA|PTR|CNAME|NS|MX|SRV|TXT olddata newdata
Update a DNS record.

dns zonecreate server zone [options]
Create a zone.

dns zonedelete server zone [options]
Delete a zone.

dns zoneinfo server zone [options]
Query zone information.

dns zonelist server [options]
List zones.

domain
Manage Domain.

domain backup

Create or restore a backup of the domain.

domain backup offline
Backup (with proper locking) local domain directories into a tar file.

domain backup online
Copy a running DC’s current DB into a backup tar file.

domain backup rename
Copy a running DC’s DB to backup file, renaming the domain in the process.

domain backup restore
Restore the domain’s DB from a backup-file.

domain classicupgrade [options] classic_smb_conf
Upgrade from Samba classic (NT4-like) database to Samba AD DC database.

domain dcpromo dnsdomain [DC|RODC] [options]
Promote an existing domain member or NT4 PDC to an AD DC.

domain demote
Demote ourselves from the role of domain controller.

domain exportkeytab keytab [options]
Dumps Kerberos keys of the domain into a keytab.

domain info ip_address [options]
Print basic info about a domain and the specified DC.

domain join dnsdomain [DC|RODC|MEMBER|SUBDOMAIN] [options]
Join a domain as either member or backup domain controller.

domain level show|raise options [options]
Show/raise domain and forest function levels.

domain passwordsettings show|set options [options]
Show/set password settings.

domain passwordsettings pso
Manage fine-grained Password Settings Objects (PSOs).

domain passwordsettings pso apply pso-name user-or-group-name [options]
Applies a PSO’s password policy to a user or group.

domain passwordsettings pso create pso-name precedence [options]
Creates a new Password Settings Object (PSO).

domain passwordsettings pso delete pso-name [options]
Deletes a Password Settings Object (PSO).

domain passwordsettings pso list [options]
Lists all Password Settings Objects (PSOs).

domain passwordsettings pso set pso-name [options]
Modifies a Password Settings Object (PSO).

domain passwordsettings pso show user-name [options]
Displays a Password Settings Object (PSO).

domain passwordsettings pso show-user pso-name [options]
Displays the Password Settings that apply to a user.

domain passwordsettings pso unapply pso-name user-or-group-name [options]
Updates a PSO to no longer apply to a user or group.

domain provision
Promote an existing domain member or NT4 PDC to an AD DC.

domain trust
Domain and forest trust management.

domain trust create DOMAIN options [options]
Create a domain or forest trust.

domain trust delete DOMAIN options [options]
Delete a domain trust.

domain trust list options [options]
List domain trusts.

domain trust namespaces [DOMAIN] options [options]

Manage forest trust namespaces.

domain trust show DOMAIN options [options]
Show trusted domain details.

domain trust validate DOMAIN options [options]
Validate a domain trust.

drs
Manage Directory Replication Services (DRS).

drs bind
Show DRS capabilities of a server.

drs kcc
Trigger knowledge consistency center run.

drs options
Query or change *options* for NTDS Settings object of a domain controller.

drs replicate destination_DC source_DC NC [options]
Replicate a naming context between two DCs.

drs showrepl
Show replication status. The [--json] option results in JSON output, and with the [--summary] option produces very little output when the replication status seems healthy.

dsacl
Administer DS ACLs

dsacl set
Modify access list on a directory object.

forest
Manage Forest configuration.

forest directory_service
Manage directory_service behaviour for the forest.

forest directory_service dsheuristics VALUE

Modify dsheuristics directory_service configuration for the forest.

forest directory_service show
Show current directory_service configuration for the forest.

fsmo
Manage Flexible Single Master Operations (FSMO).

fsmo seize [options]
Seize the role.

fsmo show
Show the roles.

fsmo transfer [options]
Transfer the role.

gpo
Manage Group Policy Objects (GPO).

gpo create displayname [options]
Create an empty GPO.

gpo del gpo [options]
Delete GPO.

gpo dellink container_dn gpo [options]
Delete GPO link from a container.

gpo fetch gpo [options]
Download a GPO.

gpo getinheritance container_dn [options]
Get inheritance flag for a container.

gpo getlink container_dn [options]
List GPO Links for a container.

gpo list username [options]
List GPOs for an account.

gpo listall
List all GPOs.

gpo listcontainers gpo [options]
List all linked containers for a GPO.

gpo setinheritance container_dn block|inherit [options]
Set inheritance flag on a container.

gpo setlink container_dn gpo [options]
Add or Update a GPO link to a container.

gpo show gpo [options]
Show information for a GPO.

group
Manage groups.

group add groupname [options]
Create a new AD group.

group addmembers groupname members [options]
Add members to an AD group.

group delete groupname [options]
Delete an AD group.

group edit groupname
Edit a group AD object.

--editor=EDITOR
Specifies the editor to use instead of the system default, or 'vi' if no system default is set.

group list
List all groups.

group listmembers groupname [options]
List all members of the specified AD group.

group move groupname new_parent_dn [options]

This command moves a group into the specified organizational unit or container.

The groupname specified on the command is the sAMAccountName.

The name of the organizational unit or container can be specified as a full DN or without the domainDN component.

group removemembers groupname members [options]
Remove members from the specified AD group.

group show groupname [options]
Show group object and it’s attributes.

group stats [options]
Show statistics for overall groups and group memberships.

ldapcmp *URL1 URL2 domain|configuration|schema|dnsdomain|dnsforest* [options]
Compare two LDAP databases.

ntacl
Manage NT ACLs.

ntacl changedomsid original-domain-SID new-domain-SID file [options]
Change the domain SID for ACLs. Can be used to change all entries in acl_xattr when the machine’s SID has accidentally changed or the data set has been copied to another machine either via backup/restore or rsync.

--use-ntvfs
Set the ACLs directly to the TDB or xattr. The POSIX permissions will NOT be changed, only the NT ACL will be stored.

--service=SERVICE
Specify the name of the smb.conf service to use. This option is required in combination with the --use-s3fs option.

--use-s3fs
Set the ACLs for use with the default s3fs file server via the VFS layer. This option requires a smb.conf service, specified by the --service=SERVICE option.

--xattr-backend=[native|tdb]

Specify the xattr backend type (native fs or tdb).

--eadb-file=EADB_FILE
Name of the tdb file where attributes are stored.

--recursive
Set the ACLs for directories and their contents recursively.

--follow-symlinks
Follow symlinks when --recursive is specified.

--verbose
Verbosely list files and ACLs which are being processed.

ntacl get file [options]
Get ACLs on a file.

ntacl set acl file [options]
Set ACLs on a file.

ntacl sysvolcheck
Check sysvol ACLs match defaults (including correct ACLs on GPOs).

ntacl sysvolreset
Reset sysvol ACLs to defaults (including correct ACLs on GPOs).

ou
Manage organizational units (OUs).

ou create ou_dn [options]
Create an organizational unit.

The name of the organizational unit can be specified as a full DN or without the domainDN component.

--description=DESCRIPTION
Specify OU’s description.

ou delete ou_dn [options]
Delete an organizational unit.

The name of the organizational unit can be specified as a full DN or without the domainDN component.

--force-subtree-delete
Delete organizational unit and all children reclusively.

ou list [options]
List all organizational units.

--full-dn
Display DNs including the base DN.

ou listobjects ou_dn [options]
List all objects in an organizational unit.

The name of the organizational unit can be specified as a full DN or without the domainDN component.

--full-dn
Display DNs including the base DN.

-r|--recursive
List objects recursively.

ou move old_ou_dn new_parent_dn [options]
Move an organizational unit.

The name of the organizational units can be specified as a full DN or without the domainDN component.

ou rename old_ou_dn new_ou_dn [options]
Rename an organizational unit.

The name of the organizational units can be specified as a full DN or without the domainDN component.

rodc
Manage Read-Only Domain Controller (RODC).

rodc preload SID|DN|accountname [options]

Preload one account for an RODC.

schema
Manage and query schema.

schema attribute modify attribute [options]
Modify the behaviour of an attribute in schema.

schema attribute show attribute [options]
Display an attribute schema definition.

schema attribute show_oc attribute [options]
Show objectclasses that MAY or MUST contain this attribute.

schema objectclass show objectclass [options]
Display an objectclass schema definition.

sites
Manage sites.

sites create site [options]
Create a new site.

sites remove site [options]
Delete an existing site.

spn
Manage Service Principal Names (SPN).

spn add name user [options]
Create a new SPN.

spn delete name [user] [options]
Delete an existing SPN.

spn list user [options]
List SPNs of a given user.

testparm
Check the syntax of the configuration file.

time
Retrieve the time on a server.

user
Manage users.

user add username [password]
Create a new user. Please note that this subcommand is deprecated and available for compatibility reasons only. Please use samba-tool user create instead.

user create username [password]
Create a new user in the Active Directory Domain.

user delete username [options]
Delete an existing user account.

user disable username
Disable a user account.

user edit username
Edit a user account AD object.

--editor=EDITOR
Specifies the editor to use instead of the system default, or 'vi' if no system default is set.

user enable username
Enable a user account.

user list
List all users.

user setprimarygroup username primarygroupname
Set the primary group a user account.

user getgroups username
Get the direct group memberships of a user account.

user show username [options]
Display a user AD object.

--attributes=USER_ATTRS
Comma separated list of attributes, which will be printed.

user move username new_parent_dn [options]
This command moves a user account into the specified organizational unit or container.

The username specified on the command is the sAMAccountName.

The name of the organizational unit or container can be specified as a full DN or without the domainDN component.

user password [options]
Change password for a user account (the one provided in authentication).

user setexpiry username [options]
Set the expiration of a user account.

user setpassword username [options]
Sets or resets the password of a user account.

user getpassword username [options]
Gets the password of a user account.

user syncpasswords --cache-ldb-initialize [options]
Syncs the passwords of all user accounts, using an optional script.

Note that this command should run on a single domain controller only (typically the PDC-emulator).

vampire [options] *domain*
Join and synchronise a remote AD domain to the local server. Please note that samba-tool vampire is deprecated, please use samba-tool domain join instead.

visualize [options] *subcommand*
Produce graphical representations of Samba network state. To work out what is happening in a replication graph, it is sometimes helpful to use visualisations.

There are two subcommands, two graphical modes, and (roughly) two modes of operation with respect to the location of authority.

MODES OF OPERATION

samba-tool visualize ntdsconn
: Looks at NTDS connections.

samba-tool visualize reps
: Looks at repsTo and repsFrom objects.

samba-tool visualize uptodateness
: Looks at replication lag as shown by the uptodateness vectors.

GRAPHICAL MODES

--distance
: Distances between DCs are shown in a matrix in the terminal.

--dot
: Generate Graphviz dot output (for ntdsconn and reps modes). When viewed using dot or xdot, this shows the network as a graph with DCs as vertices and connections edges. Certain types of degenerate edges are shown in different colours or line-styles.

--xdot
: Generate Graphviz dot output as with [--dot] and attempt to view it immediately using /usr/bin/xdot.

-r
: Normally, samba-tool talks to one database; with the [-r] option attempts are made to contact all the DCs known to the first database. This is necessary for samba-tool visualize uptodateness and for samba-tool visualize reps because the repsFrom/To objects are not replicated, and it can reveal replication issues in other modes.

help

Gives usage information.

VERSION

This man page is complete for 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.