Table of Contents

NAME

dacontrol − enable, disable, or view session or individual command auditing for the local computer.

SYNOPSIS

dacontrol [−−installation *installation−name* [−−enable] [−−disable] [−−query] [−−command *path*] [−−monitor] [−−no−monitor] [−−force] [−−all−commands] [−−suspend] [−−resume] [−−verbose] [−−version]

DESCRIPTION

The **dacontrol** command allows you to enable or disable session or individual command auditing on a Linux or UNIX−based computer. If you want to audit specific commands, you must specify the full path to the each command to be audited. You can also use **dacontrol** to suspend or resume auditing on a local computer. For example, you might want to temporarily suspend auditing if there is a problem with the collector service, then resume auditing when the issue is resolved.

If you do not use the Installation group policy to identify the audit installation, you can use this command to manually configure the audit installation for the local computer to use. If you attempt to set the installation locally when the Installation group policy is enabled, **dacontrol** displays an error message. To change the installation to which an audited computer sends information, change the group policy setting or verify that the Installation group policy is set to Not Configured.

Note Only users with root privileges can run **dacontrol** commands.

OPTIONS

You can use the following options with this command:

−i, −−installation
installation_name Locally configure the audit installation for the audited system. This option is not valid for agents that have been configured to use a specific installation by group policy. If the installation has not been configured, running **dacontrol** with no parameters lists the valid installation names. A return code of 0 indicates success; 1 indicates unexpected errors; and 2 indicates a usage error.

−e, −−enable
Enable the auditing of activity on the local computer. You can enable auditing for a specific command by using this option in combination with the **−c** option.

−d, −−disable
Disable the auditing of activity on the local computer. You can also disable auditing for a specific command by using this option in combination with the **−c** option, or disable auditing for all commands with the **−a** option. If no option is specified, session auditing is disabled.

−q, −−query
Reports whether auditing is enabled or disabled. The output is the same as running **dacontrol** without any options.

−c, −−command
path Specify the path to a command for which to enable, disable, or query. After you enable auditing for individual commands, older versions of the auditing service required you to open the centrifyda.conf configuration file to set the dash.allinvoked parameter to true. If the agent is 3.x or later this change is

not required to allow auditing of the shell under which the command is executed. **Note:** If you restrict auditing to specific commands and you include a command that can be called by another command, you should audit the parent command too. For example, if you audit ssh, be sure to also audit scp (which calls ssh). In some circumstances, failure to audit the parent command can result in erratic terminal behavior when the command exits. If this occurs, restart the terminal to return it to normal behavior.

−m, −−monitor
Use this option to enable advanced monitoring. (Only available on Redhat x86_64)

−n, −−no-monitor
Use this option to disable advanced monitoring. (Only available on Redhat x86_64)

−f, −−force
Use this option to force the operation despite warnings. May only be used with the −−monitor option. (Only available on Redhat x86_64)

−a, −−all−commands
Use this option in combination with the −−disable option to disable auditing on all commands.

−s, −−suspend
Suspend command−level auditing temporarily.

−r, −−resume
Resume command−level auditing after temporarily suspending it.

−V, −−verbose
Display detailed information about each operation performed.

−v, −−version
Display version information for the software.

EXAMPLES

You can use **dacontrol** to enable, disable, or view the auditing configuration on a local computer.

To enable auditing for all session activity on a local computer, type:

```
dacontrol −−enable
```

To determine whether auditing is enabled or disabled and the names of valid installations, type:

```
dacontrol
```

This command generates a summary similar to the following:

```
The Installation has not been configured for this machine.
Valid Installations:
   accountingInstallation
```

To disable all auditing, type:

```
dacontrol −−disable
```

To list the enable/disable status of a specific installation, type:

```
dacontrol −i
installationName
```

This command generates a summary similar to the following:
This machine belongs to the ’accountingInstallation’ Installation.

To enable auditing for a specific command, type:

```
dacontrol −e −c /usr/bin/ssh
dacontrol −e −c /usr/bin/scp
```

No additional configuration is required if you have an agent that is version 3.x or later. If you have an older version of the agent, you must also set the dash.allinvoked configuration parameter to true:
dash.allinvoked: true

To restart the
dad
process after running stopping it, type:

```
dacontrol −d
dacontrol −e
```

AUTHOR

Centrify Corporation

SEE ALSO

For related information, see the following command reference sections: dainfo(1), dad(1), dashellfix(1), dadebug(1), dareload(1)

NAME

dad − start the DirectAudit daemon.

SYNOPSIS

```
dad [−c] [−d] [−v]
```

DESCRIPTION

The **dad** program starts the DirectAudit daemon (dad).

Note On AIX you cannot start dad directly. Use the **dastart** command instead.

OPTIONS

You can use the following options with this command:

−c The **−c** option prevents the Centrify DirectAudit Daemon from generating a core dump.

−d The **−d** option sets the Centrify DirectAudit Daemon to run in debug mode.

−v, −−version
Display version information for the agent.

EXAMPLES

To start the DirectAudit daemon, type:

```
dad
```

On AIX, to start the DirectAudit daemon, type:

```
dastart
```

AUTHOR

Centrify Corporation

SEE ALSO

For related information, see the following command reference sections: dacontrol(1), dainfo(1), dastart(1)

NAME

dadebug − controls debug logging

SYNOPSIS

dadebug [option]

DESCRIPTION

The **dadebug** command enables or disables debug logging for the dad process on an audited Linux or UNIX computer. If you run this command without specifying an option, **dadebug** displays its current status, indicating whether debug logging is enabled or disabled.

You must be logged in as root to run this command. Note that the **clear** option is not supported on all platforms. For example, the **clear** option is not applicable if you have an operating system, such as Fedora 20, that writes system messages to the journal log file instead of using syslog.

OPTIONS

You can use the following options with the **dadebug** command:

on

The **on** option configures /etc/centrifyda/centrifyda.conf to log DEBUG messages, and configures syslog daemon (syslog|syslogd|syslog-ng) to route debug information into centrifyda.log. You should note that the log file location can vary depending on the operating system of the local computer. On most computers, the log is located in the */var/log* directory. However, you should consult the documentation for your specific operating system to determine where system messages are recorded.

off

The **off** option configures /etc/centrifyda/centrifyda.conf to log INFO messages, and configures syslog daemon (syslog|syslogd|syslog-ng) to route nothing to centrifyda.log.

clear

The **clear** option clears the contents of the existing log file, then continues logging activity to the cleared log file if the local computer uses the traditional syslog location to log data. If the local computer uses systemd journal to log system messages, however, this option is not supported.

[syslog|journal]

The **syslog** or **journal** option forces the traditional syslog daemon or systemd journal daemon to reload its configuration file. Specifying this option is useful if you are running DirectSecure. If the local computer uses the traditional syslog to log messages, use the **syslog** option. If the local computer uses systemd journal to log messages, use the **journal** option. If the local computer writes system messages to the journal, log files are located in the /var/log/journal and /run/log/journal directories. You can use

journalctl to view and manage journal log files.

[status]

The **status** option prints the current logging level for all modules. The supported levels are TRACE, DEBUG, INFO, WARN, ERROR, FATAL and DISABLED.

[set [module name] [level]]

The **set** option allows you to set a *module* and *level.* You can set a level without a module, in which case it applies to the default (log) module, or you can specify a module name and set the level for that module. The level must be specified by using one of the following key words, from the most detailed logging of messages (TRACE) to the least level of detail (DISABLED). You must use all capital letters when specifying the level keyword: TRACE, DEBUG, INFO, WARN, ERROR, FATAL and DISABLED.

RETURN CODES

Code	Description
0	Command executed successfully
1	Unexpected error
2	Usage error

EXAMPLES

Example 1. Turn on debugging.

```
[root@inst_x]# dadebug on

Configure /etc/syslog.conf

Send HUP signal to syslogd

Configure log level in /etc/centrifyda/centrifyda.conf

Reload /etc/centrifyda/centrifyda.conf

Centrify DirectAudit debug logging is on
```

Example 2. Turn off debugging.

```
[root@inst_x]# dadebug off

Configure /etc/syslog.conf

Custom setting of /var/log/centrifydc.log found in /etc/syslog.conf.

Send HUP signal to syslogd

Configure log level in /etc/centrifyda/centrifyda.conf

Reload /etc/centrifyda/centrifyda.conf

Centrify DirectAudit debug logging is off
```

AUTHOR

Centrify Corporation

SEE ALSO

For related information, see the following command reference sections: dacontrol(1), dad(1), dadiag(1), dainfo(1), dareload(1), dashellfix(1)

NAME

dadiag − display detailed information about the auditing status for the local computer.

SYNOPSIS

dadiag

DESCRIPTION

The **dadiag** command displays detailed information about the auditing configuration and the current auditing status for the local computer. The **dadiag** command returns the same information as the **dainfo** command with the −d option. The **dadiag** command does not have any options.

Note: You must run this command as root to see complete information. It is equivalent to using **dainfo** without the **−−diag** option. If you run as a user other than root, the command displays a status summary.

EXAMPLES

To display complete diagnostic information for the local computer, type:

```
dadiag
```

If the connection to the **dad** process is successful, the **dadiag** command returns detailed information about the local computer and the auditing infrastructure, including the size of the offline storage file, and the installation, audit store, and collector that the agent is sending its data to. The output is exactly the same as running the **dainfo −d** command.

AUTHOR

Centrify Corporation

SEE ALSO

For related information, see the following command reference sections: dainfo (1) dacontrol(1), dad(1),

NAME

daflush − Clear the in−memory cache of Centrify auditing−related information.

SYNOPSIS

daflush [−−name−service] [−−installation−info]

DESCRIPTION

The **daflush** command auditing−related information from the Centrify agent in−memory cache. You can clear the cache of information related to name service queries, the audit installation, or both.

The **daflush** command also automatically clears the cache for common name services−−such as nscd and pwgrd−−if those services are running on the local computer. The **−−name−service** option is especially useful if you make changes that would affect the results of a name service query, and want to ensure you get updated information. For example, if you remove the UNIX Login role for an Active Directory user, some information for that user might remain in the auditing service cache and be returned when you run a command such as "getent passwd" for that user. You can run **daflush** to ensure the user is removed completely from the local computer cache, including the auditing service cache.

You must be logged on as the root user to run this command.

OPTIONS

You can use the following options with this command.

−n, −−name−service
The **−−name−service** option removes information returned by name service queries from the auditing service cache.

−i, −−installation−info
The **−−installation−info** option remove information about the audit installation from the auditing service cache.

EXAMPLES

To remove both name service and audit installation information from the cache for the local computer, type:

```
daflush
          DA  name cache flushed successfully.  DA installation information cache flushed successfully.
```

AUTHOR

Centrify Corporation

SEE ALSO

For related information, see the following command reference sections: dacontrol(1), dad(1), dadiag(1)

NAME

dainfo − display detailed information about the auditing status for the local computer.

SYNOPSIS

dainfo [−−begin <timestamp>] [−−config] [−−diag] [−−end <timestamp>] [−−lastnhrs <n>] [−−support] [−−username] [−−version] [−−product−version] [−−dadactioncount] [−−query *info]*

DESCRIPTION

The **dainfo** command displays detailed information about the configuration of the auditing infrastructure and the current auditing status−for the local computer. If you do not specify an option, **dainfo** returns a reduced set of diagnostic information.

Note that not all options are supported on all platforms. For example, some options, such as −−begin, −−end, and −−lastnhrs, are only applicable if the operating system writes system messages to the journal log file instead of using syslog. For example, some distributions of Linux, such as Fedora 20, use systemd to log messages in the journal.

The −−query option enables you to return specific information about the status or configuration of the auditing infrastructure and is particularly useful if you include **dainfo** calls in scripts.

OPTIONS

You can use the following options with this command:

−b, −−begin <timestamp>
Specify the timestamp at which you want to begin getting information from the log file. Use the following format to specify the timestamp: "yyyy−mm−dd hh:mm:ss"

−c, −−config
Display the parsed contents of the agent configuration file for auditing−related parameters.

−d, −−diag
Display complete diagnostic information. If you do not specify any options, **dainfo** displays a reduced set of diagnostic information, including the status of the auditing service (DirectAudit daemon or "dad" process) and whether NSS auditing is enabled and disabled.

−e, −−end <timestamp>
Specify the timestamp at which you want to end getting information from the log file. use the following format to specify the timestamp: "yyyy−mm−dd hh:mm:ss"

−l, −−lastnhrs <n>
Display the last <n> number of hours of logging activity. The value you specify must be a positive integer [1...999999].

−t, −−support
Output complete diagnostic information to be sent to Centrify Support for analysis. Use this option in conjunction with the −−begin and −−end options or the −−lastnhrs option if your operating system uses the systemd journal for logging (for example, if the local computer runs Fedora 20).

−u, −−username
Display audited status for the specified username.

−v, −−version
Display version information for the agent.

−x, −−product−version
Display DirectAudit version and Centrify Infrastructure Services version information.

−C, −−dadactioncount
Display details about the number of operations performed. The dad process keeps track of different types of network operations, such as the number of reconnections, active sessions, and agent status updates. You can use this option to see these statistics for troubleshooting and analysis.

−q, −−query info
Display the current status or configuration detail based on the type of information requested. You can query for the following types of information using the following keywords as the "info" argument:

- **adclient_status** will return available or not_available with the result codes 0, 1.

- **advanced_monitoring** will return the status of the advanced monitoring feature with the one of the following result codes enabled: online (0), enabled: offline (1), enabled: unknown (2), disabled (3), not supported (4) or unknown (5).

- **dad_status** will return online, offline, or not_available with the result codes 0, 1, 2.

- **collector_name** will return <host:port:spn> or not_available with the result codes 0, 1.

- **spool_rate** will return the spool rate in bytes per second with the return codes of 0 for no transmission or the transmission rate.

- **spool_size** will return the spool size in bytes with the return codes of 0 for no spool or the spool size.

- **installation** will return the installation name or not_available with the return codes 0, 1.

- **installation_source** will return local or group_policy with the return codes 0, 1.

- **nss_status** will return active or inactive with the return codes 0, 1.

- **command_audit** will return the list of audited commands, if applicable, with the return code equal to the total number of audited commands.

- **parameter_value:<parameter_name>** will return the parameter value for specified parameter name with the result codes 0 if the parameter is defined in the centrifyda.conf file, 1 if the parameter is using a default value not specified in the centrifyda.conf file, or 2 if the parameter value is not defined.

EXAMPLES

To display the basic diagnostic information, you can type "dainfo" without any command line options. The command returns information similar to the following:

```
Pinging adclient:   adclient is available
Daemon status:      Online
Current                collector:                   DC2008r2−LG.pisto−
las.org:5063:HOST/dc2008r2−lg@PISTOLAS.ORG
Session offline store size:     0.00 Bytes
Session despool rate:           0.00 Bytes/second
Audit trail offline store size: 0.00 Bytes
Audit trail despool rate:       0.00 Bytes/second
Getting offline database information:
   Size on disk: 14.00 KB
   Database  filesystem  use:  3.20 GB used, 15.52 GB total, 12.31 GB
free
DirectAudit NSS module: Active
User (fred) audited status: Yes
DirectAudit is not configured for per command auditing.
```

To display complete diagnostic information for the local computer, type:

```
dainfo −d
```

The **−d** option returns information similar to the **dadiag** command. To display auditing status for a user, type:

```
dainfo −u username
```

The **−u** option returns information similar to the following:

```
User (username) audited status: Yes
```

To display only the status of the adclient process, you can use the query option. For example, type: dainfo −−query adclient_status

This command returns the result to standard output. For example: available

To display the host name, port, and service principal name of the collector, you can type: dainfo −−query collector_name

The command returns information similar to the following to standard output: w2012r2.acme.com:5063:HOST/w2012r2.acme.com@ACME.COM

AUTHOR

Centrify Corporation

SEE ALSO

For related information, see the following command reference sections: dacontrol(1), dad(1), dadiag(1)

NAME

dareload

− Forces reload of dad configuration and applies properties without restarting the dad daemon

− Forces reload of advanced monitoring configuration properties without restarting the dad daemon

− Forces rebind to another collector without restarting dad daemon

SYNOPSIS

dareload [−−reload−properties] [−−reload−monitoring] [−−rebind−collector]

DESCRIPTION

The **dareload** command with **−p** forces dad to reload the configuration properties in /etc/centrifyda/centrifyda.conf, and the changes made to the configuration properties take effect without restarting the dad daemon.

The **dareload** command with **−m** forces dad to reload the advanced monitoring properties in /etc/centrifyda/centrifyda.conf without restarting the dad daemon.

The **dareload** command with **−b** forces dad to rebind to another collector without restarting the dad daemon if two or more collectors are available.

You must be logged in as root to run it.

OPTIONS

You can use the following options with this command.

−p, −−reload−properties
The **−−reload−properties** option forces reload of dad configuration and applies properties.

−m, −−reload−monitoring
The **−−reload−monitoring** option forces a reload of the advanced monitoring configuration parameters. (Only available on Redhat x86_64)

−b, −−rebind−collector
The **−−rebind−collector** option forces rebind to another collector.

RETURN CODES

Code	Description
0	Command executed successfully
1	DirectAudit daemon not running or unreachable
2	Root privilege required
3	Other unexpected errors

EXAMPLES

```
[root@installation_x]# dareload
The auditing service’s properties have been successfully reloaded.

[root@installation_x]# dareload −p
The auditing service’s properties have been successfully reloaded.

[root@installation_x]# dareload −m
The DirectAudit advanced monitoring configuration has been successfully reloade

[root@installation_x]# dareload −b
Collector rebound successfully: Collector was changed from xxx to yyy.
```

AUTHOR

Centrify Corporation

SEE ALSO

For related information, see the following command reference sections: dacontrol(1), dad(1), dadebug(1), dadiag(1), dainfo(1), dashellfix(1)

NAME

dashellfix −

SYNOPSIS

dashellfix

DESCRIPTION

The **dashellfix** command is provided to support releases earlier than 2015, in which per−user auditing was supported.

The **dashellfix** command points user shells back to their original source. You need to run the **dashellfix** command if you enable auditing on a per user basis and if any machines in the zone that is being audited do not have DirectAudit installed.

Note The **dashellfix** command is installed with the Centrify DirectAudit package. Therefore, machines that do not have DirectAudit installed will not have **dashellfix** installed. To be able to run **dashellfix,** you must copy **dashellfix** from a machine with Centrify DirectAudit installed to all UNIX machines in the zone that do not have DirectAudit installed.

The **dashellfix** command is intended to be run only on machines that do not have DirectAudit installed. If you run **dashellfix** on a machine with DirectAudit installed, the command simply returns an error message.

DirectAudit uses the **cdash** shell to record terminal sessions. When you enable auditing in per user mode on a machine, you set the shell for each user to be audited to load **cdash** instead of the original shell. To preserve the original shell choice for the user, **cdash** is extended. For example, to load **cdash** when the shell for the user is /usr/bin/bash, the path of the user must be set to /usr/bin/cdash_usr_bin_bash.

On a machine without DirectAudit, **cdash** is not installed, so users whose shell has been changed, have no shell to load. To fix the problem, run **dashellfix** on machines without DirectAudit. It points the extended **cdash,** for example, /usr/bin/cdash_usr_bin_bash, back to the original shell, in this case, /usr/bin/bash.

EXAMPLES

To return all shells on a non−DirectAudit machine to their original paths, type:

```
dashellfix
```

AUTHOR

Centrify Corporation

SEE ALSO

For related information, see the following command reference sections: dacontrol(1), dainfo(1), dad(1) dadiag (1)

NAME

daspool − Display information about the auditing−related offline cache (spool) files.

SYNOPSIS

daspool [[−−directory *path*] | [−−session−file *file_name*] | [−−audit−trail−file *file_name*]] [−−check] [−−version]

daspool [−−resume] *spool_id*

DESCRIPTION

You can use the **daspool** command to display information about the contents of auditing−related spool files, check a spool file for internal consistency, or resume a paused spool file. You can specify a spool directory, an individual session spool file, an individual audit trail spool file, or list information about the contents of all spool files.

On most Linux and UNIX computers, the offline cache spool files are located in the /var/centrifyda/spool−atdbqc, /var/centrifyda/spool−dbqc, and /var/centrifyda/spool−sessions directories.

In most cases, you execute **daspool** without any command line arguments. If the auditing service (dad) is running, the **daspool** command requests information about the spool files from the auditing service and displays the results. If the auditing service isn’t running, you can use **daspool** to open the spool files directly to report their status, view details for offline analysis, or to check the files for consistency. However, you must have root privileges to use **daspool** to work with the spool files directly.

Note that you should never copy spool files or report on individual spool files while the auditing service is running because they might be in an inconsistent state. If a collector has a problem processing a message to be written to one of the spool files, that spool is paused until the auditing service resumes processing for all spool file to determine whether the problem still exists. You can use the **daspool** command to attempt to manually resume a paused spool or all spools before the auditing service does.

OPTIONS

You can use the following options with this command.

−d, −−directory
path The **−−directory** option enables you to specify the location of the spool directory that contains the spool files you want to review..

−s, −−session−file
dbq_file_name The **−−session−file** option enables you list the contents of a single session spool file specified by the *dbq_file_name* argument.

−a, −−audit−trail−file
dbq_file_name The **−−audit−trail−file** option enables you to list the contents of a single audit trail spool file specified by the *dbq_file_name* argument.

−c, −−check
The **−−check** option enables you to check all spool files for internal consistency.

−V, −−version
Display version information for the agent.

−r, −−resume
spool_id The **−−resume** option enables you to resume a paused spool. You can specify an individual session globally−unique identifier (GUID) or use one of the following keywords:

− "all" to resume all paused spool files.

− "common" to resume the common spool file.

− "at" to resume the audit trail spool file.

EXAMPLES

To list information about the contents of the common, session, and audit trail offline cache spool files, type:
daspool

This command displays output similar to the following:

```
Common Spool:
   Paused:       no
   Status:       ok
   Queue file: 0
      Message count: 6
      Size:          192 bytes
      Size    on     disk:      3584     bytes     Session     Spool:
e2ed9c24−c8e9−a148−b53d−4ccd88c96873
   Paused:       no
   Status:       ok
   Queue file: 0
      Message count: 104
      Size:          6651 bytes
      Size     on     disk:      54272     bytes    Session    Spool:
bbf6573d−3fc0−6344−bccc−f82b372e1dcc
   Paused:       no
   Status:       ok
   Queue file: 0
      Message count: 12009
      Size:          787981 bytes
      Size    on    disk:     6155776    bytes     Session     Spool:
c6c559b0−6f29−bd40−9e6c−dd128acafe45
   Paused:       no
   Status:       ok
   Queue file: 0
      Message count: 0
      Size:          0 bytes
      Size on disk:  1024 bytes Audit Trail Spool:
   Paused:       no
   Status:       ok
   Queue file: 0
      Message count: 4
      Size:          569 bytes
      Size on disk:  2560 bytes
```

To resume all spools, type:
daspool −−resume all

To report information for an individual session spool while the auditing service is stopped, type a command similar to this: daspool −s /var/centrifyda/spool−sessions/53/e2ed9c24−c8e9−a148−b53d−4ccd88c96873.dbq/0

AUTHOR

Centrify Corporation

SEE ALSO

For related information, see the following command reference sections: dacontrol(1), dad(1), dadiag(1)

NAME

dastart − start the auditing daemon (dad).

SYNOPSIS

dastart

DESCRIPTION

The **dastart** program starts the auditing service daemon (dad) on AIX computers. On AIX computers, you cannot start the dad process directly. This program does not have any options.

EXAMPLES

To start the auditing service daemon, type:

```
dastart
```

AUTHOR

Centrify Corporation

SEE ALSO

For related information, see the following command reference sections: dacontrol(1), dainfo(1), dad(1) dadiag (1)

NAME

cdash − auditing service shell wrapper

SYNOPSIS

cdash

DESCRIPTION

The **cdash** program is an auditing shell wrapper that records all terminal traffic. The Centrify auditing service is able to capture stdin, stdout, and stderr shell traffic by replacing shell binaries with copies of the **cdash** wrapper program when auditing is enabled on a computer. You can control whether individual commands or user sessions are audited using the **dacontrol** command.

OPTIONS

This command takes no options.

AUTHOR

Centrify Corporation

SEE ALSO

For related information, see the following command reference sections: dacontrol(1), dainfo(1), dad(1)

NAME

adbindproxy.pl − configure Centrify for Samba to work with Centrify DirectControl.

SYNOPSIS

adbindproxy.pl [−−help] [−−info] [−−restore] [−−unconfig] [−−adjoinExtraOptions] [−−adleaveExtraOptions] [−−version] [−−verbose]

adbindproxy.pl [−−export] [−−groupFile *filename]* [−−userFile *filename]* [−−tdbfile *filename]*

adbindproxy.pl [−−record] [−−responseFile *filename]*

adbindproxy.pl [−−nonInteractive] [−−responseFile *filename]*

DESCRIPTION

The **adbindproxy.pl** script is both a utility that you can use to configure a Centrify for Samba build to work with Centrify DirectControl, and a configuration script built around the utility that guides an administrator through the configuration process. This man page provides a reference to the utility.

Use the **−−info** option to retrieve interoperability information about Samba and Centrify DirectControl.

You may also use the **−−restore** option to restore files backed up from the previous installation.

Use **adbindproxy.pl** without options to run the script and configure Centrify for Samba to work with Centrify DirectControl.

Note To run **adbindproxy.pl** , you must be logged in as root.

OPTIONS

You can use the following options with this command:

−E −−export
Export user IDs (UIDs) and group IDs (GIDs) that are stored in the windbindd idmap tdb file. After export, you can use the Centrify Access Manager Console to import the users and groups with their existing UID and GID mappings into a zone. Use the −g and −u options to specify the export files for the GIDs and UIDs. Use the −t option to specify the .tdb file that contains the GIDs and UIDs.

−f −−responseFile filename
The *filename* specifies the response file for recording with the −x option, or for non−interactive mode with the −n option.

−g −−groupfile filename
The *filename* specifies the file in which to write the Samba−created ADGroup to GID mappings. Use this option with the −E option. By default, this file is: /var/centrify/samba/group.

−h −−help
Display the **adbindproxy.pl** help screen.

−i −−info
Display Centrify for Samba interoperability information.

−j −−adjoinExtraOptions adjoinoptions
The *adjoinoptions* are the additional options to be used for the **adjoin** command.

−l −−adleaveExtraOptions adleaveoptions
The *adleaveoptions* are the additional options to be used for the **adleave** command.

−n −−nonInteractive
Run **adbindproxy.pl** in non−interactive mode using the response file.

It is recommended to have the machine joined to the AD domain before running this script in non−interactive mode.

Otherwise, **adbindproxy.pl** needs to obtain the AD authorized user password from the command line with the −j/−l option, or interactively from the terminal.

WARNING: Typing password in command line is insecure, do not do that unless you know what you are doing.

−r −−restore
Restore files backed up from the first time you configured Centrify for Samba to work with DirectControl. Typically, you run **adbindproxy.pl** with the −r option to restore Samba configuration files before uninstalling Centrify for Samba.

−t −−tdbfile filename
The *filename* specifies the location of the windbindd idmap tdb file that contains Samba UID and GID information.

When using the −E option to export UID and GID information, use this option to specify an alternate windbindd idmap tdb file for exporting. If you omit this option, the default setting is to export from /var/lib/samba/winbindd_idmap.tdb.

−u −−userfile filename
The *filename* specifies the file in which to write Samba−created ADUser to UID mappings. Use this option with the −E option. By default, this file is: /var/centrify/samba/passwd.

−U −−unconfig
Unconfigure CentrifyDC Samba service.

−v −−version
Display version information for the installed software.

−V −−verbose
Display detailed information for each operation.

−x −−record
Record the user input into the response file which can be used later in non−interactive mode.

EXAMPLES

You can use **adbindproxy.pl** to display information about interoperability between Samba and Centrify DirectControl:

```
# adbindproxy.pl −i
The Samba base path is:        /usr

CentrifyDC version           = 5.5.0−180
CentrifyDC Architecture      = 64−bit
CentrifyDC Realm             = ARCADE.NET
CentrifyDC NTLM Domain       = ARCADE
CentrifyDC Host              = magnolia.arcade.net
CentrifyDC Short Host        = magnolia

Samba Version                = 4.2.3
Samba Architecture           = 64−bit
Samba Realm                  = ARCADE.NET
Samba NetBIOS Name           = MAGNOLIA

Samba Version Supported      = yes
Samba and CDC in same Realm  = yes
Samba and CDC share machine account = yes
Password sync using libtdb   = <not specified>
```

To export existing Samba GID and UID information for import to Centrify DirectControl, using the −V option to show details of the operation:

```
# adbindproxy.pl −EV
The existing UID mappings have been exported to /var/centrify/samba/passwd.
The existing GID mappings have been exported to /var/centrify/samba/group.
```

To record the user input to a response file:

```
# adbindproxy.pl −x
```

To run **adbindproxy.pl** in non−interactive mode with the response file that generated previously at the default location:

```
# adbindproxy.pl −n
```

AUTHOR

Centrify Corporation

SEE ALSO

For related information, see the following command reference sections: adinfo(1), adsmb(1)

NAME

adcache − maintain the Centrify UNIX agent object cache service.

SYNOPSIS

adcache [−−live] [−−cachename *path*] [−−outputfile *path*] [−−directory *path*] [−−quiet] [−−key *value*] [−−reorg] [−−checksum] [−−fromversion *version* | *checksum* | *list* | *auto*] [−−version]

DESCRIPTION

The **adcache** command enables you to manually clear the local Centrify UNIX agent cache on a computer. You can use this command to dump all cache files or a specific cache file. You can also use the command to check a cache file for a specific key value and to reclaim disk space. By default, the program dumps all cache files.

You can run the **adcache** command in one of two ways:

- Without stopping the agent process by using the −−live option. In this case, you must also specify an output file name by using the −−outputfile option.
- After stopping agent (adclient) process. You can stop the adclient process by using the following command:

  ```
  /usr/share/centrifydc/bin/centrifydc stop
  ```

  To restart the adclient process after clearing the cache, use the following command:

  ```
  /usr/share/centrifydc/bin/centrifydc start
  ```

You can automatically stop adclient, optimize the cache disk space, and

restart adclient by specifying **adcache −−reorg** on the command line.

Note that you must have root privileges to run the **adcache** command.

OPTIONS

You can use the following options with this command:

−L, −−live
The **−−live** option enables you to run the **adcache** without stopping the adclient process. If you specify this option, you must specify an output file with the **−−outputfile** option

−c, −−cachename path
The **−−cachename** option enables you to specify the full *path* to the cache file you want to check or clear.

−o, −−outputfile path
The **−−outputfile** option allows you to specify the full *path* to the outputfile. This option is required when using the **−−live** option.

−d, −−directory path
The **−−directory** option allows you to specify the directory for the cache files. The default directory is */var/centrifydc.*

−s, −−checksum
The **−−checksum** option displays the checksum of the current cache format.

−F, −−fromversion version | checksum

The **−−fromversion** option converts the cache file from the specified *version* format to the current format, or converts the cache file from the specified *checksum* format to the current format.

A checksum is a hexidecimal value of the cache format. To specify a checksum, provide the hexdecimal value that starts with "0x", for example, "0x21027".

In most cases, it is not necessary to convert the cache manually to the latest format. The cache is automatically updated when you upgrade to a newer version of the Centrify agent.

You should only run the **adcache** command with the **−F** option if instructed to do so by Centrify Support.

You must stop the adclient process before running the **adcache** command with this option. Before using the −F option after an upgrade, you should restart the adclient process. After the agent starts successfully, run **/usr/share/centrifydc/bin/centrifydc stop** to stop the agent.

−F, −−fromversion list

The **−−fromversion list** option displays a list of the supported version numbers and their checksums. You do not need to stop the agent to use this option.

−F, −−fromversion auto

The **−−fromversion auto** option converts the cache file to the latest format. Starting from version 5.2.1, the cache format information is with the cache therefore it is not necessary to provide the *version* or *checksum* to do the cache conversion.

−q, −−quiet

The **−−quiet** option runs the command without displaying any output. This option is useful for running the command as a scheduled maintenance job.

−k, −−key value

The **−−key** option checks the Centrify agent cache for a specific key *value.*

−r, −−reorg

The **−−reorg** option reorganizes the Centrify agent cache and index files and recovers disk space used by negative items.

To use this option, you must run the **adcache** command as root. If you use this option, **adcache** automatically stops and starts the adclient process.

−v, −−version

The **−−version** option returns the version number for the software you have installed.

EXAMPLES

To check the domain controller cache for a specific key value while the adclient process is running, type a command similar to this:

```
adcache −−live −o /tmp/dcCacheOut.txt −−cachename /var/centrifydc/dc.cache −−key andre
```

The output is sent to the file /tmp/dcCacheOut.txt.

To check the domain controller cache for a specific key value, after stopping adclient, type a command similar to this:

```
adcache −−cachename /var/centrifydc/dc.cache −−key andre
```

To reorganize the Centrify agent cache and index files and recover disk space used by negative items, you would run the following command:

```
adcache −−reorg
```

You should run the **adcache −−reorg** command on a regular basis in a cron job. Depending on how quickly the size of the cache tends to increase in your environment, you may want to schedule this command to run approximately once a week.

AUTHOR

Centrify Corporation

NAME

adcdiag − check if the environment is ready for multi−factor authentication.

SYNOPSIS

adcdiag [−−version] [−−help] [−−verbose] [−−noreport] [−−feature mfa] [−−timeout *test_connection_timeout]* [−−showzoneconfigs] [−−list *[connectors]|[instances]]* [−−visible] [−−tenantid *tenant_id]* [−−instance *cloud_instance]* [−−test *[connection]|[iwaserver]]* [−−cloudurl *url]* [−−connector *fqdn:port]* [−−iwaserverurl *iwaurl]* [−−insecure] [−−cloudinsecure] [−−certstore] [−−proxyauth *method]* [−−proxycredential *username:password]*

DESCRIPTION

The **adcdiag** command is used to check if the environment is ready for multi−factor authentication.

To run **adcdiag** you must be logged in as root.

OPTIONS

You can use the following options with this command:

−f, −−feature mfa
Specify the feature for which you want to check the environment. You can only check whether the environment will support multi−factor authentication.

−n, −−noreport
Perform full set of checking without generate the diagnostic report.

−k, −−insecure
Skip verifying Centrify Connector certificate when checking IWA server function.

−K, −−cloudinsecure
Skip verifying Centrify Identity Platform server certificate when checking Centrify Identity Platform function.

−C, −−certstore
Specify the cert store to verify the Centrify Identity Platform certificate. If not set, Centrify curl will find it itself.

−T, −−timeout test_connection_timeout
Specify the connection timeout in seconds for all connections to Centrify Identity Platform during testing.

The default is 5.

−z, −−showzoneconfigs
Show Centrify Identity Platform configurations in the joined zone.

−l, −−list resourcename
Specify the resource name you want to list:

connectors: list all connectors in the forest.

instances: list the trusted Centrify Identity Platform instance configured in the zone.

−d, −−visible
This option is used as a filter so that only the resources

visible to DirectControl are shown. That is to apply the configurations for DirectControl to search the resources.

−I, −−tenantid tenant_id
When the "resourcename" of "−−list" option is connectors, this option is used as a filter so that only connectors for the specified tenant ID are shown.

−i, −−instance cloud_instance
When the "resourcename" of "−−list" option is connectors, this option is used as a filter so that only connectors to the specified Centrify Identity Platform instance are shown.

−t, −−test functionname
Specify the name of the function which you want to test:

connection: test the connection to the Centrify Identity Platform instance.

iwaserver: test the IWA Server function of the connector.

−U, −−cloudurl url
Specify the URL of your Centrify Identity Platform instance.

−c, −−connector fqdn:port
Specify the FQDN and port for Agent Gateway of the connector used in the test, e.g.

connector.domain.com:8080

If this option is not specified, the tool can talk directly to Centrify Identity Platform.

−A, −−proxyauth method
If not specified, then proxy authentication method is none.

The valid proxy authentication method is among "anyauth", "negotiate", "ntlm", "digest", "basic".

−P, −−proxycredential username:password
This option should be set when proxy authentication type is set.

−s, −−iwaserverurl iwaurl
Specify the URL of IWA server on the connector used in the test, e.g.

http://connector.domain.com:80/

IWA server on the connector is to authenticate the UNIX machine for Centrify Identity Platform authentication.

−T, −−timeout test_connection_timeout
Specify the connection timeout in seconds for all connections to Centrify Identity Platform during testing.

The default is 5.

−V, −−verbose
Print debug information.

−v, −−version
This option displays version information for the installed software.

−h, −−help
This option displays help information for the command line.

EXAMPLES

1. Perform full set of checking for MFA:

```
adcdiag
```

2. Perform full set of checking for AAPM:

```
adcdiag −f aapm
```

3. List all connectors to specific Centrify Identity Platform instance:

```
adcdiag −l connectors −i abc0001.centrify.com
```

4. List all Centrify Identity Platform instances to which the connectors are serving to within the forest:

```
adcdiag −l instances
```

5. Test connection to Centrify Identity Platform through specific HTTP proxy with authentication and timeout 30 seconds:

```
adcdiag −t  connection  −U  https://abc0001.centrify.com:443/  −c
proxyserver.mydomain.com:8080 −A anyauth −P anyone:password −T 30
−V
```

6. Test IWA server function on the connector:

```
adcdiag −t iwaserver −U https://abc0001.centrify.com:443/ −c con−
nector1.mydomain.com:8080  −s  http://connector1.mydomain.com:80/
−V
```

AUTHOR

Centrify Corporation

SEE ALSO

For related information, see the following command reference sections: adinfo(1), addebug(1), adclient(1)

NAME

adcert − Manage Active Directory Certificates.

SYNOPSIS

adcert −−enrollment[−−certdir *directory]* [−−certname *certificate_name]* [−−caname *name]* [−−password *create_password]* [−−caserver *server]* [−−template *template]* [−−algorithm *algorithm]* [−−hash *algorithm]* [−−keysize *size]* [−−help] [−−version] [−−verbose]

adcert −−machine [−−certdir *directory]* [−−certname *certificate_name]* [−−keysize *size]* [−−verbose] [−−storereq]

adcert −−user [−−certdir *directory]* [−−certname *certificate_name]* [−−keysize *size]* [−−verbose] [−−storereq]

DESCRIPTION

The **adcert** command enables you to manage trusted Active Directory Certificate Authority certificates using the Public Key Infrastructure (PKI).

When using the auto−enrollment feature,**adcert** will retrieve all certificate templates in the CA and evaluate the templates individually. If the template is for enrollment and also for auto−enrollment,and there is no valid corresponding certificate present in the certificate output directory,**adcert** will generate a new key based on the template, and will use this key to generate a Certificate Signing Request (CSR) to request a new certificate from the CA.

The **adcert** command can be used to do the following:

- Manually enroll a certificate by specifying the CA, CA server and template (option −e, −−enroll).
- Auto−enroll certificates for the current computer/machine (option −m, −−machine).
- Auto−enroll certificates for the current user (option −u, −−user).

The **adcert** command is mainly used by Group Policy (certgp.pl) to retrieve and renew certificates from Active Directory.

Commands

You can use the following commands with this command:

−e, −−enroll
Enroll certificates for the computer you are using.

−m, −−machine
Retrieve certificates for the machine you are using.

−u, −−user
Retrieve certificates for the specified user. Adcert retrieves the user certificates from the user credential cache.

Options

You can use the following options with this command:

−d, −−certdir <directory>
Specify the directory to which certificates are written.

−n, −−caname <name>
Specify the name of the Certificate Authority you would like to connect to.

−N, −−certname <cert>
Specify the name of the certificate to retrieve.

−p, −−password <password>
Specify a password which will encrypt the PKCS#12 bundle that is created during certificate enrollment.

−s, −−caserver <server>
Specify the name of the server where the Certificate Authority is located.

−t, −−template <template>
Specify the name of the certificate template to use.

−A, −−algorithm <algorithm>
Specify an asymmetric algorithm to generate the key pair for the certificate.

−H, −−hash <algorithm>
Specify the Certificate Signing Request hash algorithm. The following algorithms are available: DSS, DSS1, ECDSA, MD2, MD4, MD5, RIPEMD160, SHA, SHA1, SHA224, SHA256, SHA384, SHA512.

The default algorithm is SHA1.

Note The certificate authority may not support all of the algorithms listed above.

−V, −−verbose
Print detailed information about the operation being performed.

−R, −−storereq
Store the certificate Signing Request (CSR) in PEM format with extension .csr.

−v, −−version
Print the version information.

−h, −−help
Display usage information.

−i, −−ignore
Adcert will not check whether the output directory is world−writable when writing certificates.

−z, −−keysize <size>
Specify the key length.

AUTHOR

Centrify Corporation

SEE ALSO

For related information, see the following command reference sections: adjoin(1), adpasswd(1), adupdate(1), adinfo(1), addebug(1)

NAME

adcheck − check readiness of machine to join an Active Directory domain.

SYNOPSIS

adcheck *[domainName]* [−−alldc] [−−bigdomain *number]* [−−check−space *var_size* : *installdir_size* : *tmp_size*] [−−xml *filename]* [−−tmp_path *path]* [−−skip−ntp] [−−test [os] | [net] | [ad] [−−performance] [−−dnsmarg *threshold]* [−−servername *domainController]* [−−xdomain] [−−user *username]* [−−password *passwd]* [−−recursive] [−−verbose] [−−version] *domain*

DESCRIPTION

The **adcheck** command performs operating system, network, and Active Directory tests to verify that a machine is ready to join the specified Active Directory domain. The *domain* should be a fully−qualified domain name, for example, sales.acme.com.

The output from adcheck includes, notes, warnings, and fatal errors, including suggestions on how to fix them.

By default, when you run **adcheck,** the program performs the following tests:

- Operating system check to verify that the operating system is supported and at the correct patch levels, and that there is sufficient disk space.
- Network check to verify DNS and SSH.
- Active Directory check to verify various aspects of the Active Directory configuration, including the domain name, time and domain synchronization, and checking up to 10 domain controllers (which can be extended by an adcheck parameter for large domains).

You must specify a domain unless you are running the operating system check only (−t os).

OPTIONS

You can use the following options with this command:

−a, −−alldc
Check all domain controllers. This option overrides the **--siteonly** and **--bigdomain** options. The **--servername** option overrides this option. If you do not specify **--alldc, --siteonly,** or **--servername, adcheck** checks the number of domain controllers specified by the **--bigdomain** option (default is 10).

−S, −−siteonly
Check all domain controllers for the first detected site. This option overrides the **--bigdomain** option. The **--alldc** and **--servername** options override this option.

−b, −−bigdomain number
The *number* specifies the number of domain controllers to check. The default is 10. The **--alldc --siteonly,** and **--servername** options override this option.

−x, −−xml filename
The *filename* specifies the filename in which to generate XML output.

−c, −−check−space var_size:installdir_size:tmp_size
Note: Use this option only if requested to do so by Centrify Support. By default, **adcheck** performs a check (SPACECHCK) to verify that the directories required by the DirectControl agent (/var, /usr or /opt, and /tmp) have enough disk space.

Specify the size, in megabytes (MB), for *var_size, installdir_size,* and *tmp_size.* For example, enter this command to verify that /var has at least 500MB, /usr has at least 100MB, and /tmp has at least 10MB:

```
adcheck acme.com −c 500:100:10
```

−m, −−tmp_path path
The *path* specifies the directory in which to generate temporary output. Be certain that this directory has execute permission, otherwise **adcheck** will fail to run. By default, **adcheck** generates temporary output in /tmp for normal users and in /var/centrify/tmp for root users.

−N, −−skip−ntp
Skip the NTP port check, which **adcheck** uses to probe the NPT port (123) to determine whether the domain controller is available. If the domain controller has the SNTP service turned off (for example, the computer synchronizes on a different time source), adcheck reports the failure.

−t, −−test os | net | ad
Run a subset of the tests, as follows:

os Run the operating system check only; does not require that you specify a domain name.

net Run the network check only; requires that you specify a domain name .

ad Run the Active Directory check, which also runs the network check; requires that you specify a domain name.

You can enter multiple **−t** options to specify multiple sub−tests, for example:

```
adcheck ajax.com −t os −t net
```

−P, −−performance
Output a warning message if only one domain controller is found for a domain. The warning message appears in the ADDC section of the output. For optimal performance, more than one DC per domain is recommended.

−T, −−dnsmarg threshold
The *threshold* specifies the response−time threshold, in seconds, which determines whether the DNS server should be classified as marginal. If the DNS response time exceeds the threshold, **adcheck** issues a warning and lists the marginal DNS servers in the DNSCHECK section of the output. The default value is 0.1 seconds.

−s, −−servername domainController
The *domainController* specifies the domain controller to connect to when performing the network checks. You can use this option to override the automatic selection of a domain controller based on the Active Directory site information.

This option overrides the **−−alldc, −−siteonly,** and **−−bigdomain** options.

−X, −−xdomain
This option checks trusts in addition to the specified domain.

−u, −−user username
This option specifies a user with rights to run the Active Directory checks. If this option is not specified, DirectControl uses cached Kerberos credentials for the current user, and if it cannot find credentials, it uses administrator.

−p, −−password passwd
This option specifies a password for the user who is executing the command. If this option is omitted, DirectControl prompts for a password.

−r, −−recursive
This option sends recursive DNS requests. Some caching−only DNS servers only accept recursive DNS requests, such as dnscache of djbdns. If this option is not set, this kind of DNS server is reported as offline.

−V, −−verbose
This option displays diagnostic information about the host, the domain, and the domain controller.

−v, −−version
This option displays version information for **adcheck.**

EXAMPLES

To perform all checks on the acme.com domain using all of the default options, you could type a command line similar to the following:

```
adcheck acme.com
```

You see output similar to the following:

```
OSCHK    : Verify that this is a supported OS                        : Pass
PATCH    : Linux patch check                                         : Pass
PERL     : Verify perl is present and is a good version              : Pass
SPACECHK : Check if has enough disk space in /var /usr /tmp          : Pass
DNSPROBE : Probe DNS server 192.168.43.130                           : Pass
DNSCHECK : Analyze basic health of DNS servers                       : Pass
WHATSSH  : Is this an SSH that DirectControl works well with         : Pass
SSH      : SSHD version and configuration                            : Note
         : You are running sshd version OpenSSH_3.5p1
         : We suggest that you install the Centrify build of OpenSSH
         : This can be obtained from www.centrify.com

DOMNAME  : Check that the domain name is reasonable                  : Pass
ADDC     : Find domain controllers in DNS                            : Pass
ADDNS    : DNS lookup of DC centrify−qa1.acme.com                    : Pass
ADPORT   : Port scan of DC centrify−qa1.acme.com                     : Pass
ADDNS    : DNS lookup of DC centrify−qa1.acme.com                    : Pass
GCPORT   : Port scan of GC centrify−qa1.acme.com                     : Pass
DCUP     : Check DCs in acme.com                                     : Pass
SITEUP   : Check DCs for acme.com in our site                        : Pass
DNSSYM   : Check DNS server symmetry                                 : Pass
ADSITE   : Check that this machine’s subnet is in a site known by AD : Pass
GSITE    : See if we think this is the correct site                  : Pass
```

```
TIME     : Check clock synchronization                              : Pass
ADSYNC   : Check domains all synchronized                           : Pass
```

You can run a subset of the checks. For example, to run only the operating system checks:

```
adcheck acme.com −t os
```

You see output similar to the following:

```
OSCHK    : Verify that this is a supported OS                       : Pass
PATCH    : Linux patch check                                        : Pass
PERL     : Verify perl is present and is a good version             : Pass
SPACECHK : Check if has enough disk space in /var /usr /tmp         : Pass
```

AUTHOR

Centrify Corporation

SEE ALSO

For related information, see the following command reference sections: adjoin(1),adinfo(1)

NAME

adchzone − move a joined computer from a classic zone to a hierarchical zone.

SYNOPSIS

adchzone −z *zoneName* [−u *user*] [−p *passwd*] [−v]

DESCRIPTION

The **adchzone** command allows you to move a joined computer from a classic zone to a hierarchical zone.

Before moving the computer be certain to migrate the classic zone’s data to a hierarchical zone by running the **admigrate** command.

OPTIONS

You can use the following options with this command:

−z zoneName
Specify the distinguished name of the hierarchical zone to join. This parameter is required.

−u user
Specify the Active Directory User Principal Name or Samaccountname of a user account with permission to delete the computer account in the classic zone and add a profile for the computer in the new zone. If you omit this parameter, **adchzone** uses Kerberos credentials for the current user.

−p password
Specify the password for the user account. You will be prompted if you omit this parameter.

−v Print verbose information while the command runs.

EXAMPLES

The following command moves the joined computer on which the command is run to the hierarchical zone "finance", which is a child zone of the parent zone "global".

```
/usr/share/centrifydc/adedit/adchzone \
−z "cn=finance,cn=global,cn=zones,ou=unix,dc=acme,dc=com" \
−u administrator −p passwd
```

AUTHOR

Centrify Corporation

SEE ALSO

For related information, see the following command reference sections:

admigrate (1)

NAME

adclient − control the operation of the Centrify DirectControl Agent.

SYNOPSIS

```
adclient [−x] [−d] [−F]
```

DESCRIPTION

The **adclient** command enables you to control the operation of the Centrify DirectControl Agent on a computer.

Note Although you can run adclient directly from the command line to control the operation of the Centrify DirectControl Agent on a local computer, it is recommended that you do so only under the direction of Centrify support. Typically, you should start and stop **adclient** from a startup script, which is located by default in the /usr/share/centrifydc/bin directory. For example, to start the adclient daemon, run this command:

```
/usr/share/centrifydc/bin/centrifydc start
```

On Solaris, Mac OS X, and certain Red Hat computers, such as computers running RHEL 5.2, you cannot use the **−x** option to stop **adclient,** and on AIX computers, you cannot start or stop **adclient** directly from the command line. When running computers with any of these operating systems, you should use the centrifydc startup script or system resource controller commands, such as **startsrc, stopsrc,** and **lssrc.** For example, to stop the agent use:

```
/usr/share/centrifydc/bin/centrifydc stop
```

or to start adclient with the **−d** and **−F** options on AIX, use a command such as:

```
startsrc −s centrifydc −a "−d −F"
```

OPTIONS

You can use the following options with this command:

−x The **−x** option stops the Centrify DirectControl Agent (adclient) if it is currently running.

Note: On computers running AIX, Solaris, Mac OS X, or RHEL 5.2, this option is not available.

−d The **−d** option sets the Centrify DirectControl Agent to run in debug mode.

−F The **−F** option flushes the Active Directory cache when the Centrify DirectControl Agent is restarted.

−M The **−M** option enables in−memory logging of Centrify DirectControl Agent operations.

EXAMPLES

To flush the cache when the Centrify DirectControl Agent starts:

```
adclient −F
```

AUTHOR

Centrify Corporation

SEE ALSO

For related information, see the following command reference sections: adjoin(1), adpasswd(1), adinfo(1), addebug(1)

NAME

addbloader− create a database file with zone information.

SYNOPSIS

addbloader −db *dbPath* −config *filename* [−v]

DESCRIPTION

The **addbloader** command creates an sqlite database file containing information about the zone. You can use the **adreport** command to generate reports from this file, or read it with standard sqlite tools.

OPTIONS

You can use the following options with this command:

−db dbPath

Specify the path, including the file name, to the sqlite database file to create.

−config filename

Specify a configuration file that you have created. In the configuration file, you need to specify bind and load information for the zones in which you are interested. You should also turn caching on in this file.

If you have any role that is assigned to ’All AD users’ and you want to get the role assignments for users who are not zone enabled, you need to use load_ad_users to load all AD users. load_ad_users has only one required parameter which is the base DN for searching all AD users. There is an optional second parameter for load_ad_user if you want to add more limitation on top of the default filter (&(objectClass=user)(objectcategory=user)). The logic operation between default filter and additional filter is & (AND).

For example, the configuration file could contain information such as the following:

```
bind centrify−qa.test administrator {myP@$swd}
cache on
load_ad_users DC=centrify−qa,DC=test
load_root "cn=finance,cn=global,cn=zones,ou=unix,dc=centrify−qa,dc=test"
load_root "cn=global,cn=zones,ou=unix,dc=centrify−qa,dc=test"
```

If you do not enter a password in the file, you will be prompted for one, however, you must specify a user account with permission to bind to the domain. **−v** Generate verbose information, **−v2** Generate more verbose information,

EXAMPLES

The following command creates a database file containing zone information.

```
/usr/share/centrifydc/adedit/addbloader \
−db /tmp/zone_report \
−config ./zone_report.config
−v
```

AUTHOR

Centrify Corporation

SEE ALSO

For related information, see the following command reference sections:

adreport (1)

NAME

addebug − start or stop detailed logging of Centrify adclient activity on the local computer.

SYNOPSIS

addebug [option]

DESCRIPTION

The **addebug** command is used to start or stop detailed logging activity for the Centrify adclient process on a local UNIX computer. If you do not specify an option, **addebug** displays its current status, indicating whether logging is active or disabled. When you run this command with the *on* option, all of the Centrify adclient activity is written to the system log directory in the *centrifydc.log* file or *journal* file.

For most operating systems, the system log directory is */var/log.* However, for HPUX computers, the system log directory is */var/admin/syslog.* In addition, some distributions of Linux, such as Fedora 20, write system messages to the journal file instead of the traditional syslog location.

For performance and security reasons, you should only enable Centrify logging when necessary, for example, when requested to do so by Centrify Support, and for short periods of time to diagnose a problem. Keep in mind that sensitive information may be written to the log file and you should evaluate the contents of the file before giving others access to it.

To run the **addebug** command, you must be logged in as root.

If the adclient process stops running while logging is on, the **addebug** program records messages from PAM and NSS requests in the *centrify_client.log* file in the system log directory. Therefore, you should also check that file location if you enable logging.

OPTIONS

You can use the following options with this command:

[on] The *on* option starts logging all Centrify adclient activity in the *centrifydc.log* file or the *journal* file as described above.

[off] The *off* option stops logging all Centrify adclient activity.

[clear]
The *clear* option clears the existing log file, then continues logging activity to the cleared log file if the local computer uses the traditional syslog location to log data. If the local computer uses systemd journal to log system messages, however, this option is not supported.

[syslog|journal]
The *syslog* or *journal* option forces the traditional syslog daemon or systemd journal daemon to reload its configuration file. Specifying this option is useful if you are running DirectSecure. If the local computer uses the traditional syslog to log messages, use the *syslog* option. If the local computer uses systemd journal to log messages, use the *journal* option. If the local computer writes system messages to the journal, log files are located in the /var/log/journal and /run/log/journal directories. You can use **journalctl** to view and manage journal log files.

[status]
The *status* option prints the current logging level for all modules. The supported levels are TRACE, DEBUG, INFO, WARN, ERROR, FATAL and DISABLED.

[set [module name] [level]]
The *set* option allows you to set a *module* and *level.* You can set a level without a module, in which case it applies to the default (log) module, or you can specify a module name and set the level for that module. The level must be specified by using one of the following key words, from the most detailed logging of messages (TRACE) to the least level of detail (DISABLED). You must use all capital letters when specifying the level keyword: TRACE, DEBUG, INFO, WARN, ERROR, FATAL and DISABLED.

EXAMPLES

You use the **addebug** command to start and stop detailed Centrify-specific logging to help you trace and resolve problems. To display the current status of logging, type:

```
/usr/share/centrifydc/bin/addebug
```

Note You must type the full path to the command because **addebug** is not included in the path by default. This command displays information similar to the following:

```
       Centrify DirectControl debug logging is off
```

To turn on logging, type:

```
/usr/share/centrifydc/bin/addebug on
```

This command records information in the centrifydc.log file or journal file similar to the following:

```
Dec 14 00:31:59 jon adjoin[11198]: com.centrify.join: Joining  domain
       garfield.com

Dec 14 00:31:59 jon adjoin[11198]: com.centrify.base: Getting the KDC
       List for garfield.com

Dec 14 00:31:59 jon adjoin[11198]: com.centrify.base: Updating config
       file with domain garfield.com

Dec  14  00:31:59  jon adjoin[11198]: com.centrify.join: Created user
       LDAP connection

Dec 14  00:31:59  jon  adjoin[11198]:  com.centrify.daemon.ADBinding:
       Destroying binding to ’garfield.com’

Dec  14  00:31:59  jon  adjoin[11198]: com.centrify.daemon.ADBinding:
       Attempting connection to server

Dec 14  00:31:59  jon  adjoin[11198]:  com.centrify.daemon.ADBinding:
       Connecting to odie.garfield.com:389

Dec  14  00:31:59  jon  adjoin[11198]: com.centrify.daemon.ADBinding:
       Connected
```

To discontinue logging, type:

```
addebug off
```

AUTHOR

Centrify Corporation

SEE ALSO

For related information, see the following command reference sections: adjoin(1), adleave(1), adgpupdate(1), adpasswd(1), adinfo(1), adobfuscate(1)

NAME

addns − update DNS records on an Active Directory−based DNS server.

SYNOPSIS

addns --update|--add [--nocreds] [--machine] [--user *username*] [--password *user_password*] [--server *servername*] [--domain *domainname*] [--name *hostname*] [--ignoreptrerr] [--ipaddr *ipaddress*] [--interface *interfacename*] [--force] [--refresh] [--ttl *value*][--version] [--verbose] [--secure]

addns --delete [nocreds] [--machine] [--user *username*] [--password *user_password*] [--server *servername*] [--domain *domainname*] [--name *hostname*] [--force] [--version] [--verbose]

addns --list [--server *servername*] [--domain *domainname*] [--name *hostname*] [--ipaddr *ipaddress*] [--interface *interfacename*]

DESCRIPTION

The **addns** command enables you to dynamically update DNS records on an Active Directory−based DNS server in environments where the DHCP server cannot update DNS records automatically. For example, if you are using an Active Directory−based DNS server configured for secure updates with a router acting as a DHCP server, the router cannot automatically register its DHCP clients with the DNS server because it has no way of establishing a security context that will allow the update. By running the **addns** command, you can use Kerberos credentials to establish a security context for updating the DNS records in the Active Directory−based DNS server.

With the addns command, you can:

- Create or update a local host’s IP addresses in DNS.

- Create or update a specified host’s IP addresses in DNS.

- Update pointer records in DNS.

- Remove the local or another host’s DNS records.

- Remove the local or another host’s IP addresses in DNS.

- List details about a DNS record.

Note In most cases, you do not need to use this command if a host’s IP address is managed by a Windows−based DNS server and the host obtains its IP address from a Windows−based DHCP server because the DHCP server updates the DNS record for the host automatically. If you are not using a Windows−based DNS server, you should use nsupdate or a similar command appropriate to the operating environment of the DNS server to update DNS records.

OPTIONS

You can use the following options with this command:

-U, --update
Create or update the IP address (A) and domain name pointer (PTR) records in the DNS server for the local or specified computer hostname.

-D, --delete
Remove the DNS records for the local or specified computer

hostname. Note that this option does not accept the −i (IP address) argument or the −e (interface name) argument.

−A −−add
Create new IP address (A) and domain name pointer (PTR) records in the DNS server for the local or specified computer hostname, even if a record already exists for the same hostname. If you update a host’s IP addresses by specifying the **−−update** option, current records are deleted when the new record is created. The **−−add** option allows you to add a record with one or more additional IP addresses without deleting current records.

If you a specify a hostname and IP address that are identical to an existing entry, **addns** returns an error.

−L, −−list
List DNS record details. If no additional parameters are specified, this option displays details about the DNS record for the computer on which you execute the command. You can use additional parameters to specify a particular domain (−d), server (−s), host (−n), or IP address (−i). You can use these parameters in combination, for example, the following specifies a specific host and the IP address for a different computer:

```
addns −L −n rhe5.acme.com −i 192.168.161.128
```

−N, −−nocreds
Do not require or prompt for credentials. This option only works if the DNS server is configured for non−secured updates.

−m, −−machine
Use the local computer account’s Active Directory credentials to establish a security context with the DNS server.

−u, −−user username[@domain]
Specify an Active Directory username with sufficient rights to add, update, and delete records in the relevant DNS zones.

You must use the username@domain format to specify the user account if the username is not a member of the joined domain.

If you do not specify the −−user option, the credentials for the currently logged−on user are used by default. If there are no Kerberos credentials for the current user and you are not using the computer account credentials, the Administrator user account is used to establish the security context.

−p, −−password userpassword
Specify the password for the Active Directory user account performing the add, update, or delete operation. If you do not provide the password at the command line, you are prompted to enter the password before the command executes. Specifying a password at the command line represents a security risk because the password can be retrieved while the command is running or from command history after the command has completed its execution.

For better security, you should do one of the following instead of specifying the password in the command line:

− Allow the addns command to prompt for the password.

− Use kinit to establish a valid credential cache before running the addns command.

− Use the −−machine option to use the computer account credentials to establish the security context.

−s, −−server servername
Specify the DNS server to send the DNS update records to. You can use this option more than once to specify backup DNS servers if the first one fails. If you do not specify this option, the addns program attempts to discover the DNS servers available on its own.

−d, −−domain domainname
Specify the fully qualified domain name of the DNS domain name to be updated. If you do not specify this option, the DNS domain name for the local host is used.

−n, −−name hostname
Specify the name of the host to update IP records for. If you do not specify this option, the local host name is used. This option cannot be used if the −e option is specified.

−I, −−ignoreptrerr
Continue to update the host record even if there is an error as the result of a reverse pointer (PTR) record having been deleted.

−i, −−ipaddr ipaddress
Specify one or more IP addresses to use in the update. You can specify this option multiple times to support multi−homed hosts. If no IP addresses are provided, the addns program attempts to determine the current settings.

−e, −−interface interfacename
Specify one or more local network interface names to use in the update. You can specify this option multiple times to support multi−homed hosts. If −i options specified along with −e options, the effect is aggregated. This option is for local host only. This option cannot be used if the −n option is specified.

−f, −−force
Update DNS records even if they have not changed.

−r, −−refresh
Update unchanged records to reset time−to−live (TTL) to its starting value.

−t, −−ttl value
Specify a TTL value (in seconds) for DNS records.

−V, −−verbose
Display detailed information about the operation being performed.

−v, −−version
Display version information for the installed software.

−S, −−secure
Perform a secured update of DNS records without first attempting a non−secured update. This option is typically used with DNS servers that are configured only for secured updates. This option works only with the −U, −−update option.

EXAMPLES

If secure updates are required and the current user executing the **addns** program has valid Kerberos credentials in the cache, you only need to specify the operation to perform and the addns program will attempt to determine the rest of the parameters programmatically. For example, to perform an update for the local host:

```
addns −−update
```

If there are no valid cached credentials or the current user credentials do not have sufficient permissions to perform the update, you can specify a user name and password to use for the establishment of the security context. For example:

```
addns −−update −−user "rae@arcade.com"
```

To update the IP address with a interface name for the local host such as eth0, you would type a command similar to this:

```
addns −−update −e eth0
```

To update the IP addresses for a computer other than the local host, you can specify the host name on the command line. For example, to update the IP addresses in the DNS records for the computer picasso on the DNS server fire.arcade.com using the user rae to establish the security context, you would type a command similar to this:

```
addns −−update −−user "rae" −−server "fire.arcade.com" −−domain
"arcade.com" −−name "picasso" −−ipaddr "172.128.1.25" −−ipaddr
"172.128.1.26"
```

To remove the DNS record for a local host using the local computer’s account credentials to establish the security context, you would type a command similar to this:

```
addns −−delete −−machine
```

Note To use the −−machine option, you must invoke the addns command as the root user and the account principal in Active Directory must have sufficient rights to modify records in the relevant DNS zones. Using the computer account credentials is particularly useful when an automated script, such as /sbin/dhclient−script, is used to keep the DNS records up to date.

AUTHOR

Centrify Corporation

SEE ALSO

For related information, see the following command reference sections: adjoin(1), adpasswd(1), adupdate(1), adinfo(1), addebug(1)

NAME

adedit − manage Active Directory and DirectControl in one or more domains.

SYNOPSIS

adedit [*script* **[***scriptarg***]...]**

DESCRIPTION

Executing adedit without arguments enters adedit interactive mode where you can enter adedit commands one at a time. Enter "quit" or "exit" to exit adedit. To execute an adedit or Tcl script, follow adedit with a path to the script. If the script takes arguments, add them after the path to the script.

The typical logic flow for using adedit is:

Use the bind command to bind adedit to one or more domains.

Use a select_**xxx** command to retrieve an object of type **xxx** from Active Directory (select_zone, for example, to retrieve a zone object) and store it in memory. Or use a new_**xxx** command to create a new object in memory and select that object.

Use a get_**xxx**_field command to read a selected object’s field (attribute) or a set_**xxx**_field to write a new value to a selected object’s field.

Use a save_**xxx** command to save a selected object from memory back to Active Directory if the object has been modified or is a new object. Without saving, no work on an object in adedit will have an effect.

For information about the many adedit commands, use the "help" command within adedit.

ARGUMENTS

[script]
The path to an adedit or Tcl script to execute. Optional.

[scriptarg]...
One or more arguments that may be required by the script. Optional.

AUTHOR

Centrify Corporation

SEE ALSO

For more information, consult the ADEdit Programmer’s Guide. You may also enter "help" after executing adedit for information about specific adedit commands.

NAME

adfinddomain − display information about the Active Directory domain controller

SYNOPSIS

adfinddomain [−−format name|ldap|ip] [−−port] [−−writable] [−−verify] [−−version] *[domain|$]*

DESCRIPTION

The **adfinddomain** command displays the domain controller associated with the Active Directory *domain* you specify. If you don’t specify a domain, the command returns information for the domain the local computer is joined to. If you specify a dollar sign ($) instead of a domain, the command returns the host name and, optionally, the port number of the Global Catalog server.

OPTIONS

You can use the following options with this command:

−f, −−format name|ldap|ip
The *−−format* option specifies the format of information for the Active Directory domain controller. For example, if you set the format to **name** , the command displays the host name of the domain controller. Similarly, you can specify the format to be the format used for LDAP requests or to be the IP address of the domain controller.

−p, −−port
The *−−port* option displays the port number in the output.

−w, −−writable
The *−−writable* option insures that the command finds a writable domain controller.

−V, −−verify
The *−−verify* option checks whether the domain controller is currently operational.

−v, −−version
The *−−version* option displays version information for the installed software.

EXAMPLES

You can use the **adfinddomain** command to display the host name, LDAP URL, or IP address of the domain controller for a specified domain. For example, to display the full host name for the domain controller in the arcade.org domain, you would type:

```
adfinddomain −−format name arcade.org fire.arcade.org
```

AUTHOR

Centrify Corporation

NAME

adfixid − change the ownership of a local user’s files to match the user and group IDs defined for the user in Active Directory.

SYNOPSIS

adfixid [−−commit] [−−commit−all] [−−report *filename*] [−−usermap *filename*] [−−groupmap *filename*] [−−id *id_range*] [−−xdev] [−−follow] [−−nfs] [−−undo] [−−restart] [−−version] [−−verbose] *directory*

DESCRIPTION

The **adfixid** command compares the local password database, for example, the local /etc/passwd and /etc/group files, to the UNIX profile entries for the DirectControl zone that are retrieved from Active Directory.

The command generates a report of the local users and groups that have UIDs or GIDs that conflict with the information stored in Active Directory, in the following cases:

− A local user or group has the same local name and Active Directory name, but a different UID or GID; for example, the user gsmith has UID and GID 1006 locally, but 1007 in Active Directory.

− A local user or group and an Active Directory user or group with different names have the same UID or GID. For example, local user joe has UID and GID 1009 and Active Directory user jcool also has UID and GID 1009.

After identifying conflicts, you can run **adfixid −−commit** to change the ownership of local users files and directories to match the user and group ID values defined in Active Directory for the zone, eliminating UID and GID conflicts.

If you have mapped a local account to an Active Directory account with a different name, **adfixid** will add the local name to the report and suggest changing the UID, even though the UID is correct because the two names apply to the same user. For example, if you have mapped local user joe to Active Directory user jcool, **adfixid** will suggest changing joe’s UID (1009) to something like 51009 so it does not conflict with jcool’s UID.

To accommodate this situation, you can use a mapping file to specify how the user and group names in the local database map to the user and group names in the UNIX profiles for the current zone. You can then run **adfixid −−usermap** or **−−groupmap** to check for UID or GID conflicts and change file ownership while ignoring conflicts for local users or groups who are mapped to Active Directory users or groups with different names. For example, if your map file identifies the mapping between joe and jcool, joe will not appear on the conflict report. See the **−−usermap** option and the examples for more information.

By default, running the **adfixid** command simply lists the local users and groups that have UID or GID conflicts and require file ownership changes. If you run this command with the **−−commit** option, **adfixid** searches local file systems files owned by users defined in the /etc/passwd file, and changes the ownership and group information to match the information defined for the zone. If you run this command with the **−−commit−all** option, **adfixid** also updates the /etc/passwd and /etc/group files to contain the new ID values.

The local computer must be joined to an Active Directory domain and in a valid zone to perform most operations. This requirement is not necessary to generate a report with the **--report** option or to undo a previous operation with the **--undo** option. In addition, to run **adfixid** with the **--commit, --commit-all,** or **--undo** options, you must be logged in as root.

OPTIONS

You can use the following options with this command:

-c, --commit

The **--commit** option commits file ownership UID and GID changes to the file system. If you do not specify this option, by default, **adfixid** only displays a list of the users and groups that require ownership changes.

-C, --commit-all

On most platforms, the **--commit-all** option commits the file ownership changes to the file system and updates the local /etc/passwd and /etc/group files. This option does not update the /etc/passwd and /etc/group files on Mac OS X computers.

-u, --usermap filename

The **--usermap** option enables you to specify a *filename* of a file that shows any mapping between local UNIX user names and zone UNIX user names. This option is useful when user names have been rationalized in the zone but may not match the names in the local database file. The format of the user mapping file is: *local_UNIX_name zone_UNIX_name*

When you run **adfixid** with this option, it ignores conflicts for local users who are mapped to Active Directory users with different names.

You do not need to add entries for local UNIX user names that match a zone user name. If a local UNIX user name does not match any zone user names, the name is ignored. If the UID for the ignored name conflicts with a zone user UID, the UID of the local user will be changed to a value in the UID range set aside for conflict-resolution.

For information about setting the value range for conflict resolution, see the **--id** option.

-g, --groupmap filename

The **--groupmap** option enables you to specify a *filename* of a file that shows the mapping between local UNIX group names and zone group names. This option is useful when group names have been rationalized in the zone but may not match the names in the local database file. The format of the group mapping file is:

local_UNIX_group zone_UNIX_group

When you run **adfixid** with this option, it ignores conflicts for local groups that are mapped to Active Directory groups with different names.

You do not need to add entries for local UNIX group names that already match a zone group name. If a name does not match any zone group names, the name is ignored. If the GID for the ignored name conflicts with a zone group GID, the GID of the local UNIX group is changed to a value in the GID range set aside for conflict-resolution.

For information about setting the value range for conflict resolution, see the **--id** option.

-r, --report filename

The **--report** option generates an audit log of every chown command that was executed by the **adfixid** command and puts it in the file specified by *filename.* When you specify the **--report** option, the *filename* parameter is required, though you can use a hyphen (-) as the *filename* to output to standard out. You can generate the report at the same time as the commit operation, or at a later time.

Note This option is only valid at the same time you perform a **--commit** or **--commit-all** operation or after you have performed one of those operations. You cannot use this option to generate a preview report of changes that a **--commit** operation would perform. Use the **adfixid** command with no command line options to review conflicts prior to making file system changes.

-i, --id id_range

The **--id** option enables you to specify a range of values for assigning new UIDs or GIDs to use to resolve UID or GID conflicts. The *id_range* parameter can be of the form <start_value>-<end_value> to specify the start and end values of the range. For example:

```
--id 90000-110000
```

The default range is 50000-60000. If you specify a single number, that value becomes the starting value for the range and the end value is MAXUID. If a local UNIX UID or GID conflicts with a zone UID or GID, the local value is mapped to a value in the specified range. For example, if a local UNIX user has a UID of 126 that conflicts with a zone user UID, the local UNIX user UID would be mapped to UID 50126 by default. If the target UID value of 50126 is already used in the zone, the next sequential value, 50127, is used instead.

-x, --xdev

The **--xdev** option enables you to prevent the **adfixid** command from running across file system mount points. By default, the **adfixid** command will traverse all local, non-NFS, file system mount points.

-n, --nfs

The **--nfs** option enables **adfixid** to traverse NFS directories. The **adfixid** command does not process NFS directories unless you specify this option.

-f, --follow

The **--follow** option can be used to specify that you want the **adfixid** command to follow symbolic links to update the target files and directories. By default, the **adfixid** command only updates the link file itself, if necessary, and it does not traverse into symbolically-linked directories.

-R, --restart

The **--restart** option ignores the results of a previous run. By default, the **adfixid** command skips files that were changed by a previous run of the command. Using this option resets the **adfixid** audit log so that **adfixid** is not aware of what files were previously changed.

If you have previously run adfixid and made changes the file owner but did not resolve conflicts between the /etc/passwd and /etc/group files and Active Directory, using this option ignores the changes previously made and makes them again when the conflicts between the local files and Active Directory are detected.

−U, −−undo

The **−−undo** option reverses the action of a previous **−−commit** operation. All files that had the owner and/or group id changed are set back to their original values. If the /etc/passwd or /etc/group files were updated using a **−−commit−all** operation, this change is also reversed.

−v, −−version

This option displays version information for the installed software.

−V, −−verbose

This option displays the file and directory names as they are processed. This option is useful when running this command on a large file system, such as the root file system, so you can track its progress.

If you specify this option, the **adfixid** command:

- Lists every file it examines.

- Reports every change of ownership performed for the files and directories examined.

- Lists any files or directories being skipped.

Without this option, the **adfixid** command does not display its progress and may appear to stop running when it is processing a large number of files and directories on large file systems.

directory

Specifies the directory or directories in which to start the search for the user files to be changed. By default, **adfixid** only searches the local file systems. You can, however, specify a network file system on the command line.

You can use this parameter to change the file ownership for selected directories or if you want to change the file ownership in stages. For example, you may want to change the ownership for a limited number of directories before committing changes across the whole file system on a given computer.

If you specify a network file system, such as an NFS or CIFS mount point, you should be sure that you do not run the command remotely on the same files from different computers. Running this command remotely from more than one computer may cause the file ownership changes to be overwritten with incorrect information.

Note File ownership changes are logged in the audit file on a per−machine basis. If you run this command for a network file system, the change is recorded in the audit file on the local computer. If you run the command again from a second computer, that computer has no record that the file ownership has been

previously changed.

EXAMPLES

To understand how to use the **adfixid** command, assume the local UNIX users defined in the local password database (/etc/passwd) are as follows:

```
ballen:x:1007:1007:Bob Allen:/home/ballen:/bin/csh
joe:x:1009:1009:Joe Cool:/home/jcool:/bin/bash
kane:x:1226:1226:Kane Lewis:/home/kane:/bin/bash
jfrank:x:1345:1345:John Frank:/home/jfrank:/bin/bash
```

The UNIX user profiles defined for the zone are:

```
gsmith:x:1007:10000:George Smith:/home/gsmith:/bin/bash
ballen:x:1006:10000:Bob Allen:/home/ballen:/bin/csh
jcool:x:1009:1009:Joe Cool:/home/jcool:/bin/bash
klewis:x:10226:10226:Kane Lewis:/home/klewis:/bin/bash
tyoung:x:1345:1345:Ted Young:/home/tyoung:/bin/bash
```

To simply see a list of the local users and groups with UID or GID conflicts requiring resolution, you can run the following command:

```
adfixid
```

This generates a report similar to the following:

```
4 user−id conflicts were found.
Local UID   Zone UID    User
−−−−−−−−−   −−−−−−−−    −−−−−−−−
1006        1007        gsmith
1007        1006        ballen
1009        51009       joe
1345        51345       jfrank

2 group−id conflicts were found.
Local GID   Zone GID    Name
−−−−−−−−−   −−−−−−−−    −−−−−−−−
1006        10000       gsmith
1007        10000       ballen
```

If you want to make the file ownership changes and resolve user and group conflicts, you can run the following command:

```
adfixid −−commit
```

- The file ownership for the local user "gsmith" will be changed from UID and GID 1006 to UID and GID 1007.

- The file ownership for the local user "ballen" will be changed from UID and GID 1007 to UID and GID 1006.

- The local user "joe" appears as a UID conflict because the local UNIX user name is different from the zone user name. Similarly, the local user "kane" is be ignored because there is no mapping between the local UNIX user name and the zone user name. For these users, you would need to create and specify a user mapping file.

- The local user "jfrank" is not defined in the zone, but his local UID and GID conflicts with the user "tyoung" who has a profile defined in this zone. The adfixid command will assign a UID and GID from the temporary range, for example 51345, and change the ownership (chown) of all of files owned by the local user "jfrank" to that UID.

To create a user mapping file, use a text editor and add an entry to map the local UNIX user account "joe" to the "jcool" zone UNIX user. For example:

```
vi defaultzone_usermap
```

Add an entry to map the local users to zone users, as needed. For example:

```
joe  jcool
kane klewis
```

You can then run the
adfixid
command and specify the user mapping file. For example:

```
adfixid --usermap defaultzone_usermap --commit
```

This command will change the file ownership for the files owned by the local user "kane" to UID and GID 10226. The command will not change the files owned by the local user "joe" because once mapped there is no UID or GID conflict between the local UNIX user and the zone UNIX user.

You can use the --commit and --report options together to generate a report of the changes performed during any --commit or --commit-all operation. For example:

```
adfixid --commit --report chown_rpt1
```

AUTHOR

Centrify Corporation

SEE ALSO

For related information, see the following command reference sections: adjoin(1), adpasswd(1), adgpupdate(1), adinfo(1), addebug(1)

NAME

adflush - clear the cache on a local computer.

SYNOPSIS

adflush [--auth] [--bindings] [--dns] [--expire] [--force] [--intended] [--objects] [--trusts] [--connectors] [--health] [--verbose] [--version]

DESCRIPTION

You can use the **adflush** command to clear cached information on a local computer.

Executing **adflush** with no options expires the objects in the local domain controller (dc.cache) and global catalog (gc.cache) caches. You can selectively clear cached authorization information and DNS queries using the --auth and --dns options. If you want to clear all cached information, including objects, authorization information, and DNS queries, you can use the --force option. In most cases, you should only use the --force option when the agent is running and connected to Active Directory.

If the agent is not connected to Active Directory, clearing the cache prevents all Active Directory users from logging on until the connection to Active Directory is restored. If you want to clear all cached information while the agent is disconnected, you must use the **--intended** option with the **--force** option to confirm this is your intended operation.

Executing **adflush** with the default option also restarts the nscd daemon (pwgrd for HPUX). On Mac OS X computers, the command also flushes the system cache.

OPTIONS

You can use the following options with this command:

-a, --auth
The **--auth** option removes information from the authorization store cache.

-b, --bindings
The **--bindings** option forces adclient to refresh its connections to domain controllers in the trusted domains in order to find more efficient ones or potentially to redistribute the connection load per server.

-d, --dns
The **--dns** option removes stored DNS information from the adclient local cache.

-e, --expire
The **--expire** option expires information for the domain controller and global catalog objects.

-f, --force
The **--force** option clears all cached information even if the **adclient** process is currently disconnected from Active Directory. You should only use this option if you want to completely remove all cached information immediately on a local computer.

-y, --intended
The **--intended** option can be use with the **--force** option to remove all cached information from a local computer when the

agent is disconnected from Active Directory. Before using this option, you should note that all Active Directory users will be prevented from logging on until the connection from the agent to Active Directory is restored.

-o, --objects
The **--objects** option removes only domain controller and global catalog objects from the cache.

-t, --trusts
The **--trusts** option refreshes and replaces trusted domain information by updating the **/etc/krb5.conf** file.

-c, --connectors
The **--connectors** option flushes the Centrify Connector information for the local computer.

-H, --health
The **--health** option removes system health history for the local computer.

-V, --verbose
The **--verbose** option displays detailed information about the operation performed.

-v, --version
The **--version** option displays version information for the installed software.

EXAMPLES

To expire objects in the local cache when the adclient process can connect to Active Directory, run the following command:

```
adflush
```

To display verbose output and clear the local cache when the adclient process is running in disconnected mode without access to Active Directory, run the following command:

```
adflush --verbose --force
```

AUTHOR

Centrify Corporation

NAME

adgpresult - display group policy settings that are in effect.

SYNOPSIS

adgpresult [--all] [--machine] [--user *user_name*]

DESCRIPTION

The **adgpresult** command enables you to report the group policy settings that are in effect for the local computer, the current user, or a specified user. If you have configured and applied a Group Policy Object to a site, domain, or organizational unit that includes a Centrify-managed computer, you can use the **adgpresult** command to see the computer and user configuration policies that have been applied. The command displays a Resultant Set of Policies similar to the Microsoft Windows gpresult program.

OPTIONS

You can use the following options with this command:

-a, --all
The **--all** option displays both the computer and user group policy settings that are in effect for the local computer and the current user account.

-m, --machine
The **--machine** option displays only the computer group policy settings that are currently in effect on the local computer.

-u, --user
user_name The **--user** option displays only the user group policy settings that are in effect for the currently logged on user or for the user specified by the *user_name* argument.

EXAMPLES

To display both computer and user group policy settings for the local computer and current user, type the following command:

```
adgpresult
```

To report only the computer configuration policies and save the results to a file, you could type a command similar this:

```
adgpresult --machine > /tmp/unix-rsop-rhel6
```

The command produces output similar to the following sample:

```
Machine's group policy settings:
-----------------------------------------------------------------
Name: nico-sf$
Last update: Wed Jun 04 14:02:03 2014
Next update: Wed Jun 04 15:53:03 2014
Deny RSoP: No
Loopback Mode: Not Configured

Resultant Set of Policy
====================
secedit/kerberos policy:
    Default Domain Policy:
        MaxClockSkew = 5,
        MaxRenewAge = 7,
        MaxServiceAge = 600,
        MaxTicketAge = 10,
        TicketValidateClient = 1,
  secedit/system access:
      Default Domain Policy:
          ClearTextPassword = 0,
          ForceLogoffWhenHourExpire = 0,
          LSAAnonymousNameLookup = 0,
          LockoutBadCount = 0,
          MaximumPasswordAge = 42,
          MinimumPasswordAge = 1,
          MinimumPasswordLength = 7,
          PasswordComplexity = 1,
          PasswordHistorySize = 24,
          RequireLogonToChangePassword = 0,

  secedit/unicode:
      Pistolas-Centrify Policies:
          Unicode = yes,

  secedit/version:
      Pistolas-Centrify Policies:
          Revision = 1,
          signature = "$CHICAGO$",

  software/policies/centrify/audittrail:
      Default Domain Policy:
          AuditTrailTargets = 0000000003,

  software/policies/centrify/centrifydc/settings/passwordprompt:
      Pistolas-Centrify Policies:
          pam.password.change.required.mesg = Change your password to
continue:,
          pam.password.confirm.mesg = Confirm your new password:,
          pam.password.expiry.warn.mesg = Your password expires in %d
days.,
          pam.password.new.mesg = Type your new password:,
          pam.password.old.mesg = Type your current password:,
      UNIX Policies:
          pam.password.enter.mesg = Type your Active Directory  pass-
word:,

  software/policies/centrify/directaudit/agent:
      Default Domain Policy: N/A

  software/policies/centrify/directaudit/common:
      UNIX Policies:
          InstallationGuid                                          =
b8dc1c79-f5f9-4882-9460-ebaec7ddc020@pistolas.org,
```

AUTHOR

Centrify Corporation

NAME

adgpupdate - retrieve and apply group policy from the Active Directory domain.

SYNOPSIS

adgpupdate [--target [Computer|User]] [--version]

DESCRIPTION

The **adgpupdate** command retrieves group policies from the Active Directory domain controller and applies the policy settings to the local computer and current user immediately. Normally, group policies are updated automatically every 90 to 120 minutes. If you want a policy change to take effect immediately, however, you can force the group policy update by running the **adgpupdate** command. Upon updating the group policy, the **adgpupdate** command then resets the timer for the next automatic update to occur in the next 90 to 120 minutes.

Note Automatic group policy updates occur at a random interval between 90 and 120 minutes to prevent multiple computers from connecting to and requesting updates from the Active Directory domain controllers at the same time. However, both the default interval of 90 minutes and the default offset period of 30 minutes can be configured to other values using group policy settings. Therefore, the automatic group policy update may occur more or less frequently in your environment. For information about setting computer and user group policies, see the Centrify DirectControl Administrator’s Guide or Active Directory documentation.

By default, the **adgpupdate** command updates both the computer-based group policies and the user-based group policies for the user who is currently logged in and running the **adgpupdate** command. With a command line setting, you can restrict the group policies updated to be only computer group policies or only the current user’s group policies, if needed.

OPTIONS

You can use the following options with this command:

-T, --target [Computer|User]
Restricts the group policy update to either Computer group policy or User group policy.

-V, --verbose
Displays information about each step in the group policy update process as it occurs. This option is useful for troubleshooting purposes.

-v, --version
Displays version information for the installed software.

EXAMPLES

In most cases, you use the **adgpupdate** command to update both the computer-based group policies and the user-based group policies after changes have been made or when new policies are set. To update both the computer and user group policies on the local computer for the current user account, you can type:

```
adgpupdate
```

The command then displays update status similar to the following:

```
Refreshing Computer Policy...
Computer Policy Refresh has completed.
Refreshing User Policy...
User Policy Refresh has completed.
```

If you only want to update computer group policy on the local computer, you can type a command similar to the following:

```
adgpupdate −−target Computer
```

Note To update user policies on a computer, you must be logged on as a valid Active Directory user. If you are not logged on as a valid Active Directory user, running **adgpupdate** will refresh the computer−based group policies but no user−based group policies will be updated.

AUTHOR

Centrify Corporation

SEE ALSO

For related information, see the following command reference sections: adjoin(1), adleave(1), adpasswd(1), adinfo(1), addebug(1)

NAME

adid − display the real and effective UIDs and GIDs for the current user or a specified user.

SYNOPSIS

adid [−a] [−−user] [−−name] [*user_name* | *uid*]

DESCRIPTION

The **adid** command is intended as a replacement for the standard id program to look up user and group information for a specified user. For Active Directory users, the adid command is more efficient than the standard id program because it can request the user’s group membership list directly through the Centrify DirectControl Agent, resulting in better performance. For the standard id program, requesting a user’s group membership requires the program to search through all the groups on the system to find which groups include the user as a member. If you run the adid command and specify a user who is not an Active Directory user, the adid command transfers the request to the local id program with the same arguments you have specified.

OPTIONS

You can use the following options with this command:

−a Display all of the group IDs for the specified user or the current user if no user is specified.

Note This option is provided to support compatibility with other versions of the program. The information **adid** displays with this option is the same as the information displayed without this option.

−n, −−name
Display only the effective user name for the specified user or the current user. You must include the **−−user** (or **−u**) option on the command line to use this option.

−u, −−user
Display only the effective user ID for the user.

EXAMPLES

You can use the **adid** command to display user and group information for the current user or any specified user. For example, to display the user name, default group, and complete group membership for the current user, you can type: adid −a uid=505(alan) gid=100(users) groups=100(users),700(oracle),507(testexpert)

To display the user ID and group ID for a specific user name, you can type: adid alan uid=505(alan) gid=100(users)

To display only the user ID for a specific user name, you can type: adid −−user sloane 506

AUTHOR

Centrify Corporation

NAME

adinfo − display detailed information about the Active Directory configuration for the local computer.

SYNOPSIS

adinfo [--domain] [--gc] [--zone] [--zonedn] [--site] [--server] [--name] [--all] [--support] [--begin *timestamp*] [--end *timestamp*] [--lastnhrs *n*][--output *filename*] [--paths *paths]* [--debugcache] [--diag *[domain]]* [--config] [--mode] [--joinedcount] [--sysinfo all|[dns]|[domain]|[netstate]| [adagent]|[config]|[health]|[cip]|[zone]] [--test] [--verbose] [--version] [--product-version] [--auth [*domain*]] [--ntlmauth [*domain*]][--servername *domain_controller*]] [--computer] [--user *username[@domain]]* [--password *userpassword]* [--interactive] [--fips] [--cipinfo]

DESCRIPTION

The **adinfo** command displays detailed information about the Active Directory configuration for the local computer. If you do not specify an option, **adinfo** returns the basic set of configuration details for the local computer, which is equivalent to specifying **adinfo --all.**

Note The last line returned by **adinfo** on Mac OS X and Linux machines shows **Licensed Features: Enabled | Disabled** to indicate whether the licensed or express version of the agent is running on the local computer. This information is only relevant to Mac OS X and Linux computers so it does not appear when you run **adinfo** on other platforms.

The --domain, --gc, --zone, --zonedn, --site, --server, and --name options are intended for use in scripts to return the current Active Directory domain, global catalog domain controller, zone, site, domain controller, and computer account name. The other options provide more detailed or operation-specific information.

You can use the --user and --password options in conjunction with the --all, --support, --diag, --auth or --ntlmauth option to specify the user name and password of an Active Directory account with permission to read the computer account information in the Active Directory domain controller you are accessing. If you run **adinfo** while logged in as root, however, you do not need to specify the --user or --password option because the command uses the Active Directory account associated with the local host.

Note To run the **adinfo** command with the **--support** or **--debugcache** options, you must be logged in as root. You are not required to log in as root for any of the other **adinfo** options.

OPTIONS

You can use the following options with this command:

-d, --domain

The **--domain** option returns the name of the local computer's Active Directory domain. If the computer isn't currently joined to an Active Directory domain, then the command exits and returns status 10.

-G --gc

The **--gc** option returns the name of the local computer's Active Directory domain controller used for global catalog operations. If the computer isn't currently joined to an Active Directory domain, then the command exits and returns status 10.

-z, --zone

The **--zone** option returns the name of the local computer's Active Directory zone or "Auto Zone" if a computer is joined to Auto Zone, and is not a member of any specific zone. If the computer isn't currently joined to an Active Directory domain, then the command exits and returns status 10.

-Z, --zonedn

Return the distinguished name (DN) of the local computer's Active Directory zone or the distinguished name (DN) of the computer's Active Directory domain if computer is joined to Auto Zone.

The distinguished name is the name that uniquely identifies an entry in the directory, beginning with the most specific attribute and continuing with progressively broader attributes.

If the computer isn't currently joined to an Active Directory domain, then the command exits and returns an exit status of 10.

-s, --site

The **--site** option returns the name of the local computer's Active Directory site. If the computer isn't currently joined to an Active Directory domain, then the command exits and returns status 10.

-r, --server

The **--server** option returns the name of the local computer's Active Directory domain controller. If the computer isn't currently joined to an Active Directory domain, then the command exits and returns status 10.

-n, --name

The **--name** option returns the name of the local computer's computer account name in Active Directory. If the computer isn't currently joined to an Active Directory domain, then the command exits and returns status 10.

-a, --all

The **--all** option returns the local host name, current Active Directory domain, Active Directory computer account name, local preferred site, Centrify zone, the date and time that the password was last reset for the computer's Active Directory computer account, and whether the computer is currently connected to Active Directory.

-t, --support

The **--support** option returns the information supplied by the --all option along with the contents of /etc/centrifydc/centrifydc.conf, /etc/krb5.conf, /var/log/centrifydc.log, the nscd configuration file, and a key list from /etc/krb5.keytab.

This option is typically used to send complete diagnostic information to a file, which can then be sent to Centrify Support for analysis.

Note You can use the **--paths** option to specify additional directories from which to collect and return information.

Note By default, the output for the command is written to the file /var/centrify/tmp/adinfo_support.txt. You can save the output in a different location or using a different file name by using the optional --output argument.

−o, −−output filename

Sends the support output generated by the **−−support** option to the specified file. By default, output for the command is written to the file /var/centrify/tmp/adinfo_support.txt. To send the output specified by the −−support option to stdout, use a hyphen (−) in the command line in place of the filename. You can also use redirection (>) or piping (|) to save the output to a different location or filename. **Note** Use the −−begin and −−end options or the −−lastnhrs option in conjunction with this option if your operating system uses the systemd journal for logging (for example, if the local computer runs Fedore 20).

−b, −−begin <timestamp>

Specify the timestamp at which you want to begin getting information from the log file. Use the following format to specify the timestamp: "yyyy−mm−dd hh:mm:ss" The **−−begin** and **−−end** options should be used in conjunction with the **−−support** option on computers that support the systemd journal for logging. For example, on computers with the Fedora core, version 20 (or later), you should use these options to get logged information. The default is to get the last 8 hours of the log file.

−e, −−end <timestamp>

Specify the timestamp at which you want to end getting information from the log file. use the following format to specify the timestamp: "yyyy−mm−dd hh:mm:ss" The **−−begin** and **−−end** options should be used in conjunction with the **−−support** option on computers that support the systemd journal for logging. For example, on computers with the Fedora core, version 20 (or later), you should use these options to get logged information. The default is to get the last 8 hours of the log file.

−l, −−lastnhrs <n>

Display the last <n> number of hours of logging activity. The value you specify must be a positive integer [1...999999]. The **−−lastnhrs option should be used in conjunction with the −−support** option on computers that support the systemd journal for logging. For example, on computers with the Fedora core, version 20 (or later), you should use these options to get logged information. The default is to get the last 8 hours of the log file.

−P, −−paths paths

Used with the −−support option to collect information from additional locations. By default, the −−support option collects the following information:

The current configuration parameters set in /etc/centrifydc/centrifydc.conf

The settings from /etc/krb5.conf

The contents of the log file /var/log/centrifydc.log

The key list from /etc/krb5.keytab

−D, −−debugcache

Collects cache and NIS map files for analysis and puts them in a compressed file, /var/centrify/tmp/adinfo_debugcache.tar.gz, that you can send to C entrify Support for analysis.

You must use the root account with this option.

−g, −−diag [domain]

The **−−diag** option takes a domain name as an optional argument. If the domain argument isn’t present, the option assumes the computer’s current domain as the specified domain. The ability to specify a domain is useful when an attempt to join the computer to an Active Directory domain fails. Specifying that domain here can help diagnose why the attempt failed. The **−−diag**
option returns detailed diagnostic information for the host computer, including the following:

Local host name.

Local IP address.

List of one or more DNS servers for the specified domain as supplied by the domain controller.

Host name or IP address of the DNS host computer as supplied by the specified domain controller.

Whether the specified domain controller has up−to−date global catalog data so that it can become the global catalog, if necessary.

Configuration state of the specified Active Directory domain.

Configuration state of the specified domain’s Active Directory forest.

Configuration state of the specified domain’s controller.

Name of the Active Directory forest to which the specified domain belongs.

Name under which this computer joined the Active Directory domain. This is the name of the computer account in Active Directory for this computer.

Whether the computer joined the domain with the trusted for delegation option or is configured to use DES encryption.

Kerberos key version for this computer. The version is stored both locally and in the computer’s Active Directory account, and is incremented when a service principal’s password key changes. If the local key differs from the Active Directory account key version, it indicates that the local key is no longer in sync with the Active Directory key and this may cause authentication to fail. If the computer isn’t joined to a domain, it has no local key and the value shown is local key version unavailable. If the computer is joined to a domain other than the specified domain, the Active Directory key is shown as <unavailable>.

Configuration properties that have been set for the agent.

List of Kerberos service principal names this computer has registered with Active Directory. If the computer isn’t joined to the specified domain, the list cannot be retrieved.

−c, −−config

The **−−config** option returns the parsed contents of the agent configuration file.

-m, --mode
The **--mode** option indicates whether the computer is currently connected to Active Directory or running in disconnected mode. If the adclient process is not running, the computer is considered disconnected (to reconnect, start adclient). This option returns connected when adclient is running and down when adclient is stopped.

Note The computer must be joined to the domain controller for the -m option to return the adclient state.

-j, --joinedcount
The **--joinedcount** option displays the number of computers joined to each zone.

-y, --sysinfo all |dns,domain,netstate,adagent,config,health,cip,zone
The **--sysinfo** option displays system information for the current domain. You can specify one or more options in a comma-separated list, or specify *all* to show all available information:

all Display all available system information. Specifying this option is the same as specifying all of the following options:

dns Display the address, state , and cache contents of the current DNS server.

domain Display the domain info map for the current domain.

netstate Display the state of the network.

adagent Display binding information and connection status for the agent.

config Display adclient in-memory configuration parameter values.

health Display system health status for the local host.

cip Display Centrify Identity Platform (CIP) and multi-factor authentication (MFA) status for the local host.

zone Display the distinguished name of the zone.

-T, --test
The **--test** option tests the availability of the ports the Centrify agent requires for authentication through Active Directory.

-V, --verbose
The **--verbose** option send detailed diagnostic information to standard error (stderr) output. You can use this option in combination with other options.

-v, --version
The **--version** option displays version information for the installed software.

-x, --product-version
The **--product-version** option displays the agent and Centrify Infrastructure Services version information for the installed software.

-u, --user username[@domain]
The **--user** option identifies an Active Directory user account with sufficient rights to read the computer account information.

You must use the *username@domain* format to specify the user account if the username is not a member of the computer's current domain. If you do not specify the **--user** option, the default is the Administrator user account.

-p, --password userpassword
The **--password** option specifies the password for the Active Directory user account. If you do not provide the password at the command line, you are prompted to enter the password before the command executes.

Note Specifying a password at the command line represents a security risk because the password can be retrieved while the command is running or from command history after the command has completed its execution.

-A,--auth [domain]
The **--auth** option authenticates the user name and password for the user specified with the --user option against the specified domain. If you don't specify a domain, the user is validated against the currently joined domain.

This option only validates that the specified user name and password can be authenticated by Active Directory. You cannot use this option in combination with other options to display other types of information.

-N,--ntlmauth [domain]
The **--ntlmauth** option authenticates the NTLM user name and password for the user specified with the --user option against the specified domain. If you don't specify a domain, the user is validated against the currently joined domain.

This option only validates that the specified NTLM user name and password can be authenticated by Active Directory. You cannot use this option in combination with other options to display other types of information.

-S, --servername domain_controller
The **--servername** option connects to a specific domain controller to perform network diagnostics. You can use this option in combination with any of the other options.

-C, --computer
The **--computer** option displays the service principal names (SPNs) associated with the computer account.

-I, --interactive
The **--interactive** option prompts for the user password if a cached Kerberos ticket has been revoked. In most cases, this option is used when the Kerberos credential cache used to authenticate a user to an Active Directory domain, and a read-only domain controller of the domain has revoked the user's Kerberos ticket. By providing a valid password, the user can be granted a new Kerberos ticket to replace the revoked ticket.

-f, --fips
The **--fips** option only displays whether FIPS-compliant encryption is enabled or disabled on the local computer.

−i, −−cipinfo
The **−−cipinfo** option displays the information of the currently connected CIP, including its URL and web proxy configuration.

EXAMPLES

To display complete configuration information for the local computer, type:

```
adinfo
```

If the computer has joined a domain, the command displays information similar to the following:

```
Local host name:   magnolia
Joined to domain:  ajax.org
Joined as:         magnolia.ajax.org
Pre−win2K name:    magnolia
Current DC:        ginger.ajax.org
Preferred site:    Default−First−Site−Name
Zone:              ajax.org/Program Data/Centrify/Zones/default
Last password set: 2014−12−21 11:37:22 PST
CentrifyDC mode:   connected
Licensed Features: Enabled
```

Note Whether licensed features are enabled or disabled is only relevant for Linux and Mac computers and is not shown for Solaris and other UNIX systems.

This command used in a shell script returns the host computer's current domain:

```
adinfo −−domain

ajax.org
```

To test whether a specific user can be authenticated by a specific Active Directory domain controller, you could type a command similar to the following:

```
adinfo −−auth −−user rae −−servername ginger.ajax.org
```

You are then prompted for the Active Directory password for the user rae account. If Active Directory can authenticate the user, a confirmation message similar to the following is displayed:

```
Password for user "rae" is correct
```

To test connectivity and the availability of required ports on the Active Directory domain controller, you could type a command similar to the following:

```
adinfo −−test
```

If the computer is joined to a domain and the connection to Active Directory succeeds, the command displays information similar to the following:

```
Domain Diagnostics:
  Domain: ajax.org
    DNS query for: _ldap._tcp.ajax.org
    DNS query for: _gc._tcp.ajax.org
  Testing Active Directory connectivity:
```

```
    Global Catalog: ginger.ajax.org
      gc:       3268/tcp − good
    Domain Controller: ginger.ajax.org
      ldap:      389/tcp − good
      ldap:      389/udp − good
      smb:       445/tcp − good
      kdc:        88/tcp − good
      kpasswd:   464/tcp − good
      ntp:       123/udp − good
```

AUTHOR

Centrify Corporation

SEE ALSO

For related information, see the following command reference sections: adjoin(1), adleave(1), adupdate(1), adpasswd(1), adquery(1), addebug(1), adobfuscate(1)

NAME

adjoin − join an Active Directory domain.

SYNOPSIS

adjoin [--user *username[@domain]]* [--password *userpassword]* [--noprompt] [--container *containerDN]* [--name *computername]* [--prewin2k *accountname]* [--force] [--forceDeleteObj] [--forceDeleteObjWithDupSpn] [--forceDeleteExistingComputerZone] [--alias *aliasname]* [--zone *zonename]* [--computerrole *rolename]* [--server *domaincontroller]* [--zoneserver *domaincontroller]* [--dnsname *DNSHostName]* [--gc *domaincontroller]* [--noconf] [--notime] [--upn *userPrincipalName]* [--trust] [--des] [--ldap] [--precreate] [--compat] [--selfserve] [--useConf *list*] [--attempt] [--verbose] [--workstation] [--extramap *mapName]* [--prestage *dir]* [--noinit] [--version] [--enableAppleIDGenScheme] [--licensetype server|workstation] [--createComputerZone] *domain*

DESCRIPTION

The **adjoin** command adds the local host computer to the specified Active Directory domain. The *domain* should be a fully-qualified domain name, for example, sales.acme.com.

If the computer is already a member of another domain, you must leave the old domain by running **adleave** to remove the computer account from the old domain. Once you have left the old domain, you can run **adjoin** to join the new domain.

To run **adjoin** you must be logged in as root.

By default, when you run **adjoin,** the program performs the following tasks:

- Locates the domain controller for specified domain and contacts Active Directory.

- Synchronizes the local computer's time with Active Directory to ensure the timestamp of Kerberos tickets are accepted for authentication.

- Checks whether a computer account already exists for the local computer in Active Directory. It creates a new Active Directory computer account for the local computer, if needed.

- Adds the computer account to the specified zone when the **--zone** option is specified, or to Auto Zone when the **--workstation** option is specified.

- Updates the Kerberos principal service names used by the host computer, generating new Kerberos configuration and keytab files and new service keys for the host and http services.

- Sets the password on the Active Directory computer account to a randomly-generated password. The password is encrypted and stored locally to ensure the Centrify agent alone has control of the account.

- Starts the Centrify UNIX agent (adclient).

OPTIONS

You can use the following options with this command:

-u, --user username[@domain]

The *username* identifies an Active Directory user account with

sufficient rights to add a computer to the specified domain and create new computer accounts. You must use the username@domain format to specify the user account if the username is not a member of the domain being joined. If you do not specify the **--user** option, the default is the "administrator" user account. When specifying *username@domain,* you cannot use an alternative UPN. You must use the domain defined for your account.

-p, --password userpassword

The *userpassword* specifies the password for the Active Directory user account performing the join operation. If you do not provide the password at the command line, you are prompted to enter the password before the command executes.

Note Specifying a password at the command line represents a security risk because the password can be retrieved while the command is running or from command history after the command has completed its execution.

-I, --noprompt

If no credentials found, adjoin will prompt for user credential to proceed. If this option is specified, adjoin will not prompt and just fails.

-c, --container containerDN

The *containerDN* specifies the distinguished name (DN) of the container or Organizational Unit in which to place this computer account.

You can specify the containerDN by:

- Canonical name (ajax.org/unix/services). You cannot specify a partial name for the canonical name.

- Fully distinguished name (cn=services, cn=unix,dc= ajax,dc=org)

- Relative distinguished name without the domain suffix(cn=services,cn=unix)

If you do not specify a container, the computer account is created in the domain's default Computers container. Note that the container you specify must already exist in Active Directory or the join operation will fail. In addition, you must have permission to add entries to the specified container.

-n, --name computername

The *computername* specifies the host name you want to use for this computer in Active Directory. If you do not specify a *computername* at the command line, the computer account name in Active Directory is the same as the local host name.

This option is most commonly used if you have a disjointed DNS namespace. For example, if the local UNIX host is a member of the DNS zone ajax.org, but is joining the Active Directory domain emea.ajax.org, you can use this option to join the domain with a computer name that is different from the name of the computer in DNS:

```
--name finserv.emea.ajax.org
```

This option can also be used in conjunction with the **--alias** option if the computer has multiple IP addresses and there are

DNS records for those addresses.

The maximum length for computer account names in Active Directory is 64 characters (the limit on AD common names). However, it is recommended that you limit names to 15 or fewer characters because this limit conforms to the maximum length allowed by the NetLogon service, which is the preferred service for **adclient** to use for NTLM pass-through authentication. NetLogon is fast and automatically returns a user’s group membership.

If you specify more than 15 characters, **adclient** uses LDAP methods to fetch the user’s group membership and create the computer account. Because LDAP methods are subject to the permissions on the Active Directory container for the computer account, you may need administrative permissions to execute this command when specifying a computer name longer than 15 characters.

-N, --prewin2k accountname
The *accountname* specifies the pre-Windows 2000 name for this computer in Active Directory. The pre-Windows 2000 name is the name stored in the samAccountName attribute.

The maximum length for the samAccountName attribute is 15 characters.

Note Although the actual limit is 19 characters, it is recommended that you limit the name to 15 characters because some Windows functions use this attribute as a NetBIOS name, which has a 15-character limit. If the name is larger than 15 characters, the Centrify agent must use less efficient NTLM authentication methods.

If you do not specify this option, the default pre-Windows 2000 name is the computer account name truncated at 15 characters. This option enables you to manually specify the pre-Windows 2000 name you want to use.

This option is most commonly used if the naming conventions for computer account names result in names that are longer than the 15 character limit.

-f, --force
This option overwrites the information stored in Active Directory for an existing computer account. This option allows you to replace the information for a computer previously joined to the domain. If there is already a computer account with the same name stored in Active Directory, you must use this option if you want to replace the stored information. You should only use this option when you know it is safe to force information from the local computer to overwrite existing information.

-F, --forceDeleteObj
This option will clean up the existing computer object and extension object in Active Directory, that is to clean up all data related to the current computer in Active Directory before joining the domain. You must use this option if you want to recreate the existing computer account. You should only use this option when you know it is safe to force overwrite the existing information.

-d, --forceDeleteObjWithDupSpn
This option will clean up the existing objects with duplicate SPN in Active Directory. You should only use this option when you know it is safe to force delete the existing information.

-O, --forceDeleteExistingComputerZone
This option will clean up the existing computer zone in Active Directory, that is to clean up all data related to the computer zone of current joined machine in Active Directory before joining the domain. You must use this option if you want to recreate the existing computer zone. You should only use this option when you know it is safe to force overwrite the existing information.

Note This option should be used in conjunction with --createComputerZone

-a, --alias computeralias
The *computeralias* specifies an alias name you want to use for this computer in Active Directory. This option creates a Kerberos service principal name for the alias and the computer may be referred to by this alias. This option would normally be used if a computer has more than one ethernet port and each port is known by a different DNS name. You can include more than one --alias option on the command line if you need to specify multiple aliases for a single computer.

-z, --zone zonename
The *zonename* specifies the name of the zone in which to place this computer account. You must specify this option or use the **--workstation** option to join a domain through Auto Zone. If you have installed a Centrify Express agent, you can only join a domain through Auto Zone. You cannot specify a zone for Centrify Express agents. Use the **--workstation** option if you have installed a Centrify Express agent.

If individual zone names are not unique across the Active Directory forest, you can use the canonical name of the zone to uniquely identify the zone you want to join. For example, if you have more than one "finance" zone, you can use the full canonical name of the zone to specify which "finance" zone to join.

Note If users and groups are unique across the forest and not required to be segregated into zones, you can join the Active Directory domain using the **--workstation** option to connect to Auto Zone instead of specifying a zone. The **--workstation** and **--zone** options are mutually exclusively and you must specify one or the other.

If you specify a name for zone that does not exist, the join operation fails.

-R, --computerrole rolename
The *rolename* specifies the computer role to which the computer is added when the computer joins the domain.

-s, --server domaincontroller
The *domaincontroller* specifies the name of the domain controller to which you prefer to connect. You can use this option to override the automatic selection of a domain controller based on the Active Directory site information.

-Z, --zoneserver domaincontroller
The *domaincontroller* specifies the name of the domain controller to use for zone operations. You can use this option, for example, if the zone is defined in a different domain than the one

you are joining.

−D, −−dnsname DNSHostName

The *DNSHostName* specifies the dNSHostName attribute in the computer object. You can use this option to override the automatic selection of a DNS server based on the information in the computer's configuration files.

−g, −−gc domaincontroller

The *domaincontroller* specifies the name of the domain controller to use for global catalog operations. You can use this option if the default domain controller, or that specified by the **−−server** option is not writable or does not support global catalog operations.

−C, −−noconf

This option indicates that you do not want to update the local system's PAM and NSS configuration. If you set this option, you will need to modify the PAM and NSS configuration files manually to work with the adclient daemon.

−U, −−upn userPrincipalName

Specify a user principal name (UPN) for the computer account in Active Directory.

−T, −−trust

Set the Trust for delegation option in Active Directory for the computer account. Trusting an account for delegation allows the account to perform operations on behalf of other accounts on the network.

Note Using this option requires running **adjoin** with an account with full administrator privileges. You can also set group policy to allow a non−administrator user to set this option. For more information, see the Administrator's Guide for Linux and UNIX.

When using this option, clear the local cache before joining the domain.

−k, −−des

Set the computer account to use the Data Encryption Standard (DES) for keys.

−l, −−ldap

Use LDAP methods to fetch the user's group membership and create the computer account. Because LDAP methods are subject to the permissions on the Active Directory container for the computer account, you may need administrative permissions to execute this command when specifying this option.

−P, −−precreate

Precreate a computer account in Active Directory without joining the domain. If you use this option, you must also specify the name of the computer account you want to precreate using the **−−name** option. In addition, you must specify either **−−zone** to provide the name of the zone in which to precreate the account, or **−−workstation** to specify Auto Zone instead of a specific zone.

The −−precreate option does the following:

Creates a computer object in Active Directory in the organizational unit you specify or the Computers container.

Resets the computer account password to computer's host name (in lower case).

Creates an Extension object in the zone.

The following permissions are granted to the computer object:

Read and Write operatingSystemServicePack, operatingSystem, and operatingVersion attributes in the Computer object.

Validate write to servicePrincipalName, dNSHostName attributes.

Reset computer's password.

Read userAccountControl attributes of the computer object.

By precreating the computer account and its serviceConnectionPoint, you can allow any user to join the computer to a domain without granting any special rights or performing any zone delegation. This option also enables you to create all the computer accounts you want in a batch job and automate how computers join the domain.

−m, −−compat

Create a computer object that is compatible with DirectControl 2.x and 3.x. By default, the computer object is not compatible with these older versions of Centrify software.

−S, −−selfserve

Uses the computer object's account credentials to join the domain.

To use this option, you must have already precreated the computer account in Active Directory by using the Pre−Create Computer wizard or **−−adjoin −P,** or previously joined a domain, then left by using the **adleave −−reset** option. For information about using the wizard to precreate a computer account, see the *Centrify DirectControl Administrator's Guide.*

If you use the **−−selfserve** option, you don't need to specify a zone for the computer. The computer is automatically made a member of the zone where the precreated object was created. You must, however, specify the Active Directory domain to successfully add the computer to the domain.

Note If you precreated the computer account with the **−−workstation** (Auto Zone) option, you must specify the **−−workstation** option when joining the domain with the **−−selfserve** option. For example:

```
adjoin acme.com −−selfserve −−workstation −−name testComputer
```

−r, −−useConf list

Specifies this option to use the settings in centrifydc.conf when perform self−service join. This option only be used with −S option. The settings can be a comma separated list of:

spn: use the setting of adclient.krb5.service.principals

enctype: use the setting of adclient.krb5.permitted.encryption.types

−A −−attempt
This option attempts to grant authenticated users read permissions to Password Settings objects (PSOs) so that the computer account can read fine−grained password security policies in the current domain. Note that the administrator(s) may need to grant authenticated users read permissions to PSOs in trusted domains and forests as well for more accurate password expiration times for cross−domain and cross−forest users.

−V, −−verbose
This option displays information about each step in the join process as it occurs. This option can be useful in diagnosing join problems. This option also writes log messages to the centrifydc.log file for troubleshooting purposes.

−w, −−workstation
Join the computer to an Active Directory domain by connecting to Auto Zone rather than by making the computer a member of any specific zone.

When joined to Auto Zone, every Active Directory user and group defined in the forest and any users defined in a two−way trusted forest are valid UNIX users or groups. You can use this option when:

− Active Directory identities are unique for the forest and the trusted external forest. Note that there must be a two−way cross−forest trust relationship. Users and groups in a forest with a one−way trust relationship will not be recognized as valid UNIX users and groups for computers joined to the domain using Auto Zone.

− Active Directory users and groups only require one set of properties for all computers and do not need to be segregated into zones for any reason.

For the join to be successful, all of the domains in the forest and the trusted external forest must be unique. If domains are not unique across the forest trust, you must manually configure a unique prefix for each trusted domain using parameters in the centrifydc.conf configuration file.

Note The **−−workstation** and **−−zone** options are mutually exclusively.

−x, −−extramap mapName
The *mapName* specifies an NSS map to add to the configuration. You can specify this option multiple times to add multiple maps. For example:

```
adjoin acme.com −z finance −x protocols −x ethers
```

−i, −−noinit
Do not preload the cache.

−E, −−prestage dir
The *dir* specifies the directory which contains the pre−staged cache. The cache files will be copied from this dir.

This option speeds up join procedure by using existing cache files from another joined machine that is joined to the same domain, and same zone. computer zone and computer role are not supported. The pre−staged cache can be obtained from a joined

machine by stopping adclient and copying the whole /var/centrifydc folder. Adjoin will fail if the specified dir does not exist, or does not contain the critical cache files. If the cache file is not owned by system account, or is a symlink, file or its parent folder is group or world writable, adjoin will also fail.

−v, −−version
This option displays version information for the installed software.

−e −−enableAppleIDGenScheme
This option enables you to use the Apple algorithm to automatically generate UIDs and GIDs for Active Directory users and groups when you join using **−−workstation** mode and the Auto Zone. The Apple algorithm uses the user or group globally unique identifier (objectGUID) to automatically generate UID and GID values. You cannot use this option when joining a named zone or when preparing a computer account using the **−−precreate** options. If you use the **−−enableAppleISGenSchme** option, the setting remains in effect even if you leave the Auto Zone and rejoin a named zone.

−t, −−Licensetype server|workstation
This option enables you to specify whether the computer joining the domain should use a "Server" license or a "Workstation" license. If you don’t specify this option, the computer is licensed as a server by default. You can change the license type after joining a domain with the **adlicense** command.

−G, −−loadgroups
Preload zone groups and group members. By default, adjoin only preloads zone users.

Note The −−loadgroups and −−noinit options are mutually exclusive and you should only specify one or the other. Preload zone groups and group members. By default, adjoin only preloads zone users.

−y, −−notime
Do not update computer time

−o, −−createComputerZone
Create computer zone for the current joined machine.

EXAMPLES

To join the acme.com domain using all of the default options, you could type a command line similar to the following (note that you must specify a zone):

```
adjoin acme.com −−zone finance
```

You are then prompted for the administrator password.

If you want to join a domain using an account that is not in the same domain as the domain you are joining and you want to use a specific host name, you could type a command line similar to the following:

```
adjoin  −−user jeff@acme.com −−name orlando −−container "ou=Unix computers" sales.acme.com  −−zone finance
```

You are then prompted to provide the password for the user jeff@acme.com.

The computer is added to Active Directory using the computer name "orlando" in the "Unix computers" Organizational Unit.

When specifying *username@domain* to join a domain, you cannot use an alternative UPN. For example, if your organization uses an alternate UPN to allow you to log in as garcia@mission.org but your account is actually defined in the sf.mission.org domain, you must use that domain when specifying the
user account:

```
adjoin --user garcia@sf.mission.org --zone finance la.mission.org
```

AUTHOR

Centrify Corporation

SEE ALSO

For related information, see the following command reference sections: adleave(1), adpasswd(1), adupdate(1), adquery(1), adgpupdate(1), adinfo(1), addebug(1), adclient(1)

NAME

adkeytab - create and manage Kerberos key tables (*.keytab files) and coordinate changes with the Kerberos key distribution center (KDC) provided by Active Directory.

SYNOPSIS

adkeytab -n, --new [-T, --trust] [-k, --des] [-d, --domain domain] [-m, --machine] [-u, --user *username[@domain]*] [-p, --password *userpassword*] [-U, --upn *userPrincipalName*] [-f, --force] [-S, --samname *samAccountName*] [-s, --server *servername*] [-g, --gc] [-i, --ignore] [-M, --computer-object] [-W, --password-never-expire] [-I, --interactive] [-V, --verbose] -P, --principal *principal ...* [-e, --encryption-type *etype ...*] [-y, --set-acct-enctype] -K, --keytab *filename* -c, --container *containerDN account-name*

adkeytab -a, --addspn [-d, --domain domain] [-m, --machine] [-u, --user *username[@domain]*] [-p, --password *userpassword*] [-U, --upn *userPrincipalName*] [-s, --server *servername*] [-V, --verbose] [-I, --interactive] -P, principal *principal ...* [-E, --entries *kvno*] [-e, --encryption-type *etype ...*] [-i, --ignore] [-K, --keytab *filename*] [-I, --interactive] *account-name*

adkeytab -A, --adopt [-m, --machine] [-u, --user *username[@domain]*] [-p, --password *userpassword*] [-P, principal *principal ...*] [-e, --encryption-type *etype ...*] [-i, --ignore] -K, --keytab *filename* [-f, --force] [-l, --local] [-w, --newpassword *newpassword*] [-T, --trust] [-k, --des] [-d, --domain *domain*] [-U, --upn *userPrincipalName*] [-s, --server *servername*] [-V, --verbose] [-I, --interactive] [-y, --set-acct-enctype] *account-name*

adkeytab -C, --change-password [-l, --local] [-w, --newpassword *newpassword*] [-m, --machine] [-u, --user *username[@domain]*] [-p, --password *userpassword*] [-i, --ignore] [-K, --keytab *filename*] [-d, --domain *domain*] [-s, --server *servername*] [-V, --verbose] [*account-name*] [-I, --interactive]

adkeytab -r, --reset [-u, --user *username[@domain]*] [-p, --password *userpassword*] [-d, --domain *domain*] [-i, --ignore] [-s, --server *servername*] [-V, --verbose] [-I, --interactive] [*account-name*]

adkeytab -x, --delspn [-m, --machine] [-u, --user *username[@domain]*] [-p, --password *userpassword*] [-i, --ignore] [-K, --keytab *filename*] [-d, --domain *domain*] [-s, --server *servername*] [-U, --upn *userPrincipalName*] [-V, --verbose] [-I, --interactive] -P, --principal *principal ...* [*account-name*]

adkeytab -D, --delete [-m, --machine] [-u, --user *username[@domain]*] [-p, --password *userpassword*] [-i, --ignore] -K, --keytab *filename* [-d, --domain *domain*] [-s, --server *servername*] [-f, --force] [-V, --verbose] [-I, --interactive] *account-name*

adkeytab -o, --copy -P, --principal *principal ...* -K, --keytab *filename* -b, --srckeytab *sourcefilename* [-V, --verbose]

Note The specific required parameters and options you can use depend on the task you want to perform. See the appropriate section for information about which options to use for each task. You can use the **[-V, --verbose]** option in conjunction with any task to display detailed information about the operations performed for diagnostic purposes.

AVAILABILITY

This command runs on AIX, Citrix XenServer, HP−UX, Linux, Mac OS X, Solaris, and VMware ESX operating environments.

GENERAL DESCRIPTION

The **adkeytab** command enables you to perform the following tasks:

− Create new service accounts and new key table files.

− Add new Kerberos service principals to existing key tables.

− Adopt Kerberos service principals for an existing Active Directory account and update the key tables and centrifydc.conf entries to manage the adopted account.

− Change the password for a computer account or service account and update the keys in its key table.

− Reset a key table that is corrupt or not synchronized with the KDC in Active Directory.

− Delete a service principal from a service account and remove its keys from the key table.

− Delete a service account from Active Directory and removed its key table and all related keys from the centrifydc.conf file.

− Copy the keys that matching the specified principal names from a key table file to a new key table file.

The synopsis illustrates the **adkeytab** syntax for each of these tasks.

CREATING A NEW SERVICE ACCOUNT AND KEYTAB

You can use the **adkeytab** command to create a new service account for a computer, to generate a keytab file for the new account on the computer’s local storage, and notify the KDC in Active Directory of the new service account for the computer.

The basic syntax for creating new service accounts and keytab files and synchronizing the information with Active Directory using the **adkeytab** command is:

adkeytab −−new −−principal *principal* −−keytab *filename* −−container *containerDN* [*options*] *account−name*

OPTIONS

You can use the following options to perform this task:

−n, −−new

Creates a new service account in Active Directory and a new key table for the account that is stored locally as a keytab file. If you use this option to generate a new service account and keytab file, **adkeytab** notifies the KDC in Active Directory of the key table contents. If you use this option, you must also specify a keytab file name using the **−−keytab** option and an *account−name* that is unique in the current domain.

−P, −−principal principal

Specifies the service principal to add to the new key table. You must specify at least one service principal when creating a new service account. To specify multiple service principals, use

this option multiple times.

For *principal* , type the service type of the service principal you want to add. You can specify the principal by:

− Service type alone (http)

− Service type and the host name or alias (http/firefly)

− Service type and the fully−qualified domain name (http/firefly.arcade.com)

If you use the service type alone, the adkeytab command generates the full principal name by expanding the name to include the account name at this computer, creating a fully−qualified domain name for the service principal account. For example, if you add the service principal http for service account firefly in domain arcade.com, adkeytab generates two service principals for the keytab file:
http/firefly@ARCADE.COM
http/firefly.arcade.com@ARCADE.COM

If you specify the service type with either a long or short host name, the adkeytab command will only generate the exact principal name specified.

Note If the service account name is different from the host name, you should have a DNS alias for the service account name that resolves to the host name of the computer. This allows you to have multiple service principals of the same type on the same computer, for example, multiple database services.

−i, −−ignore

Ignore the security risk of creating or updating a keytab file in a globally writeable directory, and allow the keytab file creation or update to proceed.

If you attempt to create or update a keytab file in a globally writeable directory and you do not specify this option, the operation fails and an error message is displayed.

−K, −−keytab filename

Specifies the name and location of the new keytab file to create. For the *filename* argument, you can specify either the relative or full path to the file you are creating.

−e, −−encryption−type etype

Specifies an encryption type to use in generating keys for each of the service principals you specified with the **−−principal** option.

Alternatively, you can use the **−−des** option in place of the **−−encryption−type** option to automatically generate des−cbc−crc and des−cdc−md5 keys. Using the **−−des** option is recommended if you configuring keytab entries for Oracle’s Advanced Security Option or services that support older versions of Kerberos. If you use the **−−des** option, the **−−encryption−type** parameter is ignored.

If you use the −−encryption−type parameter, each *etype* you specify generates a key table entry for a principal/encryption type combination. For example, if you specify two service principals and one encryption type, **adkeytab** generates a key table entry for each service principal with a key that uses the selected encryption type.

To specify multiple encryption types for a service principal, use this option multiple times. For example, if you specify one service principal and three different encryption types, **adkeytab** generates a separate key table entry for each encryption type for the service principal. If you do not specify an encryption type in the command line, the encryption types defined in the centrifydc.conf file are used. The default encryption types supported are:

- For Windows Server 2003 domain functional level:
  arcfour−hmac−md5, des−cbc−md5, and des−cbc−crc

- For Windows Server 2008 domain functional level:

  aes128−cts and aes256−cts

Although you can specify the Windows 2008 types in earlier environments, they are not useful and might cause extra network round trips during the authentication process.

Note If you specify an encryption type that is not listed as a permitted encryption type in the centrifydc.conf file, the key table entry will not be created and an error is displayed. You should verify that the encryption types you want to use are listed for the adclient.krb5.permitted.encryption.types configuration parameter.

−y, −−set−acct−enctype
Uses the encryption type set in the "msDS−SupportedEncryption−Types" attribute instead of the encryption types specified in the agent configuration file. If the "msDS−SupportedEncryption−Types" attribute is set to any value, the keytab file will use the encryption types defined in the attribute.

−c, −−container containerDN
Specifies the Active Directory name of the container (CN) or Organizational Unit (OU) into which the new service account should be placed.

You can specify the containerDN by:
- Canonical name (ajax.org/unix/services)
- Fully distinguished name (cn=services, cn=unix,dc= ajax,dc=org)
- Relative distinguished name without the domain suffix(cn=services,cn=unix)

For example, if you want to place the account in the UNIX/Services container within the ajax.org domain using the canonical name, you could specify: −−container "ajax.org/UNIX/Services"

Note The account used to run the **adkeytab** command must have permission to add objects to the container or organizational unit you specify.

−T, −−trust
Sets the **Trust for delegation** option in Active Directory for the new service account. Trusting an account for delegation allows the account to perform operations on behalf of other accounts on the network. For example, if the new service account is trusted for delegation, it can forward ticket−granting tickets and perform other delegated actions.

Setting this option may require the **adkeytab** command to run using an account with administrator permission.

−k, −−des
Specifies that all service principals for this account will use the Data Encryption Standard (DES) for keys.

Setting this option enables the **Use DES encryption types for this account** flag in the userAccountControl attribute of the service account.

You can use this option in place of the **−−encryption−type** option to automatically generate des−cbc−crc and des−cdc−md5 keys. Using the **−−des** option is recommended if you configuring keytab entries for Oracle’s Advanced Security Option or services that support older versions of Kerberos.

Note If you use the **−−des** option, the **−−encryption−type** parameter is ignored.

−d, −−domain domain
Specifies the domain in which this service account should be created. This option is used to create accounts in a domain other than the currently joined domain. If you do not specify this option, **adkeytab** creates the new service account in the currently joined domain by default.

−U, −−upn userPrincipalName
Sets the userPrincipalName attribute for the account in Active Directory.

Note For user service accounts, you only need to set this option if you want the userPrincipalName to be different from the default user@REALM setting.

−f, −−force
Overwrites an existing Active Directory object with the new account information. This option removes any existing service principals, keytab files and centrifydc.conf entries related to the specified *account−name* , in preparation for creating a new service account and key table.

This option is not required for precreated accounts that are inactive. This option is only required if the existing account is active and needs to be replaced.

−m, −−machine
Use the Active Directory computer account credentials generated by Centrify DirectControl to execute the adkeytab command. This option can be used in place of user credentials if the computer account has been granted permission to update its own account information.

Note Using the local computer’s credentials to update Active Directory requires local root permission when executing the adkeytab command.

−u, −−user username[@domain]
Specifies an Active Directory user other than the current user to execute the **adkeytab** command. The user must have sufficient rights to add an account to the domain. You must use the *username@domain* format to specify the user account if the *username* is not defined in the local computer’s domain. For example, if

the local computer is joined to the fire.arcade.com domain, but the user "marie" is a member of the arcade.com domain, you must specify the **−−user** option as:

```
−−user marie@arcade.com
```

If you do not specify the **−−user** option, **adkeytab** uses the current user’s Kerberos credentials by default. If there are no cached credentials for the current user, **adkeytab** uses the Administrator user account.

−p, −−password userpassword
Specifies the password for the Active Directory user account running the **adkeytab** command. If you do not specify this option or if there are no currently cached Kerberos credentials, **adkeytab** prompts for a password before it executes.

Note Specifying a password at the command line represents a security risk because the password can be retrieved while the command is running or from command history after the command has completed its execution.

−S, −−samname samAccountName
Specifies a pre−Windows 2000 account name for the object in Active Directory. This option sets the samAccountName attribute for the Active Directory object you are creating. You should use this option:

− If the account−name you are using for the object contains more than 20 characters.

− If you want the samAccountName attribute for the object to be different from the account−name. **Note** The samAccountName attribute (also known as the pre−Windows 2000 name) can be a maximum of 20 characters. The attribute must be unique within the Active Directory forest.

−s, −−server servername
Specifies the domain controller you want to use for performing this operation. Using this option enables you to avoid replication delays.

−g, −−gc hostname
Specifies the global catalog computer you want to search to check for duplicate samAccountName attributes. Using this option enables you to avoid replication delays.

−M, −−computer−object
Create service account as computer object. Without this option, account is created as user object.

−W, −−password−never−expire
Set password to never expire when creating account.

−V, −−verbose
Displays detailed information about the operation being performed.

account−name
Creates the specified *account−name* object in Active Directory. You must specify an *account−name* that is unique in the current domain. In addition, the *account−name* must be the last argument specified in the command line.

EXAMPLES FOR CREATING A NEW SERVICE ACCOUNT

To create a new DES−encrypted service account and accompanying key table, you would type a command similar to the following:

```
adkeytab −−new −−keytab /etc/krb5/mydatabase.keytab −−principal data1
−−principal data2 −−des −−container "ajax.org/users" −−user oracleadm
mydatabase
```

ADDING SERVICE PRINCIPALS TO A KEY TABLE

You can use the **adkeytab** command to add one or more service principals to an existing key table and notify the KDC in Active Directory of the new service principals for the computer or service account.

The basic syntax for adding new service principals and synchronizing the information with Active Directory using the **adkeytab** command is:

adkeytab −−addspn −−principal principal [options] [account−name]] *account−name*]

OPTIONS

You can use the following options to perform this task:

−a, −−addspn
Adds a service principal to an existing account in Active Directory and generates the appropriate keys for the new service principal in the account’s keytab file. If you don’t specify an *account−name* , the **adkeytab** command adds the service principal to the computer account in the currently joined domain.

−P, −−principal principal
Specifies the service principal to add to the specified key table. You must specify at least one service principal. To specify multiple service principals, use this option multiple times.

For the *principal* argument, type the service type of the service principal you want to add. You can specify the principal by:
− Service type alone (http)
− Service type and the host name or alias (http/firefly)
− Service type and the fully−qualified domain name (http/firefly.arcade.co

If you use the service type alone, the adkeytab command then generates the full principal name by expanding the short name to include the account name at this computer, creating a fully−qualified domain name (FQDN) for the service principal account. For example, if you add the service principal http for service account firefly in domain arcade.com, adkeytab generates two service principals for the keytab file:

```
http/firefly@ARCADE.COM
http/firefly.arcade.com@ARCADE.COM
```

Note If the service account name is different from the host name, you should have a DNS alias for the service account name that resolves to the host name of the computer. This allows you to have multiple service principals of the same type on the same computer, for example, multiple database services.

−E, −−entries kvno
Specifies the number of password hash entries (key version numbers) to keep in the keytab file. For the *kvno,* specify a positive integer between 1 and 253. If you omit the **−−entries** parameter, the default number is 3.

Note that **−−entries** is only relevant for 2003 or newer key distribution centers (KDC). For Windows 2000, **adkeytab** manufactures key version numbers as long as the **krb5.generate.kvno** configuration parameter is true (which is the default setting).

In the following circumstances the **entries** setting is ignored and only one password hash entry is kept:

If the KDC is Windows 2000 and the centrifydc.conf parameter **krb5.generate.kvno** is set to false.

If the KDC is Windows 2003 or newer but the **dsHeuristics** attribute is set to 00000000010000001. For more information about the **dsHeuristics** bit, see http://support.microsoft.com/kb/870987.

−e, −−encryption−type etype

Specifies an encryption type to use in generating keys for each of the service principals you specified with the **−−principal** option.

Alternatively, you can use the −−des option in place of the −−encryption−type option to automatically generate des−cbc−crc and des−cdc−md5 keys. Using the −−des option is recommended if you configuring keytab entries for Oracle’s Advanced Security Option or services that support older version of Kerberos. If you use the −−des option, the −−encryption−type parameter is ignored.

If you use the −−encryption−type parameter, each *etype* you specify generates a key table entry for a principal/encryption type combination. For example, if you specify two service principals and one encryption type, **adkeytab** generates a key table entry for each service principal with a key that uses the selected encryption type.

To specify multiple encryption types for a service principal, use this option multiple times. For example, if you specify one service principal and three different encryption types, **adkeytab** generates a separate key table entry for each encryption type for the service principal.

If you do not specify an encryption type in the command line, the encryption types defined in the centrifydc.conf file are used. The default encryption types supported are:

− For Windows Server 2003 domain functional level:

arcfour−hmac−md5, des−cbc−md5, and des−cbc−crc

− For Windows Server 2008 domain functional:

aes128−cts and aes256−cts

Although you can specify the Windows 2008 types in earlier environments, they are not useful and might cause extra network round trips during the authentication process.

Note If you specify an encryption type that is not listed as a permitted encryption type in the centrifydc.conf file, the key table entry will not be created and an error is displayed. You should verify that the encryption types you want to use are listed for the adclient.krb5.permitted.encryption.types

configuration parameter.

−m, −−machine

Uses the Active Directory computer account credentials generated by Centrify DirectControl to execute the adkeytab command. This option can be used in place of user credentials if the computer account has been granted permission to update its own account information.

Note Using the local computer’s credentials to update Active Directory requires local root permission when executing the adkeytab command.

−u, −−user username[@domain]

Specifies an Active Directory user other than the current user to execute the **adkeytab** command. The user must have sufficient rights to add a service principal to the account object. You must use the *username@domain* format to specify the user account if the *username* is not defined in the local computer’s domain. For example, if the local computer is joined to the fire.arcade.com domain, but the user "marie" is a member of the arcade.com domain, you must specify the **−−user** option as:

−−user marie@arcade.com

If you do not specify the −−user option, **adkeytab** uses the current user’s Kerberos credentials by default. If there are no cached credentials for the current user, **adkeytab** uses the Administrator user account.

−p, −−password userpassword

Specifies the password for the Active Directory user account running the **adkeytab** command. If you do not specify this option or if there are no currently cached Kerberos credentials, **adkeytab** prompts for a password before it executes.

Note Specifying a password at the command line represents a security risk because the password can be retrieved while the command is running or from command history after the command has completed its execution.

−i, −−ignore

Ignore the security risk of creating or updating a keytab file in a globally writeable directory, and allow the keytab file creation or update to proceed.

If you attempt to create or update a keytab file in a globally writeable directory and you do not specify this option, the operation fails and an error message is displayed.

−K, −−keytab filename

Specifies the name and location of the keytab file to add. For the filename, you can specify either the relative or full path to the file.

−d, −−domain domain

Specifies the domain in which this service principal should be added. If you do not specify this option, adkeytab uses the currently joined domain by default.

−U, −−upn userPrincipalName

Sets the userPrincipalName attribute for the account in Active Directory.

Note For user service accounts, you only need to set this option if you want the userPrincipalName to be different from the default user@REALM setting.

−s, −−server hostname
Specifies the domain controller you want to use for performing this operation. Using this option enables you to avoid replication delays.

−V, −−verbose
Displays detailed information about the operation being performed.

account−name
The *account name* specifies the account object to which you are adding a service principal. If you don't specify an *account−name,* **adkeytab** adds the service principal to the computer account object in the currently joined domain. If you specify the I account−name , it must be the last argument in the command line.

EXAMPLES FOR ADDING SERVICE PRINCIPALS TO AN ACCOUNT

To add a new DES−encrypted service principal for oracle to the key table that belongs to the service account mydatabase, you would type a command similar to the following:

```
adkeytab −−addspn −−principal oracle −−des mydatabase
```

To add a DES−encrypted service principal for Oracle databases named oracle_d1 and oracle_d2 to the computer account key table in the currently joined domain:

```
adkeytab −−addspn −−principal oracle_d1 −−principal oracle_d2
−−encryption−type des−cbc−md5
```

SELECTING AN EXISTING ACCOUNT TO ADOPT

You can use the **adkeytab** command with the **−−adopt**
option to have the Centrify agent take over the management of keytab files for an existing account in Active Directory. This option creates the local keytab file for the account and adds entries for any existing service principal names associated with the account to the centrifydc.conf file. You can also specify additional service principal names and encryption types.

The basic syntax for adopting the service principals associated with an existing account and synchronizing the information with Active Directory using the adkeytab command is:

adkeytab −−adopt −−keytab *filename* [options] *account−name*

OPTIONS

You can use the following options to perform this task:

−A, −−adopt
Adds the appropriate keytab and centrifydc.conf entries to adopt an existing account and its service principals for management through Centrify DirectControl.

−i, −−ignore
Ignore the security risk of creating or updating a keytab file in a globally writeable directory, and allow the keytab file creation or update to proceed.

If you attempt to create or update a keytab file in a globally writeable directory and you do not specify this option, the operation fails and an error message is displayed.

−K, −−keytab filename
Specifies the name and location of the keytab file for the account.

−P, −−principal principal
Specifies an additional service principal for the account in the key table. This option is not required as long as the existing account has at least one service principal already defined. To specify multiple service principals, use this option multiple times. For *principal* , type the service type of the service principal you want to add. You can specify the principal by:
− Service type alone (http)
− Service type and the host name or alias (http/firefly)
− Service type and the fully−qualified domain name (http/firefly.arcade.co

If you use the service type alone, the adkeytab command then generates the full principal name by expanding the short name to include the account name at this computer, creating a fully−qualified domain name (FQDN) for the service principal account. For example, if you add the service principal http for service account firefly in domain arcade.com, adkeytab generates two service principals for the keytab file:
http/firefly@ARCADE.COM
http/firefly.arcade.com@ARCADE.COM

Note If the service account name is different from the host name, you should have a DNS alias for the service account name that resolves to the host name of the computer. This allows you to have multiple service principals of the same type on the same computer, for example, multiple database services.

−e, −−encryption−type etype
Specifies an encryption type to use in generating keys for each service principal you specified with the −−principal option.

Alternatively, you can use the −−des option in place of the −−encryption−type option to automatically generate des−cbc−crc and des−cdc−md5 keys. Using the −−des option is recommended if you configuring keytab entries for Oracle's Advanced Security Option or services that support older versions of Kerberos. If you use the −−des option, the −−encryption−type parameter is ignored.

If you use the −−encryption−type parameter, each *etype* you specify generates a key table entry for a principal/encryption type combination. For example, if you specify two service principals and one encryption type, adkeytab generates a key table entry for each service principal with a key that uses the selected encryption type.

To specify multiple encryption types for a service principal, use this option multiple times. For example, if you specify one service principal and three different encryption types, adkeytab generates a separate key table entry for each encryption type for the service principal.

If you do not specify an encryption type in the command line, the encryption types defined in the centrifydc.conf file are used. The default encryption types supported are:

- For Windows Server 2003 domain functional level:

  arcfour−hmac−md5, des−cbc−md5, and des−cbc−crc

- For Windows Server 2008 domain functional level:

  aes128−cts and aes256−cts

Although you can specify the Windows 2008 types in earlier environments, they are not useful and might cause extra network round trips during the authentication process.

Note If you specify an encryption type that is not listed as a permitted encryption type in the centrifydc.conf file, the key table entry will not be created and an error is displayed. You should verify that the encryption types you want to use are listed for the adclient.krb5.permitted.encryption.types configuration parameter.

−m, −−machine
Uses the Active Directory computer account credentials generated by Centrify DirectControl to execute the adkeytab command. This option can be used in place of user credentials if the computer account has been granted permission to update its own account information.

Note Using the local computer's credentials to update Active Directory requires local root permission when executing the adkeytab command.

−u, −−user username[@domain]
Specifies an Active Directory user other than the current user to execute the adkeytab command. The user must have sufficient rights to read the Active Directory account object and update the userAccountControl attribute, if necessary. If you are specifying additional service principal names, the user must also have sufficient privileges to update the account's servicePrincipalName attribute.

You must use the username@domain format to specify the user account if the *username* is not defined in the local computer's domain. For example, if the local computer is joined to the fire.arcade.com domain, but the user marie is a member of the arcade.com domain, you must specify the −−user option as:

−−user marie@arcade.com

If you do not specify the −−user option, adkeytab uses the current user's Kerberos credentials by default. If there are no cached credentials for the current user, adkeytab uses the Administrator user account.

−p, −−password userpassword
Specifies the password for the Active Directory user account running the adkeytab command. If you do not specify this option or if there are no currently cached Kerberos credentials, adkeytab prompts for a password before it executes.

Note Specifying a password at the command line represents a security risk because the password can be retrieved while the command is running or from command history after the command has completed its execution.

−f, −−force
Overwrite an existing Active Directory object with the new account information. This option removes any existing service principals, keytab files and centrifydc.conf entries related to the specified account−name, in preparation for creating a new service account and key table.

Note This option is not required for precreated accounts that are inactive. This option is only required if the existing account is active and needs to be replaced.

−l, −−local
Updates the password hashes in the local keytab file without changing the password in Active Directory. If you use this option, you must also specify the password value with the **−−new−password** option.

This option can be useful in cluster environments where you run adkeytab to force a password change on the Active Directory object and the local keytab on a master server, then run adkeytab with the −−change−password and −−local options on the backup computers to synchronize the new password in the keytab files on those computers.

−w, −−newpassword newpassword
Specifies a new password to substitute for the old password. If you do not specify this option, adkeytab generates a random password.

−T, −−trust
Sets the **Trust for delegation** option in Active Directory for the new service account. Trusting an account for delegation allows the account to perform operations on behalf of other accounts on the network. For example, if the new service account is trusted for delegation, it can forward ticket−granting tickets and perform other delegated actions.

Setting this option may require the adkeytab command to run using an account with administrator permission.

−k, −−des
Specifies that all service principals for this account will use the Data Encryption Standard (DES) for keys. Setting this option enables the **Use DES encryption types** for this account flag in the userAccountControl attribute of the service account. You can use this option in place of the −−encryption−type option to automatically generate des−cbc−crc and des−cdc−md5 keys. Using the −−des option is recommended if you configuring keytab entries for Oracle's Advanced Security Option or services that support older versions of Kerberos.

Note If you use the −−des option, the −−encryption−type parameter is ignored.

−d, −−domain domain
Specifies the domain in which this service principal should be added. If you do not specify this option, adkeytab uses the currently joined domain by default.

−U, −−upn userPrincipalName
Sets the userPrincipalName attribute for the account in Active Directory.

Note For user service accounts, you only need to set this option if you want the userPrincipalName to be different from the default user@REALM setting.

-s, --server hostname

Specifies the domain controller you want to use for performing this operation. Using this option enables you to avoid replication delays.

-V, --verbose

Displays detailed information about the operation being performed.

account-name

Specifies the existing *account-name* that you want to manage keytab entries for using Centrify DirectControl.

If you don’t specify an *account-name* , adkeytab adopts the service principals associated with the computer account object in the currently joined domain. If you specify the *account-name* , it must be the last argument in the command line.

EXAMPLES FOR ADOPTING AN EXISTING ACCOUNT

To adopt the existing service principals for the existing service account name oracle_acct, you could type a command similar to this:

```
adkeytab --adopt --user oracleadm --keytab /etc/krb5/oracle_hr.keytab
oracle_acct
```

In a cluster environment, you can use adkeytab --new to create a new account principal on the primary cluster server and set its password to a known value. You can then run adkeytab --adopt with the --local and --newpassword options on all of the other computers in the cluster to create a local copy of the keytab file. For example:

```
adkeytab --adopt  --local  --newpassword  password  --user  oracleadm
--keytab /etc/krb5/oracle_hr.keytab oracle_acct
```

After running this command, all of the computers in the cluster are synchronized with the same password.

CHANGING THE PASSWORD FOR A COMPUTER OR SERVICE ACCOUNT

You can use the **adkeytab** command to change the password for a service or computer account, generate new keys for the account’s service principals, write the new keys to the account’s key table, and notify Active Directory of the changed password and new keys.

The basic syntax for changing an account password and synchronizing the information with Active Directory using the adkeytab command is:

```
adkeytab --change-password [options] [account-name]
```

OPTIONS

You can use the following options to perform this task:

-C, --change-password

Changes the password for a specified *account-name.* Using this option generates new keys in the keytab file for the specified *account-name* , and notifies the KDC in Active Directory of the change.

-l, --local

Updates the password hashes in the local keytab file without changing the password in Active Directory. If you use this option, you must also specify the password value with the **--newpassword** option.

The **--local** option can be useful in cluster environments where you run **adkeytab** to force a password change on the Active Directory object and the local keytab on a master server, then run **adkeytab** with the **--change-password** and **--local** options on the backup computers to synchronize the new password in the keytab files on those computers.

-w, --newpassword newpassword

Specifies a new password to substitute for the old password. If you do not specify this option, **adkeytab** generates a random password.

-m, --machine

Uses the Active Directory computer account credentials generated by the Centrify agent to execute the adkeytab command. This option can be used in place of user credentials if the computer account has been granted permission to update its own account information.

Note Using the local computer’s credentials to update Active Directory requires local root permission when executing the adkeytab command.

-u, --user username[@domain]

Specifies an Active Directory user other than the current user to execute the adkeytab command. The user must have sufficient rights to read the Active Directory account object and update the userAccountControl attribute, if necessary. If you are specifying additional service principal names, the user must also have sufficient privileges to update the account’s servicePrincipalName attribute.

You must use the username@domain format to specify the user account if the *username* is not defined in the local computer’s domain. For example, if the local computer is joined to the fire.arcade.com domain, but the user marie is a member of the arcade.com domain, you must specify the --user option as:

```
--user marie@arcade.com
```

If you do not specify the --user option, adkeytab uses the current user’s Kerberos credentials by default. If there are no cached credentials for the current user, adkeytab uses the Administrator user account.

-p, --password userpassword

Specifies the password for the Active Directory user account running the adkeytab command. If you do not specify this option or if there are no currently cached Kerberos credentials, adkeytab prompts for a password before it executes.

Note Specifying a password at the command line represents a security risk because the password can be retrieved while the command is running or from command history after the command has completed its execution.

−i, −−ignore
Ignore the security risk of creating or updating a keytab file in a globally writeable directory, and allow the keytab file creation or update to proceed.

If you attempt to create or update a keytab file in a globally writeable directory and you do not specify this option, the operation fails and an error message is displayed.

−K, −−keytab filename
Specifies the name and location of the keytab file for the account.

−d, −−domain domain
Specifies the domain in which this service principal should be added. If you do not specify this option, adkeytab uses the currently joined domain by default.

−s, −−server hostname
Specifies the domain controller you want to use for performing this operation. Using this option enables you to avoid replication delays.

−V, −−verbose
Displays detailed information about the operation being performed.

−I, −−interactive
Prompts for the user password. In most cases, this option is used when the Kerberos credential cache used to authenticate a user to an Active Directory domain, and a read−only domain controller of the domain has revoked the user's Kerberos ticket. By providing a valid password, the user can be granted a new Kerberos ticket to replace the revoked ticket. Or use this option as an alternative to **−−newpasswd** to prevent entering a password in clear text on the command line.

account−name
Specifies the account object for which you are changing the password.

If you don't specify an *account−name* , the **adkeytab** command changes the password of the computer account object for the local computer in the currently joined domain. If you specify an *account−name* , it must be the last argument in the command line.

EXAMPLES FOR CHANGING AN ACCOUNT PASSWORD

To change the password for the computer account in the currently joined domain to use a new randomly−generated password, you would type a command similar to the following:

```
adkeytab −C
```

To explicitly set the password for the service account mysql−sf in Active Directory, you would type a command similar to the following:

```
adkeytab −−change−password −−newpassword 'miles8!' mysql−sf
```

Note Single quotes are required around the password in this example because the password contains a special character that would be misinterpreted by the UNIX shell.

RESETTING A KEY TABLE

You can use the **adkeytab** command to reset a key table when it is out of synchronization with the KDC in Active Directory. The −−reset option is typically used to reset the service account password to a known value (up to the first 14 characters of its common name) when the password hash for the service account is not the same the application's keytab file as the password hash in the KDC. To use the −−reset option, you must provide credentials for an account with permission to perform the password modification on the Active Directory object.

Note If the Centrify DirectControl Agent is running in disconnected mode because of a password problem, the computer account credentials are invalid and cannot be used to reset the service account password.

The basic syntax for resetting a key table and synchronizes the information with Active Directory using the **adkeytab** command is:

```
adkeytab −−reset [options] [account−name]
```

Running **adkeytab** with the **−−reset** option checks the current password for the computer account that is stored in Active Directory, uses it to regenerate keys for the account's service principals, writes those keys into the account keytab file, then reports the keys to the KDC in Active Directory.

OPTIONS

You can use the following options to perform this task:

−r, −−reset
Resets an account's key table and synchronizes its contents with the key distribution center in Active Directory.

−i, −−ignore
Ignore the security risk of creating or updating a keytab file in a globally writeable directory, and allow the keytab file creation or update to proceed.

If you attempt to create or update a keytab file in a globally writeable directory and you do not specify this option, the operation fails and an error message is displayed.

−u, −−user username[@domain]
Specifies an Active Directory user other than the current user to execute the **adkeytab** command. The user must have sufficient rights to read the computer account password. You must use the *username@domain* format to specify the user account if the *username* is not defined in the local computer's domain. For example, if the local computer is joined to the fire.arcade.com domain, but the user "marie" is a member of the arcade.com domain, you must specify the **−−user** option as:

```
−−user marie@arcade.com
```

If you do not specify the −−user option, **adkeytab** uses the current user's Kerberos credentials by default. If there are no cached credentials for the current user, **adkeytab** uses the Administrator user account.

−p, −−password userpassword
Specifies the password for the Active Directory user account running the **adkeytab** command. If you do not specify this option

or if there are no currently cached Kerberos credentials, **adkeytab** prompts for a password before it executes.

Note Specifying a password at the command line represents a security risk because the password can be retrieved while the command is running or from command history after the command has completed its execution.

−d, −−domain domain

Specifies the domain in which this service principal should be added. If you do not specify this option, adkeytab uses the currently joined domain by default.

−s, −−server servername

Specifies the domain controller you want to use for performing this operation. Using this option enables you to avoid replication delays.

−V, −−verbose

Displays detailed information about the operation being performed.

account−name

Specifies the account object for which you are resetting the key table.

If you don't specify an account−name, the adkeytab command resets the key table for the local computer account object in the currently joined domain. If you specify the account−name, it must be the last argument in the command line.

EXAMPLES FOR RESETTING A KEY TABLE

To reset the key table that belongs to the service account mydatabase, you would type a command similar to the following:

```
adkeytab −−reset mydatabase
```

To specify an Active Directory user account that is not a member of the same domain as the currently joined domain:

```
adkeytab −−reset −−user jason@arcade.com mydatabase
```

You are then prompted to provide the password for the jason@arcade.com account.

DELETING SERVICE PRINCIPALS FROM AN ACCOUNT

You can use the adkeytab command to delete a service principal from a service account and remove its keys from the key table.

The basic syntax for removing service principals and synchronizing the information with Active Directory using the **adkeytab** command is:

```
adkeytab −−delspn −−principal principal [options] [account−name]
```

OPTIONS

You can use the following options to perform this task:

−x, −−delspn

Removes a service principal from an existing account in Active Directory and remove its keys from the account's keytab file.

−P, −−principal principal

Specifies the service principal to remove from the specified

account−name key table. You must specify at least one service principal. To specify multiple service principals, use this option multiple times.

For principal, type the service type of the service principal you want to delete. You can specify the principal by:
− Service type alone (http)
− Service type and the host name or alias (http/firefly)
− Service type and the fully−qualified domain name (http/firefly.arcade.co

If you use the service type alone, the adkeytab command removes all service principal names that start with the specified service type. If you specify the service type with either a long or short host name, the adkeytab command will only remove the exact principal name specified.

Note If the service account name is different from the host name, you should have a DNS alias for the service account name that resolves to the host name of the computer. This allows you to have multiple service principals of the same type on the same computer, for example, multiple database services.

−m, −−machine

Uses the Active Directory computer account credentials generated by Centrify DirectControl to execute the adkeytab command. This option can be used in place of user credentials if the computer account has been granted permission to update its own account information.

Note Using the local computer's credentials to update Active Directory requires local root permission when executing the adkeytab command.

−u, −−user username[@domain]

Specifies an Active Directory user other than the current user to execute the **adkeytab** command. The user must have sufficient rights to delete a service principal from the account object in Active Directory. You must use the *username@domain* format to specify the user account if the username is not defined in the local computer's domain. For example, if the local computer is joined to the fire.arcade.com domain, but the user "marie" is a member of the arcade.com domain, you must specify the **−−user** option as: −−user marie@arcade.com If you do not specify the **−−user** option, **adkeytab** uses the current user's Kerberos credentials by default. If there are no cached credentials for the current user, the command uses the Administrator user account.

−p, −−password userpassword

Specifies the password for the Active Directory user account running the **adkeytab** command. If you do not specify this option or if there are no currently cached Kerberos credentials, **adkeytab** prompts for a password before it executes.

Note Specifying a password at the command line represents a security risk because the password can be retrieved while the command is running or from command history after the command has completed its execution.

−i, −−ignore

Ignore the security risk of creating or updating a keytab file in a globally writeable directory, and allow the keytab file creation or update to proceed.

If you attempt to create or update a keytab file in a globally writeable directory and you do not specify this option, the operation fails and an error message is displayed.

−K, −−keytab filename
Specifies the name and location of the keytab file for the account.

−d, −−domain domain
Specifies the domain in which this service principal should be added. If you do not specify this option, adkeytab uses the currently joined domain by default.

−s, −−server hostname
Specifies the domain controller you want to use for performing this operation. Using this option enables you to avoid replication delays.

−U, −−upn userPrincipalName
Specifies the userPrincipalName attribute for the account in Active Directory.

Note For user service accounts, you only need to set this option if you want the userPrincipalName to be different from the default user@REALM setting.

−V, −−verbose
Displays detailed information about the operation being performed.

account−name
The *account−name* specifies the account object from which you are removing a service principal. If you don’t specify an *account−name* in the command line, **adkeytab** removes the service principal from the computer account object in the currently joined domain. If you specify the *account−name* , it must be the last argument in the command line.

EXAMPLES FOR DELETING A SERVICE PRINCIPAL

To remove the service principal oracle_d1 from the key table that belongs to the service account berlin_db, you would type a command similar to the following:

```
adkeytab −−delspn −−principal oracle_d1 berlin_db
```

DELETING A SERVICE ACCOUNT

You can use the **adkeytab** command to delete a service account from Active Directory. Deleting a service account removes the account object from Active Directory, removes the key table for the account from the local computer, and removes all keys related to the account from the centrifydc.conf file.

If any of the items to be deleted is not found, the command prompts you to confirm whether you want to proceed with the delete operation for the items found. For example, if the account object is not found in Active Directory but a local keytab file is found for the service account, the command displays a warning that account object was not found and asks you to confirm whether to continue with the delete operation for the items found. If you proceed, the command then removes the keytab file and any related keys in the centrifydc.conf file. You can use the **−−force** option to skip checking for missing components and force the **adkeytab** command to proceed silently with the delete operation.

To use this command to delete service accounts, you must specify a user with sufficient rights to remove account objects in Active Directory, and key tables and related keys in the centrifydc.conf file on the local computer.

The basic syntax for removing service accounts from Active Directory using the **adkeytab** command is:

adkeytab −−delete −−keytab *filename* [options] account−name

OPTIONS

You can use the following options to perform this task:

−D, −−delete
Removes a service account object from Active Directory and removes its key table and all related key entries from the centrifydc.conf file.

−i, −−ignore
Ignore the security risk of creating or updating a keytab file in a globally writeable directory, and allow the keytab file creation or update to proceed.

If you attempt to create or update a keytab file in a globally writeable directory and you do not specify this option, the operation fails and an error message is displayed.

−K, −−keytab filename
Specifies the full path to the keytab file you want to remove.

−d, −−domain domain
Specifies the domain in which this service principal should be added. If you do not specify this option, adkeytab uses the currently joined domain by default.

−s, −−server hostname
Specifies the domain controller you want to use for performing this operation. Using this option enables you to avoid replication delays.

−m, −−machine
Uses the Active Directory computer account credentials generated by Centrify DirectControl to execute the adkeytab command. This option can be used in place of user credentials if the computer account has been granted permission to update its own account information.

Note Using the local computer’s credentials to update Active Directory requires local root permission when executing the adkeytab command.

−u, −−user username[@domain]
Specifies an Active Directory user other than the current user to execute the adkeytab command. The user must have sufficient rights to delete account objects in Active Directory. You must use the username@domain format to specify the user account if the username is not defined in the local computer’s domain. For example, if the local computer is joined to the fire.arcade.com domain, but the user marie is a member of the arcade.com domain, you must specify the −−user option as:

```
−−user marie@arcade.com
```

If you do not specify the −−user option, adkeytab uses the current user’s Kerberos credentials by default. If there are no cached credentials for the current user, adkeytab uses the Administrator user account.

−p, −−password userpassword

Specifies the password for the Active Directory user account running the adkeytab command. If you do not specify this option or if there are no currently cached Kerberos credentials, adkeytab prompts for a password before it executes.

Note Specifying a password at the command line represents a security risk because the password can be retrieved while the command is running or from command history after the command has completed its execution.

−f, −−force

Skips any checking for missing components and proceed with the delete operation, ignoring any errors encountered.

−V, −−verbose

Displays detailed information about the operation being performed.

account−name

Specifies the name of the service account you want to remove.

EXAMPLES FOR DELETING A SERVICE ACCOUNT

To remove the service account berlin_db, you would type a command similar to the following:

```
adkeytab −−delete −−user oracleadm berlin_db
```

COPYING THE KEYS TO A NEW KEY TABLE FILE

You can use the **adkeytab** command to copy the keys that matching the specified principal names from a key table file to a new key table file.

To use this command to copy the keys to a new file, you must be the local root so that you can access the local machine key table file.

The basic syntax for copying keys from a key table file to a new key table file using the **adkeytab** command is:

adkeytab −−copy −−principal *principal* −−keytab *filename* −−srckeytab *source−filename*

OPTIONS

You can use the following options to perform this task:

−P, −−principal principal

Specifies the service principal to copy to the new key table. You must specify at least one service principal when creating a new key table file. To specify multiple service principals, use this option multiple times.

For *principal* , type the service type of the service principal you want to copy. You can specify the principal by:

− Service type alone (http)

− Service type and the host name or alias (http/firefly)

− Service type and the fully−qualified domain name (http/firefly.arcade.com)

If you use the service type alone, the adkeytab command generates the full principal name by expanding the name to include the account name at this computer, trying to copy a fully−qualified domain name for the service principal account. For example, if you want to copy the service principal http for service account firefly in domain arcade.com, adkeytab tries to copy two service principals for the keytab file:
http/firefly@ARCADE.COM
http/firefly.arcade.com@ARCADE.COM

If you specify the service type with either a long or short host name, the adkeytab command will only copy the exact principal name specified.

−i, −−ignore

Ignore the security risk of creating or updating a keytab file in a globally writeable directory, and allow the keytab file creation or update to proceed.

If you attempt to create or update a keytab file in a globally writeable directory and you do not specify this option, the operation fails and an error message is displayed.

−K, −−keytab filename

Specifies the full path to the keytab file you want to create.

−b, −−srckeytab source−filename

Specifies the full path to the keytab file you want to copy from.

−V, −−verbose

Displays detailed information about the operation being performed.

EXAMPLES FOR COPYING THE KEYS FOR A SERVICE

To creat a key table file for the ftp service, you would type a command similar to the following:

```
adkeytab −−copy −−principal ftp −−keytab /var/ftp/ftp.keytab  −−srck−
eytab /etc/krb5.keytab
```

SPECIFYING THE ENCRYPTION TYPE FOR SERVICE PRINICIPALS

If you are creating a new service account and key table or adding service principals to an existing key table, you must specify the encryption type for each service principal you add. The valid encryption types are those defined by the MIT implementation of Kerberos and specified using either the Centrify DirectControl **Encryption Types** group policy or the Centrify DirectControl **adclient.krb5.tkt.encryption.types** configuration parameter.

Although Centrify supports all of the standard encryption types, some encryption types are only supported on particular versions of Windows. For example, Windows Server 2008 supports AES encryption, but earlier versions of Windows do not. The default encryption types supported by Windows Server 2003 are:
− arcfour−hmac−md5
− des−cbc−md5
− des−cbc−crc

If you are using Windows Server 2008 domain functional level, the following additional encryption types are supported:
− aes128−cts
− aes256−cts

For more information about configuring the supported encryption types using group policy, see the *Centrify Group Policy Guide.* For more information about configuring encryption types using configuration parameters in the centrifydc.conf file, see the *Centrify Configuration and Tuning Reference Guide.*

AUTHOR

Centrify Corporation

SEE_ALSO

adclient(1) and adjoin(1) for information about how a Kerberos key table is first created for a computer when the computer is added to an Active Directory domain.

NAME

adleave − leave an Active Directory domain.

SYNOPSIS

adleave [−−user *username[@domain]]* [−−password *userpassword]* [−−noprompt] [−−server *domaincontroller]* [−−zoneserver *domaincontroller]* [−−noconf] [−−force] [−−nogp] [−−remove] [−−restore] [−−reset] [−−removekeytab] [−−removecomputerzone] [−−removemachinescope] [−−version] [−−verbose]

DESCRIPTION

The **adleave** command removes the local host computer from its current Active Directory domain. Once a computer has become a member of a domain, you must run the **adleave** command to leave that domain before you can move a computer to a new domain.

To run **adleave** you must be logged in as root.

By default, when you run adleave, the program performs the following tasks:

− Contacts Active Directory and deactivates the computer account associated with the local UNIX host. The program does not remove the computer account from Active Directory. To remove the computer account entirely, you must delete it from Active Directory manually with Active Directory Users and Computers.

− Reverts any computer settings that were changed by the adjoin command to their pre−adjoin condition. This includes reverting PAM and NSS configuration files to their pre−adjoin states and deleting the /var/centrifydc/* files.

Note When you join a domain, the Kerberos configuration file, /etc/krb5.conf, and keytab file, /etc/krb5.keytab, are automatically generated for you. Because the /etc/krb5.conf file can contain entries used by other applications, it is not removed automatically when you leave a domain. If you leave the domain, you should check whether this file is used by any other applications or if it has been manually edited. If it is not used by other applications, you can safely delete the file after leaving the domain.

− Stops the Centrify agent (adclient).

OPTIONS

You can use the following options with this command:

−u, −−user username[@domain]
The *username* identifies an Active Directory user account with sufficient rights to remove a computer from the domain. You must use the *username@domain* format to specify the user account if the *username* is not a member of the computer’s current domain. If you do not specify the **−−user** option, the default is the "administrator" user account.

−p, −−password userpassword
The *userpassword* specifies the password for the Active Directory user account performing the leave operation. If you do not provide the password at the command line, you are prompted to enter the password before the command executes.

Note Specifying a password at the command line represents a security risk because the password can be retrieved while the command is running or from command history after the command has completed its execution.

−I, −−noprompt
If no credentials found, adleave will prompt for user credential to proceed. If this option is specified, adleave will not prompt and just fails.

−s, −−server domaincontroller
The *domaincontroller* specifies the name of the domain controller that you prefer to use to disconnect from the domain. You can use this option to override the automatic selection of a domain controller based on the Active Directory site information.

−Z, −−zoneserver domaincontroller
The *domaincontroller* specifies the name of the domain controller to use for zone operations. You can use this option, for example, if the zone is defined in a different domain than the domain you are leaving.

−C, −−noconf
This option indicates that you do not want to revert the local system’s PAM and NSS configuration files to their original state. Normally, if you leave a domain, any changes that have been made to the PAM and NSS configuration files to work with the Centrify agent are removed. If you set this option to leave the file changes in place, you should review the PAM and NSS configuration files for potential changes.

Note Be sure to review and, if necessary, edit the PAM and NSS configuration files **before** you use this option. If you don’t take precautions before using this option, the computer may become inoperable and require a reboot in single user mode to fix the problem.

−f, −−force
This option indicates that you want to force the local computer’s settings to their pre−join conditions even if the adleave command cannot connect to Active Directory or is not successful in deactivating the Active Directory computer account.

You must use this option if the Active Directory computer account has been modified or deleted so that the host computer can no longer work with it.

−G, −−nogp
This option indicates that you do not want to revert any group policies applied to the computer to their original state. Normally, if you leave a domain, any group policy changes that have been applied to UNIX configuration files are reverted to restore the files to their pre−join state.

−r, −−remove
This option removes the computer account from Active Directory.

−k, −−removekeytab
This option removes the keytab file. If you don’t specify this option, adleave only cleans up the keytab entries.

−o, −−removecomputerzone
For the currently joined computer, this option removes the computer zone from Active Directory.

−O, −−removemachinescope
For the currently joined computer, this option removes the privilege elevation scope from Active Directory.

−R, −−restore
This option restores the system configuration files to their pre−join state without leaving the domain.

−t, −−reset
This option resets the computer account to its precreated, pre−joined state.

It resets the computer account password to the hostname (in lowercase) and disables the computer zone object.

Specifying −−reset allows you to leave a domain, then rejoin using the adjoin −−selfserve option, which allows you to specify machine credentials when joining a domain. This option is valuable for virtual, cloud−computing environments that require the ability to dynamically join and leave a domain.

−v, −−version
This option displays version information for the installed software.

−V, −−verbose
This option displays detailed information for each operation.

EXAMPLES

To remove a computer from the current domain, you could type a command line similar to the following:

```
adleave −−user raj@acme.com
```

You are then prompted for the password for the user raj@acme.com.

To remove a computer from its current domain using a specific user account and without reverting the PAM and NSS configuration files to their pre−join state, you could type a command line similar to the following:

```
adleave −−user raj@acme.com −−noconf
```

To revert all computer settings to their pre−join state even if unable to deactivate the host computer’s in Active Directory account, you could type a command line similar to the following:

```
adleave −−force
```

You are then prompted for the password for the user raj@acme.com.

AUTHOR

Centrify Corporation

SEE ALSO

For related information, see the following command reference sections: adjoin(1), adpasswd(1), adgpupdate(1), adinfo(1), addebug(1)

NAME

adlicense − enable or disable licensed features or change the license type on a local computer.

SYNOPSIS

adlicense [--licensed] [--express] [--licensetype server|workstation] [--query] [--verbose] [--version]

DESCRIPTION

The **adlicense** command can be used to enable or disable licensed features on a local computer.

If you execute **adlicense** with no options, it displays the current mode, either "licensed" or "express".

In licensed mode, a computer has access to group policies and may join any existing zones.

In express mode (licensing is disabled) a computer may not download or execute group policies and cannot join a zone. The computer is automatically joined to Auto Zone.

To run **adlicense** you must be logged in as root.

OPTIONS

You can use the following options with this command:

-l, --licensed

The **--licensed** option enables licensed features, including the ability to use group policies and join a specific zone. After you enable licensed features, the computer is still joined to Auto Zone. You may keep the computer joined to Auto Zone or join a specific zone, in which case, you must first leave the zone with **adleave,** then rejoin the domain with the **adjoin -z** command.

Note: To enable licensing, you must have installed a valid license key. A license is consumed when you enable licensing.

-e, --express

The **--express** option disables licensed features. It unmaps group policies and prevents the machine from joining any specific zones. The computer is automatically joined to Auto Zone.

If you are running in licensed mode, and execute **adlicense --express** to switch to Express Mode, a license is restored.

Note: You cannot use this option if the machine is currently joined to a zone. You must first leave the domain, then connect to Auto Zone when rejoining the domain.

-t, --licensetype server|workstation

The **licensetype** option enables you to specify the type of license a managed computer uses. This option is only applicable if you are using licensed features. You can use this option to change the type of license being used after joining a domain.

-q, --query

The **--query** option displays the licensing status and license type for the local computer. If you use this option and

"unspecified" is displayed as the license type, you can use the **--licensetype** option to set the license type to either "server" or "workstation" for the local computer.

-V, --verbose

The **--verbose** option displays detailed information about the operation performed.

-v, --version

The **--version** option displays version information for the installed software.

EXAMPLES

To show the current mode:

```
adlicense
License mode: licensed
```

AUTHOR

Centrify Corporation

SEE ALSO

adjoin(1), adleave(1), adinfo(1)

NAME

admanagelocal - Display information for managed local accounts and trigger reload of managed local accounts.

SYNOPSIS

admanagelocal [--status, -s] [--reload, -R [--force, -f] [--profileonly, -p]] [--list, -l <all, visible, remove> < --user, -u>|<--group, -g>]

DESCRIPTION

admanagelocal - The **admanagelocal** command allows you to list currently managed local accounts, get status of local account management, and force reload of local accounts from Active Directory.

OPTIONS

You can use the following options with this command:

-s, --status
Check if management of local account is currently enabled or disable in UNIX agent. If Unix agent is not running, get the value from centrifydc.conf, at the same time 156 and 157 code is returned for Enable and Display status correspondingly.

-R, --reload
Sync local user, local group file and APU list with information in Active Directory. This should fail with error if UNIX agent is disconnected or not running, or local account management is disabled.

-f, --force
Use with --reload option. Force reload of managed local user, local groups from Active Directory, regardless if AD contain newer information or not, and update local passwd/group. This will fail with error if UNIX agent is disconnected or not running, or local account management is disabled.

-p, --profileonly
Use with --reload option. Reload the local user profile, local group profile only.

-l, --list <all, visible, remove>
Use in conjunction with --user or --group option to list local users or local groups. Each of the entries display is in the file native format. User can specify what type of local account to list, and acceptable values are:
visible: local profile accounts that are visible in the computer
remove: local accounts that are marked for removal in the computer
all: complete list of local accounts currently cached in UNIX agent

This should fail with error if UNIX agent is not running, or local account management is disabled

-u, --user
Use with --list, when specify, return local user information

-g, --group
Use with --list, when specify, return local group information

-V, --verbose
Display verbose step by step information to help debug problem.

It also log debug log messages to system log.

-v, --version
Display version information for the installed software

-h, --help
Print this help information and exit

EXAMPLES

To get the status of local account management, type:

```
admanagelocal --status
```

To get the all local users:

```
admanagelocal --list all --user
```

AUTHOR

Centrify Corporation

NAME

admigrate − migrate a classic zone to a hierarchical zone.

SYNOPSIS

admigrate −in *classicZone* −z *targetZone* [−hz *parentZone*] −config *filename* [−f] [−users] [−groups] [−nismaps] [−privileges] [−v] [−n]

DESCRIPTION

The **admigrate** command allows you to migrate a classic zone to a hierarchical zone. You can migrate a classic zone to a new peer hierarchical zone, or you can specify a parent zone for the migration. When you specify a parent zone, **admigrate** puts profile data from the source zone into the new parent zone, and override data, groups, roles and rights, and NIS maps into a new child zone. You can run **admigrate** multiple times and specify the same parent zone to migrate multiple classic zones to child zones of a single parent.

The authorization model differs between classic zones and hierarchical zones. For classic zones, a user with a profile in a zone is automatically granted login access to all computers joined to the zone. In hierarchical zones, a user with a profile in a zone must be assigned to a role with login rights and PAM access rights before being able to login to a computer joined to a zone. To support this model, **admigrate** creates two new roles:

− **login_at_roles** assigns the UNIX system rights Password login... and Nonpassword login. It does not assign Login with non−Restricted Shell because the user may be assigned to a restricted shell.

− **login_all_apps** assigns the login−all PAM right, which grants access to all PAM applications. It does not assign any UNIX system rights.

All users are added to the login_all_apps role so if they are granted login rights, they have access to all PAM applications, which is the default for users in classic zones. If PAM access rights are restricted by a role assignment, the restricted role assignment will override the rights granted by login_all_apps. See the *Administrator's Guide for Linux and UNIX* for details about how data is migrated from a classic zone to a hierarchical zone.

By default, **admigrate** migrates users, groups, role and right definitions, role assignments, and NIS maps from the classic zone, to the specified hierarchical zone. You can specify a subset of data by using one or more of the −users, −groups, −privileges, or −nismaps options.

When migrating right and role data, admigrate runs a series of checks to verify that none of the names from the classic zone will conflict after migration. If admigrate finds conflicts, it issues an error message (and quits without creating the new zone) or a warning message (and completes the migration), depending on the type of error.

If you specify the **−n option,** admigrate will perform the name checks, and issue an error message if conflicts are find, but will complete the migration and create the new zone even with conflicting name errors. You should rename conflicting roles in the new zone after migration is complete.

The admigrate command performs the following checks:

− Verifies that no restricted environment command has the same name as a privileged command because after migration they will be in the same namespace (Commands) and will conflict. The admigrate command will exit with an error if there are conflicts. You must rename one of the rights before running **admigrate** again.

− Verifies that no PAM rights are named "login−all", which is a predefined PAM right in a hierarchical zone. The admigrate command will exit with an error if there is a conflict. You must rename the right before running **admigrate** again.

− Verifies that no roles are named "UNIX Login", "listed", "login_at_roles", or "login_all_apps", because these are predefined role names in a hierarchical zone. If conflicting names are found, admigrate will rename the role by appending the objectGUID attribute to the name, issue a warning message, and complete the migration to the new zone.

− Checks whether the migrated names for PAM applications contain special characters (other than alphanumeric, space, underscore (_), or dash (−). The migrated names are based on the value (application name) for the PAM application, not on the user−defined name. However, if the value contains an illegal special character, **admigrate** continues to run but issues a warning and uses the user−defined name rather than the value.

OPTIONS

You can use the following options with this command:

−in classicZone
Specify the distinguished name of the classic zone to migrate. This parameter is required.

−z targetZone
Specify the distinguished name of the new zone. This parameter is required.

−hz parentZone
Specify a parent zone for the migration. The specified zone must be an existing zone.

When you specify this option, **admigrate** creates the zone named by the −z option as a child zone of this parent zone. You may run **admigrate** as many times as necessary and specify the same parent zone each time to migrate multiple classic zones to a set of child zones of the same parent zone.

−config filename
Specify a configuration file that you created to use with the migration. The configuration file is primarily useful to specify bind information if you are migrating zones from domains that are different from the target zone's domain.

This file is a tcl (text) file that gets sourced.

For example, the file could contain bind calls, such as the following:

```
bind acme.com administrator {myP@$swd}
bind −write eng.acme.com administrator {@lt!pas$}
```

−f Overwrite the target zone if it already exists. If the specified zone already exists and you do not specify the −f option, the

admigrate command exits unsuccessfully.

−users
Migrate only user data to the new zone.

−groups
Migrate only group data to the new zone.

−privileges
Migrate only right and role definitions and role assignments to the new zone.

−nismaps
Migrate only NIS maps to the new zone.

−n Prevent name conflicts from aborting the migration.

When migrating right and role data, admigrate runs a series of checks to verify that none of the names from the classic zone will conflict after migration. If conflicts are found, some checks return a warning message and some an error message. By default, if a name conflict error is returned, **admigrate** terminates without creating a new zone.

If you specify the **−n** option, admigrate will still issue an error message when conflicts are found, but will finish the migration and create the new zone. After the migration is complete, you should rename conflicting names in the new zone.

−v Print verbose information while the command runs.

EXAMPLES

The following command migrates the classic zone "finance" to a new hierarchical zone of the same name and creates this zone as a child zone of the parent zone "global"; it uses the bind credentials in the ~/admigrate.txt file, and outputs verbose information to the migrate_finance.txt file.

```
/usr/share/centrifydc/adedit/admigrate \
−in "cn=finance,cn=zones,ou=unix,dc=acme,dc=com" \
−z "cn=finance,cn=global,cn=zones,ou=unix,dc=acme,dc=com" \
−hz "cn=global,cn=zones,ou=unix,dc=acme,dc=com" \
−config ~/admigrate.txt \
−f −v >migrate_finance.txt
```

AUTHOR

Centrify Corporation

SEE ALSO

For related information, see the following command reference sections:

adchzone(1)

NAME

adnisd − control the operation of the Centrify DirectControl Network Information Service.

SYNOPSIS

```
adnisd [−d] [−f] [−v]
```

DESCRIPTION

The **adnisd** process is a daemon that enables a computer where the DirectControl Agent is installed to receive and respond to NIS client requests. On most platforms, it is started from an init.d control script (on Solaris 10 or later, the daemon is controlled through the Solaris Service Management Facility).

OPTIONS

You can use the following options with this command:

−d The **−d** option runs the **adnisd** process in the foreground to allow debugging operation.

−f The **−f** option flushes cached data before starting the **adnisd** process to force information to be reloaded from Active Directory.

−v The **−v** option displays version information for the installed software.

EXAMPLES

To flush the cache when the Centrify DirectControl Network Information Service starts:

```
adnisd −f
```

ENVIRONMENT CONFIGURATION PARAMETERS

The following configuration parameters can be set in the centrifydc.conf file to control **adnisd** operation.

log.adnisd Specifies the logging level for the Centrify DirectControl Network Information Service. The default logging level is the logging level set for the log configuration parameter or INFO if neither parameter is defined in the configuration file.

log.adnisd.netgroup
Specifies the logging level for netgroup processing of the Centrify DirectControl Network Information Service. The default logging level is the logging level set for the log.adnisd parameter if that parameter is defined. This parameter value can be set to DEBUG to log netgroup diagnostics or to INFO to suppress messages.

You can also set lower−level logging for netgroup processing using the following parameters

log.adnisd.netgroup.syntax Syntax warnings and errors for netgroup processing. The default value is the value defined for the log.adnisd.netgroup parameter log.adnisd.netgroup.inv Inversion processing. The default value is the value defined for the log.adnisd.netgroup parameter. This parameter value can be set to DEBUG to log netgroup diagnostics or to INFO to suppress messages.

logger.facility.adnisd

Specifies the syslog facility to use for logging adnisd operations. This parameter enables you to log adnisd messages using a different syslog facility than the facilities used for logging general adclient messages or adclient audit messages. This parameter’s value can be any valid syslog facility. For example, you can set this parameter to log messages to auth, authpriv, daemon, security, or localn facilities. The default is the auth facility.

nisd.domain.name

Specifies the NIS domain name for the adnisd process to use when communicating with NIS clients.

For example, to specify that you want to use euro−all as the NIS domain name in the zone named Europe−00−Zone, you can set this parameter as follows: nisd.domain.name: euro−all

If this parameter is not defined in the configuration file, the zone name is used by default.

nisd.exclude.maps

Specifies the name of the NIS maps you want to prevent the NIS service from using in response to NIS clients. This parameter enables you to exclude specific maps rather than explicitly specifying the maps you want to make available. For example, if you have a large number of automount maps or other network information that you want to make available to NIS clients but do not want to use agentless authentication, you can use this parameter to exclude the passwd and group maps but respond to automount or netgroup requests.

To use this configuration parameter, you must add the parameter name to the /etc/centrifydc.conf configuration file, then define its value. The parameter value must be a list of valid NIS map names, separated by spaces. For example: nisd.exclude.maps: group passwd

NOTE: This parameter excludes the named map and all derived maps. For example, if you specify group, the derived maps, group.byname, and group.bygid, are excluded.

If this parameter is not defined in the configuration file, all NIS maps found in Active Directory are retrieved and available for service.

NOTE: This configuration parameter overrides the setting of the nisd.maps parameter. If the same map is specified for both the nisd.exclude.maps and nisd.maps parameters, the map is excluded.

nisd.largegroup.name.length

Specifies the maximum number of characters to use in group names when groups with a large number of members

are split into multiple new groups. Because some devices that submit NIS requests have limitations on the length of group names, you can use this parameter to specify the maximum length for group names.

When the adnisd process splits the group membership for a large group into multiple smaller groups, it truncates the original group name as needed to append the suffix defined in the nisd.largegroup.suffix parameter and not exceed the number of characters specified by this parameter. For example, if you have a large group named worldwide−all−corp, and have defined the suffix string as "−all" and the maximum length for group names as 10, when the worldwide−all−corp group membership is split into multiple groups, the groups are named as follows:

world−all1

world−all2

world−all3

world−all3

For example, to set the maximum length for group names to 20 characters:

nisd.largegroup.name.length: 20

If this parameter is not defined in the configuration file, the maximum group name length is 1024 characters by default.

nisd.largegroup.suffix

Specifies the suffix string or character to use in group names when automatically splitting up a group with a large number of members.

Because group.bygid and group.byname NIS maps can often contain membership lists that exceed the 1024 limit for how much NIS data can be served to clients, the adnisd process automatically truncates the membership list when this limit is reached. To allow the additional membership data to be retrieved, you can configure the Centrify DirectControl Network Information Service to automatically split a large group into as many new groups as needed to deliver the complete membership list.

If you specify any value for the nisd.largegroup.suffix parameter, you enable the adnisd process to automatically split a large group into multiple new groups. When a group’s data size exceeds 1024 data limit, a new group is created. The new group name is formed using the original group name, followed by the string defined for the nisd.largegroup.suffix parameter and ending in a number that represents the numeric order of the new group created.

For example, if you have a large group named performix−worldwide−corp, and have defined the suffix string as "−all" and the maximum length for group names as 10, when the performix−worldwide−corp group membership is split into multiple groups, the groups are named as follows:

performix−worldwide−corp−all1

performix−worldwide−corp−all2

performix−worldwide−corp−all3

performix−worldwide−corp−all4

All of the new groups have the same group identifier (GID) as the original group. If the new group names would exceed the maximum length for group names on a platform, you can use the nisd.largegroup.name.length parameter to set the maximum length for the new groups created.

If this configuration parameter is not set, the adnisd process truncates the group membership list such that each group entry is under 1024 characters.

nisd.maps

Specifies the name of the NIS maps currently available for NIS service. When the adnisd daemon connects to Active Directory, it retrieves the list of NIS maps available for the local computer’s zone, creates a local map data store, and updates this configuration parameter, if necessary, to indicate the maps retrieved. If any NIS client requests a map that is not in the list specified by this parameter, the daemon refuses the request.

The parameter value must be a list of NIS map names. If the parameter is included in the configuration file but no value is set, no maps are retrieved from Active Directory or available for service.

For example, to make the netgroup maps available, but no other maps, you can set this parameter as follows:

```
nisd.maps: netgroup,netgroup.byhost,netgroup.byuser
```

NOTE: You must specify all maps, including the derived maps.

If this parameter is not defined in the configuration file, all NIS maps found in Active Directory are retrieved and available for service.

nisd.maps.max

Specifies the number of alternate sets of NIS maps to retain. A new set of NIS maps is normally created when adnisd switches to an alternate domain controller. Keeping these alternate sets of maps allows Centrify DirectControl Network Information Service to more efficiently switch between domain controllers.

The parameter value must be an integer greater than zero. The default is 2 map sets. For example:

```
nisd.maps.max: 2
```

nisd.net_addr

Sets the IP address the adnisd process uses for the NIS client socket. For example, the following sets the IP address to 192.168.212.11:

```
nisd.net_addr: 192.168.212.11
```

On systems with multiple Ethernet interfaces, adnisd configures RPC to the first interface. If an NIS client is trying to communicate on a different interface, adnisd will not receive the request.

Before creating sockets, adnisd reads centrifydc.conf file to see if an IP address and TCP and UPD ports are specified. If not, it uses localhost and random port numbers assigned by the operating system.

Use the nisd.port.udp and nisd.port.tcp parameters to complete the NIS port assignment.

nisd.passwd.expired.allow

Specifies whether a user with an expired Active Directory password should be allowed to log on to computers authenticated through NIS requests. The parameter value can be set to true or false.

By default, when a user’s Active Directory password expires the password hash field in the passwd NIS map is replaced by two exclamation marks (!!), and the user is not allowed to log on to the local NIS client computer without first logging on to a Windows computer or a DirectControl−managed computer running adclient to update the expired password. You can use this parameter to allow the user to log on locally using the expired password.

If you set the parameter value to true, users with an existing password hash in the passwd map generated from Active Directory do not have their password hash replaced by the exclamation marks and they can continue to log on using the expired password until they update their password in Active Directory. Once they update their password in Active Directory, in the NIS map is updated with a new password hash and users can log on with the new password. If a user never updates the Active Directory password by logging on to a Windows or DirectControl−managed computer, however, the user’s expired password may be used indefinitely.

The default value for this parameter is false. For example:

```
nisd.passwd.expired.allow: false
```

nisd.port.tcp

Sets the TCP port number the adnisd process uses to create the socket for NIS client communications. For example, the following sets the TCP port to 2556:

```
nisd.port.tcp: 2556
```

By default, no port number is specified. If you do not specify the port number, the operating system assigns a random port number.

Use the nisd.port.udp and nisd.net_addr parameters to complete the NIS client socket configuration.

nisd.port.udp

Sets the UDP port number the adnisd process uses to create the socket for NIS client communications. For example, the following sets the UPD port to 2555

```
nisd.port.udp: 2555
```

By default, no port number is specified. If you do not specify the port number, the operating system assigns a random port number.Use the nisd.port.tcp and nisd.net_addr parameters to complete the NIS client socket configuration.

nisd.securenets

Specifies a list of one or more subnets from which the daemon will accept NIS requests. You use this parameter to restrict access to the Centrify DirectControl Network Information Service by IP address. NIS requests that do not come from the IP addresses specified in this configuration parameters are refused by the asnisd daemon.

NOTE: You do not need to specify the local IP address for this parameter. The Centrify DirectControl Network Information Service will always accept local NIS client requests.

The parameter value must include both the specific IP address or subnet and the subnet mask, separated by a forward slash. For example:

```
nisd.securenets: 192.168.111.0/255.255.255.0
```

You can specify multiple IP addresses by separating each IP address−subnet mask pair with a comma or a space. For example:

```
nisd.securenets:
192.68.11.0/255.255.255.0,192.147.10.0/255.255.255.0
```

If this parameter is not defined in the configuration file, only local NIS client requests are accepted by the asnisd process.

nisd.server.switch.delay

Specifies how long, in seconds, to wait before loading maps from a backup domain controller when the connection to the primary domain controller is lost. If the Centrify DirectControl Network Information Service is unable to connect to its primary Active Directory domain controller, it will respond to NIS client requests using information in the local cache until the switch to the backup domain controller is complete.

The parameter value must be an integer equal to or greater than zero. If the value is zero, then the delay is disabled. For example, to set the delay period to 2 hours:

```
nisd.server.switch.delay: 7200
```

If this parameter is not defined in the configuration file, the default delay for switching to the backup domain controller is ten minutes (600 seconds).

nisd.startup.delay

Specifies the maximum number of seconds that the adnisd

process should wait before responding to NIS client requests.

While adnisd retrieves and generates its NIS maps, it does not respond to client requests for the maximum number of seconds specified by this parameter. At the end of the startup delay time, adnisd will respond to NIS client requests whether all maps are loaded or not. Therefore, setting this parameter enables the adnisd process to begin responding to NIS clients requests before all NIS maps are loaded or created. You should be aware, however, that if the delay time is reached before all of the NIS maps are available, NIS clients may receive partial or empty answers to their requests.

NOTE: If all of the NIS maps are loaded or created in less time than specified by this parameter, adnisd will begin responding to NIS requests without any startup delay.

By default, the maximum startup delay is 180 seconds. If you set this configuration parameter to zero, the adnisd process will only respond to NIS client requests after all NIS maps have been loaded or created. Therefore, in most cases, the parameter value should be a positive integer. For example, to set the startup delay to two minutes, you would set the parameter value to 120:

```
nisd.startup.delay: 120
```

nisd.threads

Specifies the maximum number of threads to allocate for processing NIS client requests.

The parameter value must be a positive integer within the valid range of 1 to 200. If you want to increase or decrease the number of threads used, you should stop the adnisd process, modify this parameter and save the configuration file, then restart the adnisd process.

The default value for this parameter is 4 threads. For example:

```
nisd.threads: 4
```

nisd.update.interval

Specifies the interval, in seconds, that the adnisd daemon waits between connections to Active Directory. At each interval, the adnisd daemon connects to Active Directory, gets the latest NIS maps for the local computer’s zone, and updates its local NIS map data store.

The parameter value must be an integer equal to or greater than zero. If the value is zero, then the update interval is disabled and the local NIS map data store is not updated. For example, to set the interval for getting NIS maps to 1 hour:

```
nisd.update.interval: 3600
```

If this parameter is not defined in the configuration file, the default interval is 30 minutes (1800 seconds).

AUTHOR
Centrify Corporation

NAME
adobfuscate − obscure sensitive data in a log file, such as email addresses, hostnames, and usernames

SYNOPSIS
adobfuscate [−−both] [−−logfile *filename]* [−−mapfile *filename]* [−−outputfile *filename]* [−−obfuscate] [−−patternfile *filename]* [−−verbose]

DESCRIPTION
The **adobfuscate** command allows you to obscure sensitive data in a log file, such as email addresses, hostnames, and usernames, before sending the file to Centrify for analysis. You create a pattern file using regular expressions to identify specific patterns in the file. The command reads the pattern file and replaces items matched by the patterns with generic values.

The **adobfuscate** command operates in two passes. The first pass searches for patterns (as defined in the pattern file) in the log file and creates a map file that contains the specific values to be hidden, as well as a unique token to replace each one. For example, in the pattern file you can search for host names using regular expressions to identify items to hide. In the map file, **adobfuscate** creates a list of specific host names and replacement value tuples. For example:

```
centrify.com    hostcom_0
ajax.com        hostcom_1
```

The second pass applies the value−token tuples in the map file to the log file, replacing each instance of the value with its corresponding token. For example, each instance of **centrify.com** in the log file is replaced by **hostcom_0.**

By default, the sanitized log file is written to obfuscate.txt in the directory in which you run **adobfuscate.** You can use the **−−outputfile** option to specify a different file name or directory.

By default, **adobfuscate** performs the first pass only, although you can use the **−−both** option to perform both. Once you create a map file, you can edit it to add other known host names, email addresses or other information. After you have identified all sensitive names that might be in a log file, you can run this map file against any log file without performing the first pass each time.

OPTIONS
You can use the following options with this command:

−b, −−both
The *−−both* option performs both passes of **adobfuscate.** The first pass searches the log file for patterns specified in the pattern file and creates a map file that contains values to be replaced and the token to replace them with. The second pass reads the map file and replaces the patterns in the log file with the replacement token.

When you specify the **−−both** option, the replacement values created by pass one are used during pass two, rather than read from a map file. If you do not specify the **−−both** option, only pass one is performed.

-f, --logfile filename
The *filename* specifies the input log file. It must be a text-based file in which lines are separated by the newline character.

Note Although the purpose of this command is to hide sensitive information in log files generated by Centrify commands, you can specify any valid text file. The default input file is log.txt.

-l, --outputfile filename
The *filename* specifies the output log file. The default output file is obfuscate.txt in the directory in which you run **adobfuscate.**

-m, --mapfile filename
The *filename* specifies the map file to create, or use, depending on the pass you are running. When you run only the first pass of **adobfuscate** , this option specifies the map file to create.

If you run only the second pass of this command by using the **--obfuscate** option, this option specifies the map file to apply to the log file.

Note If you use the **--both** option to run both passes, you do not need to specify a map file because the command creates replacement values during the first pass, and applies them to the log file during the second pass. The map file contains a list of lines, each with a value and replacement token, separated by a tab. For example:

```
centrify.com      hostcom_0
ajax.com          hostcom_1
rdavis@ajax.com   email_1
```

The default input map file is map.txt.

-o, --obfuscate
The **--obfuscate** option runs the second pass of the operation only. The second pass reads the replacement values from the specified map file and replaces matching values in the specified log file with the appropriate tokens. The default input file is **log.txt.** The default map file is **map.txt.**

-p, --patternfile filename
The *filename* specifies the input pattern file to use. The pattern file contains regular expressions to find sensitive information, such as email addresses, and host names, to replace with generic tokens. The default pattern file is: **/etc/centrifydc/adobfuscate.conf.** You can use this file as-is, or use it as a template to create your own pattern file.

-v, --verbose
The **--verbose** option prints verbose information while the command runs. Specify multiple **--verbose** options to increase the verbosity level. The maximum is 2.

EXAMPLES

Using adobfuscate command is a multi-step process:

1. Create a pattern file to identify the types of names to hide in the log file. Centrify provides a default pattern file that you can use as-is, or use as a template to create your own pattern file.

2. Run the first pass of adobfuscate, and specify the pattern file to create a map file that contains all the specific names to replace as well as a replacement value for each name.

3. Run the second pass of adobfuscate, and specify the map file to apply the replacement values to each specified name in the log file. The following example steps you through this process.

Creating a pattern file

In the pattern file, use regular expressions to identify sensitive names that you want obscured in the log file. Each line in the pattern file uses the following syntax:

action reg-expr-pattern repl-token

where:

action is one of the following:

⊕ **match** - Replaces any items that match the specified pattern.

⊕ **exclude** - Keeps the item even if it matches the specified pattern.

reg-expr-pattern is a regular expression pattern to identify sensitive names in the log file, such as email addresses and host names.

repl-token is the token to replace names of each type in the log file. For example, specific email addresses are replaced by **email_n** and host names by **hostcom_n,** and so on.

The easiest way to create a pattern file is to modify the sample file provided in this location: **/etc/centrifydc/adobfuscate.conf** The following shows the pattern matching definitions from this file:

```
#You can define your own sensitive data by using the following format.
#[action type]    [regular expression]   [substitute value]
#The action type has two optional values: match | exclude .
#Lines of ’match’ specify patterns that should be obfuscated and must
#have substitute value argument.
#Lines of ’exclude’ specify patterns that shouldn’t be matched.
match   /[A-Z0-9._%+-]+@[A-Z0-9.-]+.[A-Z]{2,4}/            email
match   /[A-Z0-9-]+[A-Z0-9.-]+.com/            hostcom
match   /[A-Z0-9-]+[A-Z0-9.-]+.net/            hostnet
match   /[A-Z0-9-]+[A-Z0-9.-]+.org/            hostorg
match   /[A-Z0-9-]+[A-Z0-9.-]+.test/           hosttest
match   /[A-Z0-9-]+[A-Z0-9.-]+.land/           hostland
```

Also in the file are patterns to exclude:

```
exclude /adclient..*/
exclude /adclient.pam.util/
exclude /adclient.session/
exclude /adfs.agent/
exclude /adfs.federationinfo/
exclude /adfs.request/
exclude /adfs.request.checktoken/
exclude /adfs.request.parsetoken/
exclude /adfs.test/
 ....
```

The purpose of this list is to retain specific items in the log file that may be useful for analyzing a problem, but would otherwise be obscured because they match one of the specified patterns. You should browse this list and remove any specific items that you do not want to appear in a log file you send to Centrify.

Running the first pass of adobfuscate

After you create a pattern file, you can run the first pass of the **adobfuscate** command to create a map file. For example:

```
adobfuscate −f /var/log/centrifydc.log −m myMap
```

This command example applies the default /etc/centrifydc/adobfuscate.conf pattern file to the centrifydc.log file and creates a map file called myMap. If the log file contains the following lines of text (modified for clarity):

```
WARN  <main> adnisd No NIS maps found on server win2k8.acme.com
DEBUG <fd:16 ldap fetch> base.bind.ldap win2mk.acme.com:389 fetch dn="" filter="..."
DEBUG <fd:16 get object> base.bind.ldap win2mk.acme.com:389 pagedSearch base="...)"
WARN  <main> adnisd No NIS maps found on server win2k8.acme.com
```

By applying the pattern file, the **adobfuscate** command creates a map file with the following entries:

```
win2k8.acme.com    hostcom_0
win2mk.acme.com    hostcom_1
```

The entry **base.bind.ldap** has the form of a host name, and would normally be replaced with a **hostname_n** token. However, the default pattern file contains the entry **exclude /base.bind.ldap** to exclude it, so it remains in the log file.

Running the second pass of adobfuscate

Now when you run the second pass of the command using the **−o** option and specify the map file you created in the previous step, the command obscures the host names in the log file. For example:

```
adobfuscate −f /var/log/centrifydc.log −m myMap −o
```

The sanitized log file contains the following modified entries:

```
WARN  <main> adnisd No NIS maps found on server hostcom_0
DEBUG <fd:16 ldap fetch> base.bind.ldap hostcom_1:389 fetch dn="" filter="..."
DEBUG <fd:16 get object> base.bind.ldap hostcom_1:389 pagedSearch base="..."
WARN  <main> adnisd No NIS maps found on server hostcom_0
```

As you can see, specific host names have been replaced with the generic host name tokens.

AUTHOR

Centrify Corporation

SEE ALSO

For related information, see the following command reference sections: addebug(1), adinfo(1)

NAME

adobjectrefresh − Refresh a user or group.

SYNOPSIS

adobjectrefresh [−g, −−group *groupname*] [−u, −−user *username*] [−i, −−ignoremembers] [−f, −−force] [−h, −−help] [−v, −−version] [−V, −−verbose]

DESCRIPTION

The **adobjectrefresh** command enables you to manually refresh a user or group on a local agent−managed UNIX computer that is connected to the domain. When you execute **adobjectrefresh** on a connected computer, the user or group that you specify is flushed from the Centrify cache and retrieved again from Active Directory. When you execute **adobjectrefresh** on a disconnected computer, the user or group that you specify is flushed from the Centrify cache, but is not retrieved from Active Directory.

OPTIONS

You can use the following options with this command:

−g, −−group groupname
The **−−group** option refreshes the specified group. This option cannot be used with the **−−user** option. The following group names are supported:
- unixname
- samAccountName
- canonicalName

−u, −−user username
The **−−user** option refreshes the specified user. This option cannot be used with the **−−group** option. The following user names are supported:
- unixname
- dn
- samAccountName
- userPrincipalName
- canonicalName

−i, −−ignoremembers
When refreshing a user, specify the **−−ignoremembers** option to refresh the user without also refreshing the groups to which the user belongs. When refreshing a group, specify the **−−ignoremembers** options to refresh the group without also refreshing the group’s members. If a user belongs to a large number of groups, or if a group has a large number of users, this option can improve performance significantly.

−f, −−force
The **−−force** option removes the specified user or group from the Centrify cache if adclient is not connected. If adclient is connected when you use this option, the user or group is refreshed from Active Directory after being removed from the cache. This option is required if adclient is not connected.

−h, −−help
The **−−help** option displays information about this command.

−v, −−version
The **−−version** option displays version information for the installed software.

−V, −−verbose
The **−−verbose** options displays detailed information about each operation as it is performed.

EXAMPLES

To refresh a user on a connected computer:

```
adobjectrefresh −u username
```

To flush a group from the Centrify cache on a disconnected computer:

```
adobjectrefresh −fg groupname
```

To refresh a group without refreshing the group's members on a connected computer:

```
adobjectrefresh −gi groupname
```

AUTHOR

Centrify Corporation

NAME

adpasswd − change the password for an Active Directory user.

SYNOPSIS

adpasswd [−−adminuser *adminuser[@domain]]* [−−adminpass *adminpassword]* [−−oldpass *oldpassword]* [−−newpass *newpassword]* [user[@domain] [−−validate] [−−version]

DESCRIPTION

The **adpasswd** command changes the password for an Active Directory user account. It can be used to change the password of the current user executing the command or to change the password of another Active Directory user. If you want to change the password for any Active Directory account other than your own, you must provide the user name and password of an administrative account with the authority to change that user's password.

If a *user@domain* is specified in the command line, you must provide an administrative user name and password for an Active Directory account with the authority to set passwords for other Active Directory users. If a *user@domain* is not specified in the command line, this command can only be used to change the password for the current user account. Because **adpasswd** allows a user to change his or her own password, you do not need to be logged in as root to run this command.

Note Changing a user's password with this command updates the user's Active Directory account. Once changed, the new password must be used for all activities that are authenticated through Active Directory, including logging on to the UNIX shell, logging on to Windows computers, and accessing applications on both UNIX and Windows.

OPTIONS

You can use the following options with this command:

−a, −−adminuser adminuser[@domain]
The *adminuser* identifies an Active Directory user account with sufficient rights to modify another Active Directory user account.

You must use the adminuser@domain format to specify the account if the administrative user is not a member of the host computer's current domain.

If you do not specify this option, the default is the Administrator user account.

−p, −−adminpass adminpassword
The *adminpassword* specifies the password for the Active Directory administrative account when changing another user's Active Directory password. If you do not provide the password at the command line, you are prompted to enter the password before the command executes. However, if **adpasswd** detects Kerberos credentials, it uses those for the command, and if these credentials are not sufficient, you receive an error message rather than a prompt for a password.

Note Specifying a password at the command line represents a security risk because the password can be retrieved while the command is running or from command history after the command has completed its execution.

−o, −−oldpass oldpassword

The *oldpassword* specifies the current password for the Active Directory user account. This option is only used when the user executing the command is trying to change the password for his own account. This option is ignored if the administrator is trying to change the password for another user account.

If you are trying to changing your own password and do not provide the current password at the command line, you are prompted to enter the old password before the command executes.

−n, −−newpass newpassword

The *newpassword* specifies the new password for the Active Directory user account. If you do not provide the password at the command line, you are prompted to enter the new password and confirm the new password by retyping it before the command executes. The new password must meet the Active Directory domain password policy requirements for length and complexity.

If this option isn't present, the command prompts for a new password.

Note Specifying a password at the command line represents a security risk because the password can be retrieved while the command is running or from command history after the command has completed its execution.

user[@domain]

This option specifies the Active Directory user account for the password change. You must use this option if you are changing another Active Directory user's account password. You should not use this option when changing your own account password. If a user name is not specified, the default is always the current user's account.

You must use the user@domain format to specify the account if the user is not a member of the host computer's current domain.

−V, −−validate

This option validate the new password meets complexity requirements.

−v, −−version

This option displays version information for the installed software.

EXAMPLES

In most cases, you use this command to change the password for your own account. The following command illustrates how to change the password for the current user account. It prompts for the old and new passwords because they aren't provided in the command:

```
adpasswd
Old password: xxx
New password: xxx
Repeat password: xxx
```

The following command illustrates changing the password for another user account, jane@acme.com, which is in a domain outside the host computer's own Active Directory domain. Because this example changes the password for another user, the command specifies an Active Directory administrative account, admin@acme.com, with the authority to change the password for Jane's account:

```
adpasswd −−adminuser admin@acme.com jane@acme.com
```

You are then prompted for the administrator password and the user's new password because these values aren't provided in the command line.

```
Administrator password: xxx
New password for jane@acme.com: xxx
Repeat password: xxx
```

AUTHOR

Centrify Corporation

SEE ALSO

For related information, see the following command reference sections: adjoin(1), adleave(1), adgpupdate(1), adinfo(1), addebug(1)

NAME

adquery − query Active Directory for information about users and groups

SYNOPSIS

```
adquery user|group [options] [username|groupname]
```

DESCRIPTION

The **adquery** command is provided for backward compatibility to enable you to query Active Directory for information about users and groups from the command line on a Centrify−managed computer. You can use this command to query information for classic or hierarchical zones. In most cases, however, you should use **adedit** commands or scripts to query Active Directory for information in hierarchical zones.

The options you can use depend on whether you are looking up user information or group information. You can look up information for a specific user or group or for all of the users or groups in a zone.

You can specify a single option in the command line to have the information returned as one value per line suitable for use in scripts. If you specify multiple options in the command line, the information returned is formatted in a list with field labels identifying each value.

QUERYING USER INFORMATION

You can use the **adquery user** command to look up one or more details about one or more specified users in Active Directory. If you don’t specify any users in the command line, the command lists all of the users in the zone.

The basic syntax for querying user information is:

```
adquery user [−admin user@domain ] [−−password password ]
[−−attribute attributename ] [−−home] [−−group] [−−groups]
[−−adgroups] [−−shell] [−−uid] [−−display] [−−gecos] [−−unixname]
[−−samname] [−−sid] [−−principal] [−−service] [−−canonical] [−−hash]
[−−acct−expire] [−−pwd−expired] [−−pwd−expire] [−−time−to−pwd−expire]
[−−pwd−nextchange] [−−pwd−lastchange] [−−locked] [−−disabled]
[−−enabled] [−−dn] [−−userWorkstations] [−−guid] [−−audit] [−−altse−
cid] [−−all] [−−dump] [−−cache−first] [−−separator char ] [−−list−
separator char ] [−−prefix] [−−mfa] [−−zap−groups] [−−extattr]
[−−version]
 [ username ]
```

You can specify the *username* in any supported format. If the user name includes any blank spaces, it should be enclosed by quotation marks. For example, if you want to specify an Active Directory account name consisting of a first name and a last name, you can type a command similar to the following:

```
adquery user −M −e "Jae Park"
```

All options, including **−−all,** return formatted attributes and values, with the exception of **−−dump,** which returns raw attributes and values, and **−−attribute,** which allows you to specify individual raw attributes. Raw attributes are the form in which attributes are stored internally in Active Directory or DirectControl, that is, without regard to readability. For example, the raw attribute for the account expiration date is a numeric string:

```
#adquery user −j |grep −i expires
accountExpires:129389472000000000
```

whereas, the formatted attribute shows a date field:

```
#adquery user − x
Sat Jan  8 00:00:00 2011
```

OPTIONS

You can use the following options with the **adquery user** command:

−b, −−attribute attributename
Display the value of the specified Active Directory or Direct−Control raw attribute. Use the **−−dump** option to see a list of raw attributes. The **−−all** option returns formatted attributes and values.

Note Attribute names are case−sensitive. Internal DirectControl attributes begin with an underscore character. You can specify multiple **−−attribute (−b)** options, in which case, the name of the attribute is returned along with the value. For example:

```
#−b cn
rajai davis
```

```
#−b cn −b sAMAccountName
cn:rajai davis
sAMAccountName:rdavis
```

−h, −−home
Display the specified user’s home directory or the home directory for all users in the zone.

−g, −−group
Display the specified user’s primary group identifier (GID) or the primary group identifier (GID) for all users in the zone.

−G, −−groups
List the UNIX−enabled groups the user is a member of.

−a, −−adgroups
List all of the Active Directory groups the user is a member of. Active Directory groups are listed by canonical name.

−s, −−shell
Display the user’s default shell.

−u, −−uid
Display the user identifier (UID) for the specified user or for all users in the zone.

−p, −−display
Display the displayName attribute for the user or for all users in the zone.

−o, −−gecos
Display the contents of the GECOS field for the user.

−n, −−unixname
Display the UNIX login name for the user.

−M, −−samname
Display the Active Directory logon name for the user.

-i, --sid
Display the Active Directory security identifier (SID) for the user.

-P, --principal
Display the Kerberos user principal name (UPN) for the user.

-S, --service
Display the Kerberos service principal name (SPN) for the user.

-C, --canonical
Display the Active Directory canonical name for the user.

-H, --hash
Display the UNIX password hash for the specified user if you are using password synchronization between Active Directory and DirectControl-managed computers.

You must be logged on as the root user or querying Active Directory for your own account information to retrieve the password hash.

-x, --acct-expire
Display the date the user account expires.

You must be logged on as the root user or querying Active Directory for your own account information to retrieve this information.

-y, --pwd-expired
Display whether the AD user account’s password is expired.

You must be logged on as the root user or querying Active Directory for your own account information to retrieve this information.

-w, --pwd-expire
Display the date the current password for the user account expires.

You must be logged on as the root user or querying Active Directory for your own account information to retrieve this information.

-Q, --time-to-pwd-expire
Display the number of day before password expires.

You must be logged on as the root user or querying Active Directory for your own account information to retrieve this information.

-c, --pwd-nextchange
Display the date after which the user may change their password.

You must be logged on as the root user or querying Active Directory for your own account information to retrieve this information.

-l, --pwd-lastchange
Display the date of the last password change for the user.

You must be logged on as the root user or querying Active Directory for your own account information to retrieve this

information.

-k, --locked
Determine whether the Active Directory account for the user is locked because of failed attempts to log on.

You must be logged on as the root user or querying Active Directory for your own account information to retrieve this information.

-d, --disabled
Determine whether the Active Directory account for the user has been disabled.

You must be logged on as the root user or querying Active Directory for your own account information to retrieve this information.

-e, --enabled
Determine whether the Active Directory account for the user has been enabled for UNIX access in the current zone.

-D, --dn
Display the distinguished name (dn) for the user.

-W --userWorkstations
List the value of the user’s Active Directory userWorkstations attribute, which specifies the machines from which the user may log into the domain. If the output is blank, the user is not restricted to a particular machine.

-B, --guid
Display the user’s guid in MSString format.

-t, --audit
Display the effective audit information of a user.

-I, --altsecid
Display the Alt-Security-Identities of a user.

-A, --all
List all of the information returned by the other command line options for the user.

-j, --dump
List all the raw attributes and values for the user.

-F --cache-first
Read data from the cache rather than from Active Directory. Only read from Active Directory if an object has expired.

-r, --separator char
Specify the character (*char*) to use as the separator character between an attribute name and its value. The default separator between attributes and values is a colon (:). For example:

```
jae:uid:525
```

-R,--list-separator char
Specify the character (*char*) to use as the separator character between values in a list. The default separator for values in a list is a comma (,). For example:

```
jae:unixGroups:unixdev,testexpe
```

−f, −−prefix
Add the UNIX user name as a prefix when returning single values. This option formats the information returned to include the UNIX user name when you are querying for a specific attribute, such as the user’s UID or display name.

This option is not necessary if you query for multiple attributes in the command line. If you query for multiple attributes, the information returned is formatted with the UNIX user name and a label identifying each attribute by default.

−m, −−mfa
Indicates whether the specified requires multi−factor authentication to log on.

−z, −−zap−groups
Force user’s group membership to expire and trigger update of user’s sysright.

−X, −−extattr
Display the list of extended attributes or the value of a specified extended attribute.

Note Extended attributes are only applicable on AIX computers.

You can use the keyword help to view a list of the supported extended attributes. For example:

```
adquery user −−extattr help
```

To look up the value of a specific extended attribute, include the name of the attribute in the command line. For example, to look up the value of the aix.rlogin extended attribute:

```
adquery user −X aix.rlogin jae
```

−v, −−version
Display version information for the installed software. You cannot use this command to query information

QUERYING GROUP INFORMATION

You can use **adquery group** command to look up one or more details about a specified group or multiple groups in Active Directory. If you don’t specify any groups in the command line, the command lists all of the groups in the zone.

The basic syntax for querying group information is:

adquery group [−admin *user@domain*] [−−password *password*] [−−attribute *attributename*] [−−members] [−−admembers] [sammembers] [−−gid] [−−required] [−−unixname] [−−samname] [−−sid] [−−canonical] [−−dn] [−−all] [−−dump] [−−extattr] [−−cache−first] [−−version] [−−separator *char*] [−−list−separator *char*] [−−prefix] [−−type] [*groupname*]

You must use the canonical format for the group name if specifying the Active Directory group name.

All options, including **−−all,** return formatted attributes and values, with the exception of **−−dump,** which returns raw attributes and values, and **−−attribute,** which allows you to specify individual raw

attributes. Raw attributes are the form in which attributes are stored internally in Active Directory or DirectControl, that is, without regard to readability. For example, the raw attribute for the group type is a numeric string:

```
#adquery group −j |grep −i type
dnsadmin:groupType:−2147483644.fi
```

whereas, the formatted attribute shows a name:

```
#adquery group − t
local security
```

OPTIONS

You can use the following options with the **adquery group** command:

−b, −−attribute attributename
Display the value of the specified Active Directory or DirectControl raw attribute. Use the **−−dump** option to see a list of raw attributes. The **−−all** option returns formatted attributes and values.

Note Attribute names are case−sensitive. Internal DirectControl attributes begin with an underscore character. You can specify multiple **−−attribute (−b)** options, in which case, the name of the attribute is returned along with the value. For example:

```
#−b cn
DnsAdmins

#−b cn −b sAMAccountName
cn:DnsAdmins
sAMAccountName:DnsAdmins
```

−m, −−members
List the UNIX name of members of the specified group or of all groups in the zone.

−a, −−admembers
List the Active Directory users who are members of the specified group or of all groups in the zone.

−s, −−sammembers
List the Active Directory users who are members of the specified group or of all groups in the zone, in the form **name@domainName.com.**

−q, −−required
Display whether membership in the specified group is required or not. For more information about required groups, see the **adsetgroups** man page.

−g, −−gid
Display the group identifier (GID) for the group or all groups in the zone.

−n, −−unixname
Display the UNIX group name for the group.

−M, −−samname
Display the Active Directory name for the group.

−i, −−sid
Display the Active Directory security identifier (SID) for the group.

−C, −−canonical
Display the Active Directory canonical name for the group.

−D, −−dn
Display the distinguished name (dn) for the group.

−A, −−all
List all of the information returned by the other command line options for the group.

If you use this option without specifying a group name, the command lists details for all of the groups in the zone.

−j, −−dump
List all the raw attributes and values for the group.

−X, −−extattr
List extended attributes for the specified group. You can use the keyword "help" with this option to display supported extended attributes.

−F −−cache−first
Read data from the cache rather than from Active Directory. Only read from Active Directory if an object has expired.

−r, −−separator char
Specify the character (*char*) to use as the separator character an attribute name and its value. The default separator between attributes and values is a colon (:). For example:

```
unixname:qa−euro
```

−R,−−list−separator char
Specify the character (*char*) to use as the separator character between values in a list. The default separator for values in a list is a comma (,). For example:

```
unixGroups:unixdev,testexpe
```

−f, −−prefix
Add the UNIX group name as a prefix when returning single values. This option formats the information returned to include the UNIX group name when you are querying for a specific attribute, such as the group GID or membership list.

This option is not necessary if you query for multiple attributes in the command line. If you query for multiple attributes, the information returned is formatted with the UNIX group name and a label identifying each attribute by default.

−t, −−type
Display the scope and group type for a specified group. The valid group types are:

− local security

− global security

− universal security

−v, −−version
Display version information for the installed software.

EXAMPLES

You can use **adquery** to return a specific value for a user or group or to list multiple details about a user or group. The format of the output depends on whether you specify a single attribute or multiple attributes on the command line. For example, if you want to see a complete list of details about the group unixdev, you would type:

```
adquery group −−all unixdev
```

This command returns the results for the unixdev group in the following format:

```
unixname:unixdev
gid:400
required:false
dn:CN=Unix Developers,CN=Users,DC=ajax,DC=org
groupType:global security
samAccountName:Unix Developers
sid:S−1−5−21−3619768212−1024502798−2657341593−1106
canonicalName:ajax.org/Users/Unix Developers
members:ajax.org/Users/Ashish Menendez,ajax.org/Users/Ben Waters,
ajax.org/Users/Monte Fisher,ajax.org/Users/Jae Kim,ajax.org/Users/Jay  Reynolds
ajax.org/Users/Pierre Leroy,ajax.org/Users/Rae Parker,ajax.org/Users/Zoe Green
unixMembers:ashish,ben,fisher,jae,jay,pierre,rae,zoe
```

Similarly, if you want to see a complete list of details about the user jae@ajax.org, you would type:

```
adquery user −−all jae@ajax.org
```

This command returns the results for the user in the following format:

```
unixname:jae
uid:409
gid:400
gecos:Jae Kim
home:/home/jae
shell:/bin/bash
dn:CN=Jae Kim,CN=Users,DC=ajax,DC=org
userWorkstations:phoenix1
samAccountName:jae
display:jae
sid:S−1−5−21−3619768212−1024502798−2657341593−1185
userPrincipalName:jae@AJAX.ORG
servicePrincipalName:
canonicalName:ajax.org/Users/Jae Kim
passwordHash:x
accountExpires:Never
passwordExpires:Thu Apr 12 15:21:04 2007
nextPasswordChange:Fri Mar  2 14:21:04 2007
lastPasswordChange:Thu Mar  1 14:21:04 2007
accountLocked:false
accountDisabled:false
zoneEnabled:true
unixGroups:unixdev,testexpe
memberOf:ajax.org/Users/Unix Developers,ajax.org/Users/Domain Users,
ajax.org/Performix/TestExpert Team
```

If you want to return only the canonical name for the qa−euro group, you would type:

```
adquery group −−canonical qa−euro
```

This command returns the results for the qa−euro group as an

unlabeled value. For example:
arcade.com/Users/QA Europe

If you want to return only the UID for the user rae@arcade.com, you would type:

```
adquery user −−uid rae@arcade.com
```

For example:

```
10003
```

To list the UNIX group names and GIDs for all of the groups in the current zone, you would type:

```
adquery group −−gid −−prefix
```

For example:

```
unixdev:400
oracle:700
qualtrak:800
performi:401
perform2:402
financeu:403
testexpe:404
integrit:405
```

AUTHOR

Centrify Corporation

SEE ALSO

adjoin(1), adupdate(1), adsetgroups(1)

NAME

adreload − force the Centrify UNIX agent (adclient) to reload configuration properties

SYNOPSIS

adreload

DESCRIPTION

The **adreload** command enables you to force the Centrify UNIX agent (adclient) to reload the configuration properties from the /etc/centrifydc/centrifydc.conf file and in other files in the /etc/centrifydc directory. Running this command enables changes made to the configuration properties to take effect without restarting the **adclient** process.

Note that you must have root privileges to run this command. Running **adreload** , however, does not reload the properties set with the following configuration parameters:

− auto.schema.search.return.max

− adclient.ldap.timeout

− adclient.ldap.socket.timeout

− adclient.udp.timeout

− adclient.clients.threads

− adclient.clients.threads.max

− adclient.use.all.cpus

− adclient.clients.listen.backlog

− adclient.dumpcore

For these configuration parameters, you must restart the **adclient** process for changes to take effect.

OPTIONS

You can use the following options with this command:

−h, −−help
The **−−help** option enables you to display the usage message.

EXAMPLES

To reload the configuration properties on a local computer after making changes, you would type a command similar to this:

```
adreload
```

ERROR CODES

This command returns the following exit codes:

0 Command executed successfully

2 Process not authorized

3 Reload failed

AUTHOR

Centrify Corporation

NAME

adreport − generate user, computer, command, assignment and role report from the database generated by addbloader.

SYNOPSIS

adreport −db *dbPath* −report user | computer | command | assignment | special_assignment | effective_assignment | role | effective_role [−filter *filter*] [−sep *csv* | *tab* | *char*]

DESCRIPTION

The **adreport** command generates a report from the database created by the addbloader command.

You must run **addbloader** to create a sqlite database containing information about a zone before you can run **adreport** to generate a report.

OPTIONS

You can use the following options with this command:

−db dbPath
Specify the path to the sqlite database created by the **addbloader** command.

−report user | computer | command | assignment | special_assignment | effective_assignment | role | effective_role
Specify whether to generate user, computer, command, assignment or role information. You can filter the information to display by using the optional −filter.

−filter filter
Specify a filter for the user, computer, command, assignment or role information to display. The filter for user report and all assignment related reports is based on user’s upn. The filter for computer report is based on computer’s DNS name. The filter for command report is based on command. The filter for all role related reports is based on role name. For all filters, using % for wildcard match.

−sep csv | tab | char
Specify whether to create a comma separated list, tab−separated list, or user−specified character list.

EXAMPLES

The following command generates a user report from the database file */tmp/user_report.*

```
/usr/share/centrifydc/adedit/adreport −db /tmp/user_report −report user
/usr/share/centrifydc/adedit/adreport −db /tmp/user_report −report user
−filter "chris%"
```

AUTHOR

Centrify Corporation

SEE ALSO

For related information, see the following command reference sections:

addbloader (1)

NAME

adreport2 − The next generation report to generate user, computer, command, assignment and role report from the database generated by addbloader.

SYNOPSIS

adreport2 −db *dbPath* −report *reportName* [−filter *filter*] [−value *value*] [−value2 *value2*] [−sep *csv* | *tab* | *char*]

DESCRIPTION

The **adreport2** command generates a report from the database created by the addbloader command.

You must run **addbloader** to create a sqlite database containing information about a zone before you can run **adreport2** to generate a report.

OPTIONS

You can use the following options with this command:

−db dbPath
Specify the path to the sqlite database created by the **addbloader** command.

−report reportName

The valid report name and the corresponding filter/value is one of following:

UserByAny −filter

UserByADUser −value

UserByComputer −value

UserByZone −value

UserByUname −value

UserByUid −value

UserByUserComputer −value −value2

CommandByAny −filter

CommandByName −value

CommandByRole −value

CommandByZone −value

CommandByComputer −value

CommandByADUser −value

CommandByCmd −value

CommandByUserComputer −value −value2

PAMByAny −filter

PAMByName −value

PAMByRole −value

PAMByZone −value

PAMByComputer −value

PAMByADUser −value

PAMByUserComputer −value −value2

AssignmentByAny −filter

AssignmentByADUser −value

AssignmentByRole −value

AssignmentByZone −value

AssignmentByComputerRole −value

AssignmentByPrincipalType −value

EffAssignmentByAny −filter

EffAssignmentByADUser −value

EffAssignmentByRole −value

EffAssignmentByZone −value

EffAssignmentByComputer −value

RoleByAny −filter

RoleByName −value

RoleByZone −value

EffRoleByAny −filter

EffRoleByName −value

EffRoleByZone −value

EffRoleByComputer −value

−filter filter
Specify a filter for the corresponding report. Filter is the general filtering condition to narrow the report results.

−value value
Specify a value for the corresponding report. For example, use zone name as value for RoleByZone report.

−value2 value2
Some report can have two filtering fields. Specify an additional value for the corresponding report. For example, use computer name as value2 for UserByUserComputer report.

−sep csv | tab | char
Specify whether to create a comma separated list, tab-separated list, or user−specified character list.

EXAMPLES

The following command generates a user report from the database file */tmp/user_report.*

```
/usr/share/centrifydc/adedit/adreport2 −db  /tmp/user_report  −report
UserByADUser

/usr/share/centrifydc/adedit/adreport2  −db  /tmp/user_report −report
UserByADUser −value "chris%"

/usr/share/centrifydc/adedit/adreport2 −db  /tmp/user_report  −report
UserByAny −filter "zone_name='Global' and user_upn like 'chris%'"
```

AUTHOR

Centrify Corporation

SEE ALSO

For related information, see the following command reference sections:

addbloader (1)

NAME

adrmlocal - reports and removes local user names that duplicate Active Directory user names

SYNOPSIS

```
adrmlocal [--interactive] [--commit] [--force] [--version]
```

DESCRIPTION

The **adrmlocal** command displays a report of users in both local user database, for example, the local user accounts defined in the /etc/passwd file, and Active Directory to allow you to check for duplicate user names. You can remove selected duplicate local user names interactively or remove all duplicate local users without prompting.

If you run this command with the **--interactive** option, the command prompts you to remove the local user account or skip each duplicate user, regardless of whether the user’s UID or GID in /etc/passwd matches the information for the user name in Active Directory.

If you run this command with the **--commit** option, the command removes duplicate users if there are not UID or GID conflicts but prompts you to remove or skip local users that have UID or GID conflicts.

If you run this command with the **--force** option, the command removes all duplicate local users whether without prompting.

To delete local user accounts in a NIS domain, you should run the **adrmlocal** command on the NIS master server. After running the command, you must update the NIS passwd maps to make the updated information available to your NIS servers.

OPTIONS

You can use the following options with this command:

-i, --interactive
The *--interactive* option prompts you interactively for confirmation that you want to remove the duplicate local user account before performing the delete operation.

-c, --commit
The *--commit* option removes duplicate local users if the UID and GID is the same in the local database and Active Directory. If the UID or GID for a local user conflicts with the information stored in Active directory, this option prompts you to determine whether a local user account should be deleted or not.

-f, --force
The *--force* option removes all duplicate local user names without prompting even if there are UID or GID conflicts.

-v, --version
The *--version* option displays version information for the installed software.

EXAMPLES

To report duplicate user names that exist in both the local user database and Active Directory and respond to each duplicate interactively, you would type:

```
adrmlocal --interactive
```

This command displays a summary of the conflicts found, then prompts

you to decide whether each duplicate user should be deleted. For example:

```
3 local user(s) that are duplicated with AD users:
adam:uid(505):gid(503):ADuid(10001):ADgid(10000) Conflicted with AD
chin:uid(506):gid(504):ADuid(10009):ADgid(10000)  Conflicted with AD
liz:uid(507):gid(505):ADuid(10005):ADgid(10000) Conflicted with AD

adam:uid(505):gid(503):ADuid(10001):ADgid(10000) Conflicted with AD
Delete local user adam ? (Yes/No)
```

AUTHOR

Centrify Corporation

NAME

adsec − manage IPsec and display information about the IPsec configuration.

SYNOPSIS

adsec [--certs] [--debug [on | off]] [--disable] [--enable] [--flush [sa | sp | all]] [--ikeinfo] [--info] [--policy] [--reload] [--reset] [--stop] [--unconfig] [--sainfo] [--spinfo] [--status] [--support] [--version]

DESCRIPTION

The **adsec** command enables you to get information about and manage the IPsec configuration on a UNIX computer.

OPTIONS

You can use the following options with this command:

-c, --certs

The **--certs** option displays information about the certificates stored in the **/var/centrify/net/certs** directory. This option also performs a basic test to verify that the public key information stored in each certificate matches the private key data stored in the associated key file.

-g, --debug [on | off]

The **--debug** option turns IPsec debugging on or off. The default, if you do not specify this parameter, is off. Debugging information is sent to the **/var/log/centrify-racoon.log** file. Turning on debugging with this parameter, sets **racoon** debugging to verbose and updates the /etc/sysconfig/centrify.racoon configuration file with changes to RACOON_OPTS.

-d, --disable

The **--disable** option suspends processing of group policies to allow you to make manual changes to IPsec. Note that manual changes are not merged into the IPsec configuration and may be overwritten when group policy processing is re-enabled.

-e, --enable

The **--enable** option enables the processing of group policies. By default, group policy processing is enabled. Use this option to re-enable group policies after suspending them with the **--disable** option.

-f, --flush sa | sp | all

The **--flush** option flushes the Security Authority (SA) database, the Security Policy (SP) database, or both (all). If you do not specify an option, it flushes both databases. These databases hold the security authority and security policy information. If these policies are not working as expected, for example, if they are restricting traffic with the domain controller, flushing the policies allows easy recovery.

-K, --ikeinfo

The **--ikeinfo** option displays the state of IKE negotiation with its peers.

-i, --info

The **--info** option displays the state of group policy management and whether IPsec is enabled or disabled on the computer.

-p, --policy

The **--policy** option prints a readable version of the IPsec

configuration. It includes any errors or warnings that were generated while IPsec was generating the IPsec configuration files based on the IPsec group policy settings.

-l, --reload

The **--reload** option flushes the Security Authority and Security Policy databases, then reloads the information from the racoon spd.conf file.

-r, --reset

The **--reset** option restarts the IKE daemon.

-u, --stop

The **--stop** option stops the IKE daemon.

-U, --unconfig

The **--unconfig** option removes the configuration settings. This option is primarily used by the package scripts so that the package can be uninstalled. If you run the adsec --unconfig command by mistake, you can run the adgpupdate command to reconfigure the DirectSecure service.

-A, --sainfo

The **--sainfo** option lists information about the active security associations.

-P, --spinfo

The **--spinfo** option lists security policy information, including source and destination addresses, direction, protocols to control, and the rules to apply.

-s, --status

The **--status** option shows the status of the IKE daemon.

-t, --support

The **--support** option generates information that can be used by support to troubleshoot the IPsec configuration, including:

- A tar of the IKE configuration file

- The current Security Policy Database (SPD) configuration

- The IKE log file.

-v, --version

The **--version** option displays the version of IPsec.

EXAMPLES

To flush the Security Authority database:

```
adsec -f sa
```

AUTHOR

Centrify Corporation

SEE ALSO

For related information, see the following command reference sections: adpol(1)

NAME

adsendaudittrailevent − Specify audit trail events to send to the audit trail target.

SYNOPSIS

adsendaudittrailevent −t|−−type *event_type_name* −i|−−info *content* [−v|−−version] [−h|−−help]

DESCRIPTION

The **adsendaudittrailevent** command allows you to specify audit trail events to send to the audit trail target. The audit trail target can be syslog, the Centrify auditing service, or both.

If the **adsendaudittrailevent** command executes successfully, a message is displayed showing the event information that was sent to the audit trail target. If the **adsendaudittrailevent** command fails, an error message is displayed.

OPTIONS

You can use the following options with this command:

−t, −−type event_type_name
Specify the type of event to send to the audit trail target. The supported event type is **tkt_id** (trouble ticket). This option is required.

−i, −−i information_content
Specify event information to send to the audit trail target. For example, if you are sending information about a trouble ticket event, type the trouble ticket ID here. The content that you specify here cannot exceed 444 characters. Events that are sent to syslog are subject to additional truncation if additional characters are added by syslog. This option is required.

−v, −−version
Include the Centrify Infrastructure Services version number in the event information that is sent to the audit trail target.

−h, −−help
Display help information.

EXAMPLES

To send information about trouble ticket 123qwe to the audit trail target, you would type the following command:

```
adsendaudittrailevent −t tkt_id −i 123qwe
```

If this command executes successfully, an entry for trouble ticket 123qwe is created in the audit store database, and a message similar to the following is displayed:

```
adsendaudittrailevent[13172]: INFO  AUDIT_TRAIL|Centrify Suite|dzdo|1.0
|2|Trouble ticket entered|5|user=user1@aucean2k8.test pid=13166
utc=1383217637082 status=SUCCESS ticket=123qwe
```

AUTHOR

Centrify Corporation

Reference"

NAME

adsetgroups − view or change the list of groups available for the current user.

SYNOPSIS

adsetgroups [−−all] [−−list] [−−required] [−−optional] [−−samname] [−−number] [−−remove] [−−clear] [−−command <cmd>] [−−init] [−−save] [−q, −−quiet] [−−version] [−−exec <cmd>] *group*

DESCRIPTION

The **adsetgroups** command enables you to view or change the list of groups available for the current user to make a user’s group membership more flexible.

On most UNIX systems, a user can only be a member of a limited number of groups at once. Because of this limitation, it is useful to be able to change a user’s group membership to add and remove groups when necessary. The **adsetgroups** command allows you to dynamically manage the set of Active Directory groups that are available to a UNIX account.

If you run the **adsetgroups** command with no arguments, it displays the current group list for the current user. If you specify a list of groups on the command line, those groups are added to or removed from the user’s current group list, and a new shell is invoked.

To add or remove groups, the local computer must be joined to a domain and zone. If you specify that membership in a specific group is required in a zone, that group cannot be removed from the currently active set of groups.

Any time the list of groups is changed, for example, using the **−−init** , **−−clear** or when specifying a list of group names to add or remove on the command line, a new shell is created.

OPTIONS

You can use the following options with this command:

−a, −−all
Display all the Active Directory groups that the current user is a member of.

−l, −−list
Display the current set of supplementary groups for the current UNIX user account.

−r, −−required
Display only the required groups.

−o, −−optional
Display only the groups that are not required.

−m, −−samname
Display the samAccountName attribute for the group instead of the group’s UNIX group name.

−n, −−number
Display the group identifier (GID) value for the group.

−R, −−remove
group Remove all of the specified groups from the currently

active set of groups. This option creates a new shell.

−c, −−clear
[group] Start with an empty list of groups. If you have previously saved a list of groups, you can use this option to clear the existing list and specify a different set of groups. For example, to replace an existing set of groups with the single group athena, you would run a command similar to the following:

```
adsetgroups −−clear athena
```

This command would change the list of groups for the user to be the single group "athena" unless some of the user’s other groups have been marked as required. This option creates a new shell.

−C, −−command cmd
Specify a command and options to execute in the temporary shell. Enclose the command in single quotation marks; for example, to add the group dnsadmins and execute the command, ls −l:

```
adsetgroups dnsadmins −C ’ls −l’
```

The command line is limited to 256 characters.

This option is not necessary when you run **adsetgroups** interactively, because you can execute commands in the new shell after it launches. However, if you run **adsetgroups** in a script, any commands you add to the script will not execute because the script is associated with the current shell, which stops when the new shell starts, before it is able to execute these commands. This option allows you to pass the command line directly to the temporary shell.

−E, −−exec cmd
Specify a command and options to execute by first invoking *execvp.* This option is similar to the **−−command** option, except that it enables the **adsetgroups** command to return the exit code of the command specified by the *cmd* argument. If the invocation of *execvp* fails, the **adsetgroups** command returns the exit code 255. Note that the command you specify is executed using the search path and the environment variables of the current shell.

−i, −−init
Start with the last saved list of groups. This option creates a new shell.

−s, −−save
Save the current list of groups. This option sets the default list of groups for the current user when the user logs on. The saved list of groups is used when you run the **adsetgroups** command with the **−−init** option.

−q, −−quiet
Suppress any warning or new shell messages.

−v, −−version
Display version information for the installed software.

group
List the groups to add or remove.

EXAMPLES

To display the currently active list of groups for the current user, you would type a command similar to the following:

```
adsetgroups
```

To add the groups delta1 and portland_lab to the current set of groups, and save this list as the default for the current user, you would type a command similar to the following:

```
adsetgroups --save delta1 portland_lab
```

To remove the groups oxford and westlake from the current set of groups for the current user, you would type a command similar to the following:

```
adsetgroups --remove oxford westlake
```

AUTHOR

Centrify Corporation

NAME

adsmb - allows you to perform various file operations, such as get a file, write a file, or display the contents of a directory.

SYNOPSIS

adsmb *file_operation* -s *share* [-c *credentials* [-m] [-C] [-T] [-h [*hostname*]] [-d [*domainName*]] [-r *remote_file*] [-n [*pattern*]] [-l *local_file*] [-V]

DESCRIPTION

The **adsmb** command allows you to perform various file operations, such as get a file, write a file, or display the contents of a directory using the Centrify smb stack. You can run this command using your log-on credentials or using the credentials for the local computer account. To use the local computer's credential, you must have root-level permission.

You can specify the file server to use or use the nearest domain controller for the joined domain.

You can use this command in conjunction with group policies to copy files and directories to and from Windows file shares.

The valid *file_operations* are get, getnew, getmod, print, put, putnew, dir, delete, mkdir, rename, and rmdir.

OPTIONS

You can use the following options with this command:

get The *get* operation enables you to get one or more files from a specified share.

getnew
The *getnew* operation enables you to get one or more files if the copy of the file on the specified share is newer than the local copy of the file.

getmod
The **getmod** operation enables you to get one or more files if the modification time of the file on the specified share differs from the time of the local copy.

print
The **print** operation creates a spool file on the shared printer and writes data to the spool file for printing.

put The *put* operation enables you to put one or more files into the specified share.

putnew
The *putnew* operation enables you to put one or more files if the local copy of the file is newer than the copy of the file on the specified share.

dir
The *dir* operation enables you to list the contents of a directory.

delete
The *delete* operation enables you to delete one or more files.

mkdir
The *mkdir* operation enables you to create a new directory.

rename
The **rename** operation enables you to rename a file.

rmdir
The *rmdir* operation enables you to remove a directory.

−s share
The *−s share* option specifies the share name.

−c credentials
The *−c credentials* option specifies the credentials file to use in performing the selected operation. For example:

```
−c /tmp/krb5cc_cdc0_q2GoCn
```

−m
The *−m* option uses the local computer’s credentials.

−C The *−C* option converts carriage return line feeds (CRLF) in a file to line feeds (LF).

−T The *−T* option displays the timestamp information in a computer−readable format. By default, timestamp information is displayed in a human−readable format.

−h [hostname]
The *−h [hostname]* option specifies the host name of the file server that is exporting the share. If you don’t specify a host name with this option, the command uses the nearest domain controller for the joined domain.

−d [domainName]
The *−d [domainName]* option specifies the domain name of the file server that is exporting the share. If you don’t specify a domain name by using this option, the command uses the currently joined domain, or the domain part from the host if you specify the **−h** option.

−n [pattern]
The **−n** option specifies the pattern to use when listing the contents of a directory. The default pattern is *.

−r remote_file
The *−r remote_file* option specifies the remote file or directory to work with. You can use forward slashes in remote file names.

−l local_file
The *−l local_file* option specifies the local file or directory to work with.

−V The **−V** option prints debug messages.

EXAMPLES

You can use the **adsmb** command to get file or directory information or perform file or directory operation.

For example, to display details about the contents of the platforms directory on the lab file share with human−readable timestamps for when a file or subdirectory was created, last modified, and last read, you would type a command similar to the following:

```
adsmb dir −h sierra −s lab −r "platforms/*"
```

To get the file autorun.bat from the system volume (sysvol) of the nearest domain controller using the computer credentials and place it in the local /tmp directory, you would type a command similar to the following:

```
sudo adsmb get −s sysvol −m −r arcade.com/lab/autorun.bat −l /tmp/autorun.bat
```

AUTHOR

Centrify Corporation

NAME

adupdate − add, modify, or delete Active Directory and Centrify DirectControl zone information.

SYNOPSIS

adupdate add|delete|modify user|group [options]

Note The specific options you can use depend on the task you want to perform. See the appropriate section for information about which options to use for each task.

GENERAL DESCRIPTION

The **adupdate** command is provided for backward compatibility to enable you to perform user and group account management tasks from the command line on any Centrify−managed computer. You cannot use this command to update information in hierarchical zones. To update information in hierarchical zones, use **adedit.** The user and group management tasks you can perform include the following:

- Adding a new user to a zone
- Modifying a user’s UNIX profile
- Disabling and enabling a user’s access to a zone
- Deleting users from a zone
- Adding an Active Directory group to a zone
- Modifying a group’s UNIX profile
- Managing the group’s membership
- Deleting an existing Active Directory group from to a zone
- Synchronizing the time on the local computer with its domain controller

Each of these tasks can include command line options that enable the task to be accomplished using a script.

You must specify the administrative task to perform, then whether the task applies to a user or group before you specify any other command line options. In addition, the options required to complete an administrative task depend on which task you are performing. For more information about the syntax and the options you need to use for each task, see the appropriate section for the administrative task you are performing.

ADDING A UNIX USER PROFILE

You can use **adupdate add user** to add a specified user to the zone associated with the computer where the command is run. You can also use this command to create a new user account in Active Directory, if desired.

The basic syntax for adding a new user with the **adupdate add user** command is:

```
adupdate add user −U user[@domain] [options] UNIXlogin
```

You must specify the Active Directory user that the new UNIX user profile should be associated with. In specifying the Active Directory user, you must use the *user@domain* format if the user is a member of a domain other than the host computer’s domain.

OPTIONS

You can use the following options with the **adupdate add user** command:

−a, −−admin user[@domain]

The **−−admin** option identifies an Active Directory user account with sufficient rights to add a new user profile or new user account to Active Directory in the current domain.

You must use the *user@domain* format to specify the user account if the administrative user is not a member of the host computer’s current domain.

If you do not specify this option, the current Kerberos credentials are used. If there are no Kerberos credentials available, the default value is the Administrator user account.

−p, −−password password

The **−−password** option specifies the password for the Active Directory user account with administrative rights. If you are using the current Kerberos credentials, you don’t need to specify the password at the command line. If you are not using the current Kerberos credentials and do not specify the password at the command line, you are prompted to enter the password before the command executes.

Note Specifying a password at the command line represents a security risk because the password can be retrieved while the command is running or from command history after the command has completed its execution. You can pipe the password into standard input for scripting purposes.

−U, −−user loginname

The **−−user** option specifies the Active Directory user that the new UNIX user profile should be associated with. This option is required.

You use the user’s Windows login name, for example, the samAccountName attribute, or the user’s userPrincipalName attribute to identify the Active Directory account. The name you specify can also include spaces, if properly quoted according to the rules of the UNIX shell you are using. For example, if you want to specify a first name and last name:

```
−−user ’Kay Li’
```

You should use the *user@domain* format to specify the login name if the user is not a member of the host computer’s currently joined domain. If you are also using the **−−create** option to create a new Active Directory user and do not specify the **−−first name** option in the command line, the name you specify for the **−−user loginname** is also used for the displayName and CN attributes in Active Directory.

−C, −−create

The **−−create** option creates a new Active Directory user. If you don’t specify this option, the user account you specify for the **−−user** option must already exist in Active Directory.

-d, --home home_directory
The **--home** option specifies the UNIX home directory for the new user. The default home directory path is set by appending the user's login name to default_home. For example, if the user's login name is kay:

```
/default_home/kay
```

Note: You cannot specify this option if you are joined to Auto Zone.

-g, --group initial_group
The **--group** option specifies the group name or numeric identifier of the user's primary group. If you specify a group name, the group name must exist in Active Directory. If you specify a numeric group identifier (GID), the group identifier must refer to an existing group with a UNIX profile defined for the zone.

The default group number is the value specified for the aduseradd.group.default configuration parameter in the /etc/centrifydc/centrifydc.conf file.

Note: You cannot specify this option if you are joined to Auto Zone.

-G, --groups groupname,[...]
The **--groups** option lists additional groups the user is a member of. Use commas to separate group names. For example:

```
--groups qa02,sap,javax
```

You can specify the groups by UNIX group name or samAccountName attribute. The groups you specify do not need to have a UNIX profile already defined for the zone. There is no default group list. By default, only a user's initial group is defined.

-i, --foreign-sid sid_value
The **--foreign-sid** option specifies the Active Directory security identifier (SID) for a UNIX user to add from a one-way trusted forest.

You can retrieve the SID of the user with the **adquery user -i** command.

-u, --uid uid_value
The **--uid** option specifies the numeric value of the user identifier (UID) for the UNIX user account. This value must be a positive integer and must be unique in the zone unless you specify the -o option to allow duplicate values. If you do not specify the --uid option, the next available UID in the zone is used by default. You should not specify UID values between 0 and 99. Values between 0 and 99 are typically reserved for system accounts.

Note: You cannot specify this option if you are joined to Auto Zone.

-o, --allow-duplicate
The **--allow-duplicate** option allows the UID value for the new user to be the same as the UID used in another user profile.

Note: You cannot specify this option if you are joined to Auto Zone.

-s, --shell shell_path
The **--shell** option specifies the user's login shell. If you don't specify this option, the system selects the default login shell for the operating environment when the user logs on.

Note: You cannot specify this option if you are joined to Auto Zone.

-m, --make-home [-k, --skeleton skeleton_directory]
The **--make-home** option creates the user's home directory automatically if it does not already exist. If you specify this option and the **--skeleton** option, the files and directories contained in *skeleton_directory* are copied to the new home directory. If you don't specify the **--skeleton** option, the files contained in the directory specified by the **pam.homeskel.dir** configuration parameter are copied to the new home directory instead. The **--skeleton** option is only valid in conjunction with the **--make-home** option. If you don't specify this option, the **adupdate** command does not create the user's home directory or copy any files.

Note: You cannot specify this option if you are joined to Auto Zone.

-f, --first name
The **--first** option specifies the first *name* of the Active Directory user. The *name* you specify is mapped to the **givenName** LDAP attribute and is used as the first component for the **displayName** and **cn** attributes.

-l, --last name
The **--last** option specifies the last *name* of the Active Directory user. The *name* you specify is mapped to the **sn** LDAP attribute and is used as the second component for the **displayName** and **cn** attributes if the **--first name** option is specified.

-w, --new-password password
The **--new-password** option specifies the initial password for the new user account. If you not specify a password for the user, you are prompted to enter and re-enter the password before the command executes. Whether you specify the user's password at the command line or when prompted, the password must adhere to the domain's password policy requirements for length and complexity.

-W, --show-password
The **--show-password** option generates and displays an initial password for the new user account. This option enables the account to be created with a random password, which can then be reset later when the user logs on.

-c, --container containerDN
The **--container** option specifies the distinguished name (DN) of the container or Organizational Unit (OU) in which to place this user account. The DN represents the direct parent object for the user.

You can specify the containerDN by:
- Canonical name (ajax.org/unix/services)
- Fully distinguished name (cn=services, cn=unix,dc= ajax,dc=org)
- Relative distinguished name without the domain suffix(cn=services,cn=uni

You must specify the **--container** option for the new user object when creating a new user account with the adupdate command. You can use the domain’s default Users container object, for example, ajax.org/Users, or any other existing parent container object. If the container you specify does not exist in Active Directory, however, the user account will not be created. In addition, you must have permission to add entries to the specified container.

−S, −−spn servicePrincipalName

The **−−spn** option specifies the *servicePrincipalName* to use as the service principal name for this user account. Specifying a service principal name is particularly useful if you intend to use prevalidated authentication. To specify the *servicePrincipalName* , you should use the format:

```
service/samAccountName
```

For example, to add a service principal for the prevalidation service, preval, for the user account kai:

```
−−spn preval/kai kai
```

−P, −−principal userPrincipalName

The *userPrincipalName* specifies a user principal name (UPN) for the user account in Active Directory. You may only specify this option when creating new AD users.

−V, −−verbose

The **−−verbose** option displays detailed information about each operation as it is performed.

−v, −−version

The **−−version** option displays version information for the installed software.

UNIXlogin

The *UNIXlogin* specifies the UNIX login name for the user in the current zone.

EXAMPLES

To add a new UNIX profile for Active Directory user Wilson Perez if you are logged on with a user account with permission to add new users to the domain, you could type a command line similar to the following:

```
adupdate add user −U "ajax.org/Users/Wilson Perez" wilson
```

You are then prompted for the password for the new account and to retype the password for the new account.

To add a new user account when your current user account does not have permission to add new users to the domain, you must provide the user name and password for an account with permission to add new users to the domain. For example, if the user paolo@acme.com is an administrator with permission to add users to the atlas.acme.com domain, you could type a command line similar to the following:

```
adupdate add user −−uid 2367 −−admin paolo@acme.com −−create −−user
chris@atlas.acme.com −−first Chris −−last Roberts chris
```

You are then prompted for the password for the paolo@acme.com account. If the user name and password for the administrator’s account are valid, you are then prompted for the password for the new account and to retype the password for the new account.

MODIFYING A UNIX USER PROFILE

You can use **adupdate modify user** to modify login information for an user account with a UNIX profile defined for the current zone. Note that you cannot modify an Active Directory user account that does not have a UNIX profile in a zone.

The basic syntax for the **adupdate modify user** program is:

```
adupdate modify user [options] UNIXlogin
```

OPTIONS

You can use the following options with the **adupdate modify user** command:

−a, −−admin user[@domain]

The **−−admin** option identifies an Active Directory user account with sufficient rights to modify user profiles in the current domain. You must use the *user@domain* format to specify the user account if the administrative user is not a member of the host computer’s current domain. If you do not specify this option, the current Kerberos credentials are used. If there are no Kerberos credentials available, the default value is the Administrator user account.

−p, −−password password

The **−−password** option specifies the password for the Active Directory user account with administrative rights. If you are using the current Kerberos credentials, you don’t need to specify the password at the command line. If you are not using the current Kerberos credentials and do not specify the password at the command line, you are prompted to enter the password before the command executes.

Note Specifying a password at the command line represents a security risk because the password can be retrieved while the command is running or from command history after the command has completed its execution. You can pipe the password into standard input for scripting purposes.

−l, −−login newUNIXlogin

The −−login option changes the UNIX login name for the specified user. This option does not make any other changes. If you use this option, you should also use other options to create a new home directory name that reflects the new login name or move the contents of the user’s old home directory to a new home directory name.

Note: You cannot specify this option if you are joined to Auto Zone.

−d, −−home home_directory

The **−−home** option creates a new UNIX home directory for the specified user. You can use this option in conjunction with the **−−move−home** option to move the contents of a user’s current home directory to a new home directory. The new home directory is created automatically if it does not already exist.

Note: You cannot specify this option if you are joined to Auto

Zone.

−m, −−move−home

The **−−move−home** option moves the contents from a user’s old home directory to a new home directory.

Note: You cannot specify this option if you are joined to Auto Zone.

−g, −−group initial_group

The **−−group** option modifies the group name or numeric identifier of the user’s primary group. If you specify a group name, the group name must exist in Active Directory. If you specify a numeric group identifier (GID), the group identifier must refer to an existing group with a UNIX profile defined for the zone. By default, a user’s primary group is the value specified for the default GID for the zone or the next available GID.

Note: You cannot specify this option if you are joined to Auto Zone.

−G, −−groups groupname,[...]

The **−−groups** option modifies the additional groups the user is a member of. Use commas to separate group names. For example:

```
−−groups qa02,sap,javax
```

You can specify the groups by UNIX group name or samAccountName attribute. The groups you specify do not need to have a UNIX profile already defined for the zone. There is no default group list. By default, only a user’s initial group is defined.

−u, −−uid uid_value

The **−−uid** option modifies the numeric value of the user identifier (UID) for the UNIX user account. This value must be a positive integer and must be unique in the zone unless you specify the **−−allow−duplicate** option to allow duplicate values. If you do not specify the **−−uid** option, the next available UID in the zone is used by default. You should not specify UID values between 0 and 99. Values between 0 and 99 are typically reserved for system accounts.

Note: You cannot specify this option if you are joined to Auto Zone.

−o, −−allow−duplicate

The **−−allow−duplicate** option allows the UID value for the user to be the same as the UID used in another user profile.

Note: You cannot specify this option if you are joined to Auto Zone.

−s, −−shell shell_path

The **−−shell** option changes the user’s login shell. If you don’t specify this option, the system selects the default login shell for the operating environment when the user logs on.

Note: You cannot specify this option if you are joined to Auto Zone.

−i, −−foreign−sid sid_value

The **−−foreign−sid** option specifies the Active Directory security identifier (SID) for a UNIX user in an external forest with a

one−way trust.

−L, −−lock on|off

The **−−lock** option enables or disables a user’s account in Active Directory.

−f, −−forcepw on|off

The **−−forcepw** option changes whether the specified user should be forced to enter a password at the next logon.

−k, −−des on|off

The **−−des** option changes the "Use DES encryption types for this account" setting in Active Directory for the specified user.

−z, −−enable on|off

The **−−enable** option enables or disables access to the current zone for the specified user.

Note: You cannot specify this option if you are joined to Auto Zone.

−S, −−spn servicePrincipalName

The **−−spn** option specifies the *servicePrincipalName* to add for this user account. To specify the *servicePrincipalName* , you should use the format:

```
service/samAccountName
```

For example, to add a service principal for the prevalidation service, preval, for the user account kai:

```
−−spn preval/kai kai
```

−P, −−principal userPrincipalName

The *userPrincipalName* specifies a user principal name (UPN) for the user account in Active Directory.

−x, −−remove−spn servicePrincipalName

The **−−remove−spn** options specifies the ,I servicePrincipalName to remove for this user account. For example, to remove the service principal for the prevalidation service, preval, for the user account kai:

```
−−remove−spn preval/kai kai
```

−U, −−unlock

The **−−unlock** option unlocks a user account that has been locked because of failed password attempts.

−X, −−extattr [+|−]name=value

The **−−extattr** option is used to add, delete, or modify the value of an extended attribute for the user. Typing a plus sign (+) before the attribute name adds the extended attribute if it doesn’t exist. Typing a minus sign (−) before the attribute name removes the attribute, if it exists.

Note: You cannot specify this option if you are joined to Auto Zone.

For example, to set the value of the extended attribute aix.rlogin:

```
adupdate modify user −X +aix.rlogin=true jae
```

Note Extended attributes are only applicable on AIX computers.

You can use the keyword help to view a list of the supported extended attributes. For example:
adquery user −−extattr help

−V, −−verbose
The **−−verbose** option displays detailed information about each operation as it is performed.

−v, −−version
The **−−version** option displays version information for the installed software.

UNIXlogin
The *UNIXlogin* specifies the UNIX login name for the user in the current zone. The user must exist and be enabled for UNIX access in the same zone as the computer.

EXAMPLES

To change the UID for a UNIX user profile if you are logged on with an account with permission to modify user information in the domain, you could type a command line similar to the following:

```
adupdate modify user −−uid 700 jcole
```

To change the UNIX user name and home directory for the UNIX user jim to kuoj if you are logged on with an account with permission to modify user information in the domain, you could type a command line similar to the following:

```
adupdate modify user −−login kuoj −−home /home/kuoj −−move−home jim
```

To force a the user kuoj to change his password the next time he logs on, you could type a command line similar to the following:

```
adupdate modify user −−forcepw on kuoj
```

You may need to refresh the console you are using to verify changes were made.

DELETING A UNIX USER PROFILE

You can use **adupdate delete user** to remove an existing user profile from the current zone or to delete an Active Directory user.

The basic syntax for the **adupdate delete user** program is:

```
adupdate delete user [options] user[@domain]
```

OPTIONS

You can use the following options with the **adupdate delete user** command:

−a, −−admin user[@domain]
The **−−admin** option identifies an Active Directory user account with sufficient rights to remove an Active Directory user account from the domain. You must use the *user@domain* format to specify the account if the administrative user is not a member of the host computer's current domain. If you do not specify this option, the current Kerberos credentials are used. If there are no Kerberos credentials available or user account specified, the Administrator user account is used to connect to Active Directory.

−p, −−password password
The **−−password** option specifies the password for the Active Directory administrative account. If you do not provide the password at the command line, you are prompted to enter the password before the command executes.

Note Specifying a password at the command line represents a security risk because the password can be retrieved while the command is running or from command history after the command has completed its execution.

−R, −−rmhome
The **−−rmhome** option removes the user's home directory on the Centrify DirectControl−managed system.

−r, −−remove
The **−−remove** option removes the associated Active Directory user account from Active Directory without interactive confirmation.

−i, −−interactive
The **−−interactive** option prompts you to confirm the deletion of the UNIX profile or Active Directory user account interactively before removing the user.

−V, −−verbose
The **−−verbose** option displays detailed information about each operation as it is performed.

−v, −−version
The **−−version** option displays version information for the installed software.

user[@domain]
The *user* specifies the ser profile name or Active Directory login name (samAccountName@domain) for the user in the current zone.

The user must exist and be enabled for UNIX access in the same zone as the computer. If the user name you specify does not uniquely identify the user, you must include the domain name in the command line.

EXAMPLES

To remove the UNIX user profile from the current zone if you are logged in with a user account with permission to delete user information from the domain, you could type a command similar to the following:

```
adupdate delete user −V sunni
```

To remove a UNIX profile account if your current user account does not have permission to delete users from the domain, you must provide the user name and password for an account with permission to delete users from the domain. For example, if the user paolo@acme.com is an administrator with permission to remove user profiles from the domain, you could type a command similar to the following:

```
adupdate delete user −−admin paolo@acme.com −V sunni
```

You are then prompted for the Active Directory password for the paolo@acme.com account. If the user name and password for the administrator's account are valid, the user profile is removed from Active Directory.

If you also want to remove the Active Directory user account, you could type a command similar to the following:

```
adupdate delete user --admin paolo@acme.com --verbose --remove
--interactive sunni
```

After you provide the Active Directory password for the paolo@acme.com account, this command connects to Active Directory and prompts you to confirm whether you want to delete the account:

```
Delete Centrify user CN=Sunni Ashton,CN=Users,DC=ajax,DC=org ?
(Yes/No)
```

You can then type y to confirm that you want to delete the user.

You may need to refresh the console you are using to verify changes were made.

ADDING A UNIX GROUP PROFILE

You can use **adupdate add group** to add a new group profile to the current zone.

The basic syntax for the **adupdate add group** program is:

```
adupdate add group [options] groupname
```

OPTIONS

You can use the following options with the **adupdate add group** command:

-a, --admin user[@domain]
The **--admin** option identifies an Active Directory user account with sufficient rights to add a new Active Directory group to the domain. You must use the *user@domain* format to specify the account if the administrative user is not a member of the host computer's current domain. If you do not specify this option, the current Kerberos credentials are used. If there are no Kerberos credentials available or user account specified, the Administrator user account is used to connect to Active Directory.

-p, --password password
The **--password** option specifies the password for the Active Directory administrative account. If you do not provide the password at the command line, you are prompted to enter the password before the command executes.

Note Specifying a password in the command line represents a security risk because the password can be retrieved while the command is running or from command history after the command has completed its execution.

-C, --create
The **--create** option creates a new UNIX group profile and Active Directory group.

-G, --group name|canonical_name
The **--group** option specifies the group name to be associated with the new UNIX group in canonical form or by its **samAccountName** attribute in Active Directory. This option is required and is used for the **samAccountName** , **displayName** , and LDAP common name (**cn**) attributes in Active Directory.

-g, --gid
The **--gid** option specifies the numeric value of the group identifier (GID) for the new group profile.

-o, --allow-duplicate
The **--allow-duplicate** option allows the GID value for the new group to be the same as the GID used in another group profile.

-R, --required
The **--required** option makes the new group a required group for all of the users who are members of the group. Required groups cannot be removed when users change their active set of groups using the **adsetgroups** command.

-c, --container containerDN
The **--container** option specifies the distinguished name (DN) of the container or Organizational Unit (OU) in which to place this group account. The DN represents the direct parent object for the group.

You can specify the containerDN by:
- Canonical name (ajax.org/unix/services)
- Fully distinguished name (cn=services, cn=unix,dc= ajax,dc=org)
- Relative distinguished name without the domain suffix(cn=services,cn=uni

You must specify the **--container** option for the new group object when creating a new group account with the adupdate command. You can use the domain's default Users container object, for example, ajax.org/Users, or any other existing parent container object. If the container you specify does not exist in Active Directory, however, the group account will not be created. In addition, you must have permission to add entries to the specified container.

-t, --type local|global|universal
The **--type** option specifies the type of Active Directory security group to create. The valid group types are domain local, global across domains, or universal.

If you don't specify the group type, the group is added as a global group by default.

-V, --verbose
The **--verbose** option displays detailed information about each operation as it is performed.

-v, --version
The **--version** option displays version information for the installed software.

groupname
The *groupname* specifies the UNIX name for the group.

EXAMPLES

To add the group profile qa002 to the Active Directory QA group if you are logged in with a user account with permission to add groups to the domain, you could type a command line similar to the following:

```
adupdate add group −g 9000 −G ajax.org/Users/QA qa002
```

To create a new Active Directory group with a UNIX profile if you are logged in with a user account with permission to add groups to the domain, you could type a command line similar to the following:

```
adupdate  add  group  −−create  −−container  Users −−gid 9000 −−group
ajax.org/Users/QA −−type universal qa002
```

MODIFYING AN EXISTING GROUP

You can use **adupdate modify group** to modify the UNIX group profile name, numeric identifier, or membership.

You can only use this command with security groups, not distribution groups. In addition, the group must have a UNIX profile in a zone; you cannot modify an Active Directory group that does not have a UNIX profile defined for a zone.

The basic syntax for the **adupdate modify group** command is:

```
adupdate modify group [options] groupname
```

OPTIONS

You can use the following options with the **adupdate modify group** command:

−a, −−admin user[@domain]

The **−−admin** option identifies an Active Directory user account with sufficient rights to modify an Active Directory group. You must use the *user@domain* format to specify the account if the administrative user is not a member of the host computer’s current domain. If you do not specify this option, the current Kerberos credentials are used. If there are no Kerberos credentials available or user account specified, the Administrator user account is used to connect to Active Directory.

−p, −−password password

The **−−password** option specifies the password for the Active Directory administrative account. If you do not provide the password at the command line, you are prompted to enter the password before the command executes.

Note Specifying a password in the command line represents a security risk because the password can be retrieved while the command is running or from command history after the command has completed its execution.

−g, −−gid

The **−−gid** option modifies the numeric group identifier (GID) for the specified group profile.

−o, −−allow−duplicate

The **−−allow−duplicate** option allows the GID value for the group to be the same as the GID used in another group profile.

−n, −−name groupname

The **−−name** option modifies the UNIX group name for the specified group.

−m, −−member user|group

The **−−member** option adds a new user or group as a member of the specified group. You may specify multiple −m options on a single command line.

You can specify either a UNIX name or samAccountName for the user or group to add. If the agent cannot resolve the user name because it conflicts between Active Directory and the Centrify zone, it returns an error message.

The user or group to add must have a UNIX profile in a zone; you cannot add an Active Directory user or group that does not have a UNIX profile defined for a zone. In addition, a group to add must be a security group, not a distribution group.

−R, −−required on|off

The **−−required** option enables you to specify whether group membership is required (on) or not required (off).

−r, −−remove user|group

The **−−remove** option removes a user or group as a member of the specified group.

−V, −−verbose

The **−−verbose** option displays detailed information about each operation as it is performed.

−v, −−version

The **−−version** option displays version information for the installed software.

groupname

The *groupname* specifies the UNIX name for the group. The group must exist and be enabled for UNIX access in the same zone as the computer.

EXAMPLES

To change the GID for a UNIX group profile if you are logged on with an account with permission to modify group information in the domain, you could type a command similar to the following:

```
adupdate modify group −−gid 700 javax
```

To add a new user to the UNIX group javax if you are logged on with an account with permission to modify group information in the domain, you could type a command similar to the following:

```
adupdate modify group −−member jcole −V javax
```

To add a group or user as a new member of a UNIX group, the group or user must be enabled for UNIX access in the host computer’s zone. In addition, you can only specify one new user or group member each time you run this command.

To remove a group or user from the list of members for a group, you could type a command similar to the following:

```
adupdate modify group −−remove luis −V javax
```

DELETING A GROUP

You can use **adupdate delete group** to remove an existing group profile from the current zone or delete an Active Directory group.

The basic syntax for the **adupdate delete group** command is:

```
adupdate delete group [options] groupname
```

OPTIONS

You can use the following options with the **adupdate delete group** command:

−a, −−admin user[@domain]
The **−−admin** option identifies an Active Directory user account with sufficient rights to remove an Active Directory user account from the domain. You must use the *user@domain* format to specify the account if the administrative user is not a member of the host computer’s current domain. If you do not specify this option, the current Kerberos credentials are used. If there are no Kerberos credentials available or user account specified, the Administrator user account is used to connect to Active Directory.

−p, −−password password
The **−−password** option specifies the password for the Active Directory administrative account. If you do not provide the password at the command line, you are prompted to enter the password before the command executes.

Note Specifying a password in the command line represents a security risk because the password can be retrieved while the command is running or from command history after the command has completed its execution.

−i, −−interactive
The **−−interactive** option prompts you to confirm the deletion of the group profile interactively before removing the group.

−r, −−remove
The **−−remove** option removes the Active Directory group associated with the group profile.

−V, −−verbose
The **−−verbose** option displays detailed information about each operation as it is performed.

−v, −−version
The **−−version** option displays version information for the installed software.

groupname
The *groupname* specifies the UNIX name for the group. The group must exist and be enabled for UNIX access in the same zone as the computer.

EXAMPLES

To remove the UNIX group profile from the current zone when you are logged in with an account with permission to delete groups from the domain, you could type a command line similar to the following:

```
adupdate delete group performx
```

If you also want to remove the Active Directory group associated with the UNIX group, you could type a command similar to the following:

```
adupdate delete group −−admin paolo −−verbose −−remove  −−interactive
unixdev
```

After you provide the Active Directory password for the paolo account, this command connects to Active Directory and prompts you to confirm whether you want to delete the group. For example:

```
Delete  Centrify  group  CN=Unix developers,CN=Users,DC=ajax,DC=org ?
(Yes/No)
```

You can then type y to confirm that you want to delete the group.

You may need to refresh the console you are using to verify changes were made.

UPDATING THE SYSTEM CLOCK

You can also use the **adupdate** command to synchronize the system clock on the local computer with its domain controller. The syntax for synchronizing the time on the local computer with its domain controller is:

```
adupdate time
```

AUTHOR

Centrify Corporation

SEE ALSO

adjoin(1), adquery(1)

NAME

adwebproxyconf − Set, delete, list and test local http proxy configuration and credential.

SYNOPSIS

adwebproxyconf −−set [−−verbose] [−−username *username]* [−−password *password]* [−−machine] [−−server *servername:port|""]* [−−authreq true|false|""] [−−authtype basic|digest|ntlm|negotiate|anyauth|""]

adwebproxyconf −−test −−cip *cipurl* [−−verbose] [−−username *username]* [−−password *password]* [−−machine] [−−server *servername:port|""]*

adwebproxyconf −−delete [−−verbose]

adwebproxyconf −−list [−−verbose]

adwebproxyconf [−−version] [−−help]

DESCRIPTION

The **adwebproxyconf** command is used to set, delete, list and test local http proxy configuration and credential.

With the adwebproxyconf command, you can:

− Setup/Delete HTTP Proxy credential to be used by agent.

− Show HTTP Proxy user.

− Configure HTTP Proxy Server used by agent.

− List locally configured HTTP Proxy Server.

− Test the proxy connection using configured or supplied HTTP Proxy credential.

To run **adwebproxyconf** you must be logged in as root.

COMMANDS

You can use the following commands with this command:

−S, −−set
Set the HTTP Proxy Credential and HTTP Proxy Server locally.

−T, −−test
Test the HTTP Proxy Credential using the configured or supplied settings.

−D, −−delete
Delete HTTP Proxy Credential from local machine, and reset HTTP Proxy configurations in centrifydc.conf:
HTTP Proxy Server
HTTP Proxy authentication type
HTTP Proxy authentication required

−L, −−list
List out the HTTP Proxy username and the HTTP Proxy Server configured locally.

OPTIONS

You can use the following options with this command:

−u, −−username username
Proxy username. When use with −S and −T commands, if username is not supplied but −−password is supplied, username will be set to Administrator as default. When use with −T command, if username and password are not supplied, will get the username and password from proxy credential file.

−p, −−password password
Proxy user’s password. When use with −S command, will be prompted if none is supplied. When use with −T command, will be prompted if none is supplied but username is provided. If both username and password are not supplied, get it from proxy credential file.

−m, −−machine
Use local machine account for proxy authentication, and negotiate auth type is used. Cannot used this option along with −u/−p/−t.

−s, −−server servername:port|""
Specify HTTP Proxy Server. When use with −S command, the value will be set to centrifydc.conf. Empty string unsets the value. Can use individually or with other options. When use with −T command, get the value from centrifydc.conf if none is supplied.

−r, −−authreq true|false|""
Specify if HTTP Proxy authentication is required for a specified HTTP Proxy Server in centrifydc.conf. Empty string unsets the value.

−t, −−authtype basic|digest|ntlm|negotiate|anyauth|""
Specify HTTP Proxy authentication type when authenticating to HTTP Proxy Server in centrifydc.conf. Empty string unsets the value. The ntlm and digest authentication types are not allowed in FIPS mode.

−c, −−cip cipurl
Specify the URL of the Cloud Identity Platform. This parameter is required when use −T command.

−V, −−verbose
Print debug information.

−v, −−version
This option displays version information for the installed software.

−h, −−help
This option displays help information for the command line.

EXAMPLES

1. Set user specified proxy server with negotiate authentication type and credential:

```
adwebproxyconf −S −s proxyserver.mydomain.com:3128 −r true −t
negotiate −u mfa_user01 −p password
```

2. List proxy server configuration and credential:

```
adwebproxyconf −L
```

3. Delete user specified credential and reset HTTP Proxy configurations in centrifydc.conf:

```
adwebproxyconf −D
```

4. Test user specified proxy server with machine credential:

```
    adwebproxyconf −T −c abc0001.centrify.com −m
```

AUTHOR

Centrify Corporation

SEE ALSO

For related information, see the following command reference sections: adinfo(1), adcdiag(1), adclient(1)

NAME

dzedit − edit a file as another user

SYNOPSIS

```
dzedit  [−AknS]  [−C  fd]  [−g  groupname|#gid]  [−p prompt] [−u user
name|#uid] file ...
```

DESCRIPTION

The **dzedit** command enables you to edit a file as another user. It is similar to using **dzdo** with the **−e** option.

To use the **dzedit** program, you must have a role with permission to run **dzedit** as a privileged command or as an allowed restricted environment command. You can configure the right to run **dzedit** in a role definition using DirectManage Access Manager or ADEdit commands.

If a user is granted permission to run **dzedit** , the program does the following when invoked:

- Creates temporary copies of the files to be edited with the file owner set to the invoking user.

- Starts the editor specified by the VISUAL or EDITOR environment variable to edit the temporary files. If neither environment variable is set, the ,B dzedit program uses the editor listed in the editor sudoers variable.

- If the specified file does not exist, **dzedit** creaters it.

- If the files are modified, **dzedit** copies the temporary files back to their original location and the temporary versions are removed.

- If **dzdo is unable to update a file with its edited version, the user will** receive a warning and the edited copy will remain as a temporary file.

Unlike most **dzdo** commands, the **dzedit** program runs with the invoking user’s environment unmodified.

The program makes temporary copies of the files to be edited before invoking the editor to prevent users from issuing a shell escape in the editor that would then allow the user to run any command as the target user. By using **dzedit** to edit the temporary file then replace the original file after editing, users can’t use a shell escape in an editor to open a new shell and run other command as the target user.

OPTIONS

You can use the following options with this command:

−A Gets the password from a helper program rather than from the terminal. The command will exit with an error if a helper program cannot be found.

−C *fileDescriptor* Leaves the specified file descriptors open when **dzedit** exits.

Normally, the program closes all open file descriptors except standard input, standard output, and standard error. This option allows you to specify a starting point above standard error (file descriptor 3). Values less than 3 are not allowed.

−g *groupname* | *gid* Specify the primary group name or numeric identifier to set for the specified command.

The definition for a command right contains a list of valid groups that may be used with this option−−it could be restricted to certain groups or include all valid groups. If you are uncertain about the group to specify, or see an error when running the command, check with your Centrify zone administrator.

To specify a group by GID instead of the group name, use ’#gid’ enclosed in single quotes. For example, to run adquery as a privileged command and set the primary group as the group with the numeric GID of 101, you could type a command similar to the following:

```
dzdo −g ’#101’ adquery
```

−k Invalidates the user’s login timestamp by setting the time on it to the epoch. This option does not require a password. After using this option, however, the next time the user attempts to run **dzdo** , the command will prompt for a password. This option allows a user to revoke **dzdo** permissions from a .logout file.

−n Prevents **dzedit** from prompting for a password.

−p *prompt* Allows you to override the default password prompt and use a custom one. The following percentage (%) escapes are supported:

%u expands to the invoking user’s login name.

%U expands to the login name of the user the command will run as, for example, root by default.

%h expands to the local computer’s host name without its domain name.

%H expands to the local computer’s host name including the domain name.

%% collapses into a single % character.

−S Reads the password from standard input instead of the terminal device.

−u *username|uid* Runs the specified command as a user other than root.

The definition for a command right contains a list of valid users that can be used with this option−−it could be restricted to certain users or include all valid users. If you aren’t sure, or receive an error when running the command, check with your Centrify zone administrator.

The **dzedit** command will recognize any user name that is an equivalent of the user name specified for the command to be run. For example, if permission is given to the Active Directory user "bob.smith" to run **adinfo** as a privileged command, and "bob.smith" has a valid UNIX profile with the UNIX name of "bsmith", you can specify "bsmith" when you use **dzdo to run adinfo:**

```
dzdo −u bsmith adinfo
```

To specify a user by UID instead of the user’s login name, use ’#uid’ enclosed in single quotes. For example, to run adinfo as a privileged command and as the user with the numeric UID of 101, you could type a command similar to the following:

```
dzdo −u ’#101’ adinfo
```

EXAMPLES

To edit the "privs" file as the user "molly", you would type:

```
dzedit −u molly privs
```

AUTHOR

Centrify Corporation

SEE ALSO

For related information, see the following command reference sections:

dzdo(8), dzsh(1), adlicense(1)

NAME

dzinfo − display detailed information about the configuration of rights and roles for a specified user on the local computer.

SYNOPSIS

dzinfo [*username*] [−−commands] [−−diag] [−−format] [−−pam] [−−roles] [−−test *command*] [−−verbose] [−−all] [−−version]

DESCRIPTION

The **dzinfo** command displays detailed information about the configuration of rights and
roles for one or more specified users on the local computer. If you do not specify a user, **dzinfo** returns information for the currently logged on user.

To specify one or more user names on the command line, you must be logged on as root.

Note The **dzinfo** command requires that you are running Centrify with a license.

By default, the **dzinfo** command displays all roles and rights for the specified user. Some of the information included may not be applicable, however, because of role availability settings, start or expiration times, or audit integration.

The −−commands, −−pam, and −−roles options are intended to limit the information displayed to a single set of rights. For example, you can use the **−−pam** option to display only the PAM−enabled applications the specified user is allowed to access.

Similarly, the **−−commands** option lists only the commands that the user is allowed to run. The commands listed, however, may be privileged commands that can be invoked using **dzdo** or shell commands that are allowed in restricted environments within the **/bin/dzsh** restricted shell environment. The **−−roles** option lists only the roles the user has been assigned. If you don’t specify one of these options to limit the information displayed, the **.dzinfo** command returns information for all three sets of rights.

OPTIONS

You can use the following options with this command:

username[@domain]

Specify the Active Directory user by UNIX profile name or Active Directory name that you want to display details for. You can specify this option multiple times to retrieve and display the information for multiple users. If you don’t specify the *username* option, the command returns information for the currently logged on user.

Note You must be logged on as root to specify a user name.

−c, −−commands

Display only information about the commands the user can run. This option displays all of the commands the user is allowed to run as privileged commands or as restricted environment commands.

−d, −−diag

Include extended, diagnostic information in the command output. This option is intended for troubleshooting potential problems with the authorization store.

−f, −−format

Generates formatted output that can be used in scripts. The output separates the properties of each object into a single line with a colon (:) between each field. The basic output format is:

```
user:object;property:value
```

For example, for the user maya, you might see output like this:

```
maya:ROLE:Local User:No maya:ROLE:Role Name:dba
```

−p, −−pam

Display only information about the PAM−enabled applications the user has permission to access.

−r, −−roles

Display only the roles to which the specified user is assigned.

−C, −−computer−role

Display information about the computer roles for users on this computer. This option requires root privilege.

Specify a user to show computer roles for that user, or do not specify a user to show all computer roles for this computer.

−t, −−test command

Check whether the specified command can be run by the user using dzdo or in a restricted environment.

The command argument must be enclosed by quotation marks and should be the full path to a specific executable (a binary or a script). The specified command is then tested both as a privileged command using dzdo, and as a restricted environment command for the specified user.

You must specify the full path to the command you want to test in order to fully distinguish it from other commands of the same name that may be in your current $PATH. For example, this option enables you to test whether jae_m can run /bin/ls even if root accesses the ls command in /sbin/ls:

```
dzinfo jae_m −−test "bin/ls"
```

The command results are printed to standard output.

−V, −−verbose

Provide more complete information about the DirectAuthorize configuration in the command output.

−A, −−all

Provide the most complete information about the configuration of rights and roles in the command output, including information about environment variables.

−v, −−version

Display version information for the installed software. This option cannot be combined with any other options.

EXAMPLES

To display complete configuration information for the user "molly", you would type:

```
dzinfo molly
```

If roles and rights have been configured for the user, the command displays information similar to the following:

```
User: molly
Forced into restricted environment: No
Centrify MFA Service Authentication: Supported

  Role Name        Avail Restricted Env
  ---------------  ----- --------------
  MFA1/chicago     Yes   None
  roottmp/chicago  Yes   roottmp/chicago

    Effective rights:
      Password login
      Non password login
      Allow normal shell
      Visible

    Centrify MFA Service Authentication:
      Required

    Audit level:
      AuditIfPossible

    Always permit login:
      false


  PAM Application  Avail Source Roles
  ---------------  ----- --------------------
  *                Yes   MFA1/chicago


Privileged commands:
  Name             Avail Command               Source Roles
  ---------------  ----- --------------------  --------------------
  rootany/chicago  Yes   *                     roottmp/chicago


Commands in restricted environment: root_temp_role/chicago
  Name             Avail Command               Run As
  ---------------  ----- --------------------  ----------
  rootany/chicago  Yes   *                     self
```

To test whether the user sonya is authorized to run the uname command, you could type a command similar to the following:

```
dzinfo sonya --test "/usr/bin/adflush"
```

The command displays information similar to the following:

```
Testing: User = sonya command = /usr/bin/adflush
User sonya can run the command as ’root’ via dzdo, authentication will
not be required, noexec mode is off
User sonya is not allowed to run the command in restricted environment
```

RESULT CODES

The **dzinfo** command returns the following result codes upon exit:

0 Command executed successfully.

6 The attempt to execute the command generated unexpected errors.

7 The command line contained a usage error.

9 Root privilege is required to perform the selected operation.

AUTHOR

Centrify Corporation

SEE ALSO

For related information, see the following command reference sections: dzdo(8), dzsh(1), adlicense(1)

NAME

dzsh − DirectAuthorize Restricted Environment Shell.

SYNOPSIS

dzsh [−−command *cmd_string*] [−v]

DESCRIPTION

The **dzsh** restricted environment shell is a customized Bourne shell that provides environment variables, job control, command history, and command access as defined by DirectAuthorize roles. The restricted environment shell only allows the user to run the specific commands that have been defined in the user’s assigned DirectAuthorize roles.

Note The **dzsh** shell requires that you are running Centrify DirectControl with a license.

If a user is assigned to one or more roles with a restricted environment, only one of those roles may be designated as the ’active’ role at any point in time and only the commands defined for that active role are allowed to run. Within the restricted environment, however, the user can change the active role or view information about the roles available by running the **role** command. The **role** command allows the user to list, change, and query information about the currently active and available roles.

Although **dzsh** can be used as the interpreter for a script (for example, #!/usr/bin/dzsh), this is not the intended, or recommended usage. Instead, the **dzsh** shell is intended to function as an interactive shell for restricted environment users. Those users can be given the right to run specific scripts as well as commands, where the scripts should be interpreted by an existing system shell application.

Commands in a restricted environment can be executed as the current user or a specified user. If a command is configured in DirectAuthorize to be executed as a specific user, the **dzsh** shell automatically reforms the command and executes it as the specified user, without requiring another command, such as sudo, to be used.

UNDERSTANDING THE LIMITATIONS OF THE RESTRICTED ENVIRONMENT

The restricted environment does not enforce rights for commands run outside of the shell. For example, if using a graphical desktop manager, the user can run commands and applications that are launched from menu selections in the graphical user interface.

In addition, limiting the user’s command set in the dzsh shell does not prevent the user from running built−in shell commands, accessing the file system, or seeing process or system information. For example, even in a restricted environment with no rights to run any commands, a dzsh user could get a process listing using the following script:

```
for i in /proc/[0−9]*;
  do read PROC < $i/cmdline;
  echo $PROC;
done
```

Because the shell scripting environment allows the operations, the user can effectively access information that the command set defined for his restricted environment does not allow.

USING THE ROLE COMMAND

The restricted environment shell includes the built−in **role** command. The **role** command enables the user to change the active role or view information about the roles the user has been assigned.

ROLE SYNTAX AND OPTIONS

The basic syntax for using the built−in **role** command is:

```
role [role_name] [−h] [−l]
```

If no command line options are specified, running the built−in **role** command displays the name of the currently active role.

You can set the following options with the **role** command in a DirectAuthorize restricted environment shell:

role_name Change the active role to the *role_name* specified.

−h Display the usage message.

−l List the available roles for the current user.

STARTUP AND RC SCRIPTS

The **dzsh** restricted environment shell executes the following scripts when started:

```
/etc/dzsh_profile
/etc/dzshrc
~/.dzsh_profile
~/.dzshrc
```

RETURN CODES

The restricted environment shell returns 0 if command execution is successful, or the return code of the command that failed if command execution is not successful.

EXAMPLES

After logging on as a user assigned to the role "test_lab" with a restricted environment, the **dzsh** shell displays the active role. For example:

```
You are in role: test_lab
$
```

To list all of the roles for the current user and their status:

```
$ role −l
test_lab
web_maint
backup_team
$
```

To change the active role for the user:

```
$ role web_maint
Role changed to: web_maint
$
```

If the user attempts to run a command that is not allowed in the current role and restricted environment, the **dzsh** shell will reject the command. For example:

```
$ clear
clear: command not allowed
```

To switch between roles that allow the ’id’ command to run as ’root’ (in the ’test_lab’ role) or the current user (in the ’backup_team’ role):

```
$ role test_lab
Role changed to: test_lab
$ id
uid=0(root) gid=0(root) groups=10000(samson)
context=user_u:system_r:unconfined_t
$ role backup_team
Role changed to: backup_team
$ id
uid=10000(samson) gid=10000(samson) groups=10000(samson)
context=user_u:system_r:unconfined_t
$
```

AUTHOR

Centrify Corporation

SEE ALSO

For related information, see the following command reference sections: dzdo(8), dzinfo(1), adlicense(1)

NAME

nisflush − clear the cache of NIS maps on a local computer.

SYNOPSIS

```
nisflush [--force] [--restart] [--help]
```

DESCRIPTION

The **nisflush** command can be used to clear the Centrify Network Information Service cache on a local computer or to restart the service without flushing the cache. The Centrify Network Information Service cache stores the NIS maps for network information that are retrieved from Active Directory.

To run the **nisflush** command, you must be logged in as the root user.

OPTIONS

You can use the following options with this command:

-f, --force
The **--force** option clears the cache of all data even if the Centrify adclient process is currently disconnected from Active Directory.

-r, --restart
The **--restart** option restarts NIS without flushing the cache.

-h, --help
The **--help** option displays usage information.

EXAMPLES

The **nisflush** command enables you to clear the cache for the adnisd service at any time. This command can be useful when you want to force the Centrify agent to read new information from Active Directory, or when you want to remove obsolete data from the cache. You can also use this command as part of routine housekeeping to free up disk space.

To clear the cache of NIS maps for network information from the Active Directory, you would type:

```
nisflush
```

To clear the cache of NIS maps for network information from the Active Directory when the local computer is disconnected from the network, you would type:

```
nisflush --force
```

AUTHOR

Centrify Corporation

NAME

OpenLDAP − Set of programs for performing LDAP operations

DESCRIPTION

The Centrify agent package includes a set of OpenLDAP commands that have been modified to support the Active Directory environment. The Centrify distribution of OpenLDAP supports all of the standard options and syntax for performing LDAP operations, but the ldap commands included with the Centrify agent also support the following options that are not supported in a standard OpenLDAP distribution:

−m The *−m* option allows you to use the local machine account credentials from the /etc/krb5.keytab file. This option requires root user access.

−r The *−r* option disables line wrapping when printing out LDIF entries.

The Centrify distribution of OpenLDAP also provides extended URL support for Active Directory. When you use Centrify LDAP commands, you can use the following URLs to connect to Active Directory computers:

ldap://domain_name
Connects to the appropriate domain controller for the specified domain within the Active Directory site.

ldap://
Connects to the joined domain.

gc://[domain_name]
Connects to the Global Catalog domain controller for the joined domain. You can use the optional domain_name parameter to specify a domain in a different forest.

The Centrify distribution of OpenLDAP includes the following commands: − ldapsearch − ldapadd − ldapmodify − ldapmodrdn − ldapcompare − ldapdelete

All of the commands above can be used to connect to and retrieve information from Active Directory. There are also commands in the OpenLDAP package that do not work with Active Directory. For example, you cannot use the following commands to set or retrieve information from Active Directory: − ldappasswd − ldapwhoami You can still use these commands on your Linux or UNIX computers, but not with the extended options that are specific to the Centrify distribution of OpenLDAP.

You should note that the Centrify OpenLDAP package does not include Centrify−specific man pages for the **ldap*** commands that support the extended options for connecting to Active Directory. For more information about the syntax and standard options available for individual OpenLDAP commands, see the man page for each command.

AUTHOR

Centrify Corporation

NAME

sctool − enable, disable, or diagnose smart card support.

SYNOPSIS

sctool [−e, −−enable] [−d, −−disable] [−s, −−status] [−D, −−dump] [−k, −−pkinit] [−a, −−altpkinit] [−E, −−no−eku]

DESCRIPTION

The **sctool** command allows you to enable, disable, or diagnose smart card support. You may also use the **−−pkinit** option to obtain Kerberos credentials from the smart card in the reader.

The **sctool** command is available for Mac OS X, and Red Hat Linux versions 5.6 and 6.0.

When you specify the **−−enable** option, **sctool** edits the system configuration file and adds support for smart−card login. It also creates a configuration file that directs the smart card log−in to look for a user in Active Directory with a user principal name (UPN) that is the same as the NT Principal Name attribute in the smart card log−in certificate.

When you disable smart card login with the **−−disable** option, **sctool** removes smart card support from the configuration files.

Note To run **sctool,** you must have root privilege.

OPTIONS

You can use the following options with this command:

Note You may specify only one option at a time when using **sctool.**

−e, −−enable
Enable smart card support by making necessary edits to configuration files that control authentication.

−d, −−disable
Disable smart card support by removing smart−card specific strings from the configuration files that control authentication.

−s, −−status
Show whether smart card support is enabled or disabled.

This option outputs one of these two messages:

− Centrify SmartCard support is enabled (then exits with status 0).

− Centrify SmartCard support is disabled (then exits with status 1).

Note: On Red Hat Linux systems, Centrify bypasses the native smart card infrastructure. Therefore, after you enable smart card with Centrify by enabling the group policy setting or running the **sctool** command, the **sctool −−status** command will show that smart card is enabled but the Red Hat administrative tools, such as GNOME: System > Administration > Authentication > Authentication might show that it is not enabled. You can ignore the GNOME setting because it only provides information for the native smart card configuration, which is not used by Centrify.

−D, −−dump

Display information about the system setup and about any smart cards that are attached to the machine. For each card, this option lists the type of card and any summary information. It also enumerates all identities on the card and lists the following for each:

− Subject name

− UPN (if present)

− Whether the card is trusted

− Data signing success or not

− Signature verification

−k, −−pkinit

Obtain Kerberos credentials from the smart card currently in the reader and store them in the user’s cache.

This option obtains a ticket granting ticket (TGT) using the public/private key pair stored on the smart card, which is intended to be used in the same manner as the kinit(1) command: to obtain or renew credentials when they are not handled automatically (such as a long login session during which the user does not lock the screen saver), or for troubleshooting.

In normal usage you should never need to run sctool −−pkinit.

To obtain kerberos credentials, sctool must find a certificate that matches the user, is valid for smart card login, is not expired or revoked, and is trusted by the domain. There are several ways to specify how the certificate should be found (note that only one of these options is used; sctool does not try the later options if an earlier option fails to find a certificate):

If a UPN is specified on the command line, the user’s keychains and the smart card in the reader (if any) are searched for a valid certificate that matches that UPN.

If no UPN is specified on the command line, and the CDC_SMARTCARD_TOKEN environment variable is set, the smart card named in the environment variable is searched for a valid certificate. The NT Principal Name attribute of that certificate is used as the UPN.

If the USER_PRINCIPAL_NAME environment variable is set, a certificate that matches that UPN is searched for in the same manner as in the first option.

If none of the above command−line options or environment variables are set, **sctool** looks up the user in AD to obtain the UPN, and searches for a matching certificate in the same manner as in the first option.

While **sctool −−pkinit** can use certificates that are stored in an on−disk keychain rather than a smart card, only use with a smart card is officially supported.

If no suitable certificate is found, **sctool** prints an error and exits with status 1. Otherwise, it checks whether the machine is operating in disconnected mode. If it is, **sctool** immediately

exits with status 2, since Kerberos tickets cannot be obtained in disconnected mode. This allows the authorization mechanism to permit smart card login in disconnected mode, while still verifying that the certificate on the smart card is valid and trusted.

If the machine is connected to the domain, **sctool** contacts the domain controller to obtain a TGT using the associated private key. If this fails, sctool prints an error and exits with status 1.

If the user’s password has expired, **sctool** may be unable to retrieve a TGT and will issue the message:

krb5_get_init_creds_pkinit failed: Password has expired

To resolve this issue, edit the user’s ADUC Properties page by clicking the Profile tab and checking one or both of the following options:

Account option: Smart card is required for interactive login

Password never expires.

−a, −−altpkinit <unixname>

Perform PKINIT operation using a name mapping card as smart card user <unixname>

−E, −−no−eku

Allow sctool to obtain Kerberos credentials even though the certificate does not have the extended key usage attribute. This parameter must be used with the **−k (−−pkinit)** parameter or the **−a (−−altpkinit)** parameter.

EXAMPLES

To enable smart card support:

```
# sudo sctool −e
  Password:
```

AUTHOR

Centrify Corporation

NAME

sctool − enable, disable, or diagnose smart card support.

SYNOPSIS

sctool [−−enable] [−−disable] [−−status] [−−update−upn−map] [−−dump] [−−pkinit] [−−altpkinit *unixname*] [−−clearcrls] [−−revokecheck [−t <*type*>] [−p <*priority*>] [−l <*responder*>]]

DESCRIPTION

The **sctool** command allows you to enable, disable, or diagnose smart card support. You may also use the **−−pkinit** option to obtain Kerberos credentials from the smart card in the reader.

The **sctool** command is available for Mac OS X, and Red Hat Linux versions 5.6 and 6.0.

When you specify the **−−enable** option, **sctool** edits the system configuration file and adds support for smart−card login. It also creates a configuration file that directs the smart card log−in to look for a user in Active Directory with a user principal name (UPN) that is the same as the NT Principal Name attribute in the smart card log−in certificate.

When you disable smart card login with the **−−disable** option, **sctool** removes smart card support from the configuration files.

Note To run **sctool,** you must have root privilege.

OPTIONS

You can use the following options with this command:

Note You may specify only one option at a time when using **sctool.**

−e, −−enable
Enable smart card support by making necessary edits to configuration files that control authentication.

−d, −−disable
Disable smart card support by removing smart−card specific strings from the configuration files that control authentication.

−s, −−status
Show whether smart card support is enabled or disabled.

This option outputs one of these two messages:

- Centrify SmartCard support is enabled (then exits with status 0).

- Centrify SmartCard support is disabled (then exits with status 1).

Note: On Red Hat Linux systems, Centrify bypasses the native smart card infrastructure. Therefore, after you enable smart card with Centrify (through the group policy setting or the **sctool** command), the **sctool −−status** command will show that smart card is enabled but the Red Hat system (GNOME: System > Administration > Authentication > Authentication) might show that it is not enabled. You can ignore the GNOME setting because it only provides information for native smart card which is not used by Centrify.

−u, −−update−upn−map
This option updates which field of the smart card certificate to be used as UPN search value.

[mapping] denotes the preferred field to be used to override the default field (NT Principal Name) of the smart card certificate.

−k, −−pkinit
Obtain Kerberos credentials from the smart card currently in the reader and store them in the user’s cache.

This option obtains a ticket granting ticket (TGT) using the public/private key pair stored on the smart card, which is intended to be used in the same manner as the kinit(1) command: to obtain or renew credentials when they are not handled automatically (such as a long login session during which the user does not lock the screen saver), or for troubleshooting. In normal usage you should never need to run sctool −−pkinit.

To obtain kerberos credentials, sctool must find a certificate that matches the user, is valid for smart card login, is not expired or revoked, and is trusted by the domain. There are several ways to specify how the certificate should be found (note that only one of these options is used; sctool does not try the later options if an earlier option fails to find a certificate):

If a UPN is specified on the command line, the user’s keychains and the smart card in the reader (if any) are searched for a valid certificate that matches that UPN.

If no UPN is specified on the command line, and the CDC_SMARTCARD_TOKEN environment variable is set, the smart card named in the environment variable is searched for a valid certificate. The NT Principal Name attribute of that certificate is used as the UPN. If the USER_PRINCIPAL_NAME environment variable is set, a certificate that matches that UPN is searched for in the same manner as in the first option.

If none of the above command−line options or environment variables are set, sctool looks up the user in AD to obtain the UPN, and searches for a matching certificate in the same manner as in the first option.

While sctool −−pkinit can use certificates that are stored in an on−disk keychain rather than a smart card, only use with a smart card is officially supported.

If no suitable certificate is found, sctool prints an error and exits with status 1. Otherwise, it checks whether the machine is operating in disconnected mode. If so, sctool immediately exits with status 2, since Kerberos tickets cannot be obtained in disconnected mode. This allows the authorization mechanism to permit smart card login in disconnected mode, while still verifying that the certificate on the smart card is valid and trusted.

If the machine is connected to the domain, sctool contacts the domain controller to obtain a TGT using the associated private key. If this fails, sctool prints an error and exits with status 1.

If the user’s password has expired, sctool may be unable to retrieve a TGT and will issue the message:

krb5_get_init_creds_pkinit failed: Password has expired

To resolve this issue, edit the user’s ADUC Properties page by clicking the Profile tab and checking one or both of the following options:

Account option: Smart card is required for interactive login

Password never expires.

−D, −−dump
Display information about the system setup and about any smart cards that are attached to the machine. For each card, this option lists the type of card and any summary information. It also enumerates all identities on the card and lists the following for each:

− Subject name

− UPN (if present)

− Whether the card is trusted

− Data signing success or not

− Signature verification

−S, −−support
Lists the same information as the −−dump option and additionally lists the state of the system configuration files.

−c, −−clearcrls
Remove all CRLs from keychain

−r, −−revokecheck [−t] [−p] [−l]

Extra options:

−t, −−type [ocsp|crl]:[none|best|cert|all]
Change certificate validation setting for method **[ocsp|crl]** to **[none|best|cert|all]**

ocsp :
Online Certificate Status Protocol.

crl :
Certificate Revocation List.

none :
No revocation checking is performed.

best :
The certificate passes unless the server returns an

indication of a bad certificate. This setting is best for most circumstances.

cert :
If the URL to the revocation server is provided in the certificate, this setting requires a successful connection to a revocation server and no indication of a bad certificate. Use only in a tightly controlled environment that guarantees the presence of a CRL server or OCSP responder. If a CRL server or OCSP responder is not available, SSL and S/MIME evaluations could fail to respond.

all :
This setting requires successful validation of all certificates. Use only in a tightly controlled environment that guarantees the presence of a CRL server or OCSP responder. If a CRL server or OCSP responder is not available, SSL and S/MIME evaluations could fail to respond.

−p, −−priority [ocsp|crl|both]
This setting determines which method **[ocsp|crl|both]** is attempted first. If the first method chosen returns a successful validation, the second method is not attempted.

−l, −−localocsp [ocsp server url]
This setting override OCSP server URL of certificate with **[ocsp server url]**

−a, −−altpkinit <unixname>
Perform PKINIT operation using a name mapping card as smart card user <unixname>

−E, −−no−eku <−a,−−altpkinit [unixname]
Allow sctool to obtain Kerberos credentials even though the certificate does not have the extended key usage attribute. Must be used with −a (−−altpkinit) or −k (−−pkinit) parameter.

−L, −−lock−status
Show the smart card lock status for all connected smart cards. Possible values are:

−No smart card inserted

−Authentication attempts remaining: <n>

−Card is locked

−o, −−sudo enable | disable
Enable/Disable smart card authentication for sudo

EXAMPLES

You can use **sctool** to display information about the smart cards attached to the computer:

```
$ sudo sctool −D
  Password:
```

Need some output ??

To enable smart card support:

```
# sudo sctool -e
  Password:
```

AUTHOR

Centrify Corporation

NAME

pam_centrifydc - provide authentication, account, session, and password management to any application that uses PAM.

SYNOPSIS

/lib/security/pam_centrifydc.so

DESCRIPTION

Centrify DirectControl Pluggable Authentication Module (pam_centrifydc) is a shared object that enables any application that uses PAM, such as ftpd, telnetd, or login, to authenticate users through Active Directory. When you join a domain, the pam_centrifydc module is automatically placed first in the PAM stack in system-auth, so that it takes precedence over other authentication modules.

The pam_centrifydc module is configured to work with adclient to provide a number of services, such as checking for password expiration, filtering users and groups, and creating the local home directory and default user profile files for new users. The services provided through the pam_centrifydc module can be customized locally on a computer, modified through Active Directory group policy, or configured through a combination of local and Active Directory settings.

Authentication management

The authentication module provides functions to verify the identity of a user and to set user specific credentials. It compares the password the user entered with the password returned from Active Directory through the Centrify DirectControl daemon. If the passwords match, the user is authenticated.

The following options are supported:

deny This option is used to prevent Active Directory users who type the wrong password from falling through to the next PAM module in the stack and being reprompted for a password. This option only works on systems which support the requisite flag in the pam.conf configuration file.

debug
This option logs detailed debugging information in the syslog file.

get_first_pass
This option is used to prompt all users for their password.

requisite
This option forces all of the following modules in the PAM stack to fail. This option emulates designating an authentication service as requisite in the PAM configuration file when the requisite option is not implemented in the underlying operating system (for example, the requisite flag is not supported on HP-UX).

use_first_pass
This option compares the password in Active Directory with the password entered by the user when prompted to log on. If the passwords do not match, or if no password has been entered, the authentication module quits and does not prompt the user for a password. This option should only be used if the authentication service is designated as optional in the pam.conf configuration file.

try_first_pass

This option compares the password in Active Directory with the password entered when the user authenticated to the first authentication module in the stack. If the passwords do not match, or if no password has been entered, the authentication module prompts the user for a password.

unix_cred

This option maintains RMC (role-based access control) compatibility. If **/usr/lib/security/pam_unix_cred.so** is installed on a Solaris system, DirectControl automatically adds **unix_cred** to maintain RMC compatibility.

Account management

The account management module retrieves the user’s password entry from Active Directory and verifies that the user’s account and password have not expired.

The following options are supported:

debug

This option logs detailed debugging information in the syslog file.

Session management

The session management module provides functions to initiate and terminate Unix sessions. The account management module also determines the previous time the user logged in.

The following options are supported:

debug

This option logs detailed debugging information in the syslog file.

homedir

This option creates a new home directory for the user.

Password management

The password management module provides functions to enable users to change their passwords in Active Directory. This module must be required in the pam.conf configuration file. It cannot be optional or sufficient.

The following options are supported:

debug

This option logs detailed debugging information in the syslog file.

get_first_pass

This option is used to prompt all users for their password.

requisite

This option forces all of the following modules in the PAM stack to fail. This option emulates designating an authentication service as requisite in the PAM configuration file when the requisite option is not implemented in the underlying operating system (for example, the requisite flag is not supported on HP-UX).

use_first_pass

This option compares the password in Active Directory with the user’s old password (entered to the first password module in the stack). If the passwords do not match, or if no password has been entered, the password management module quits and does not prompt the user for the old password. This module also attempts to use the new password the user entered to the first password module in the stack as the new password for this module. If the new password fails, the module quits and does not prompt the user for a new password.

try_first_pass

This option compares the password in Active Directory with the user’s old password (entered to the first password module in the stack). If the passwords do not match, or if no password has been entered, the password management module prompts the user for the old password. The module also attempts to use the new password the user entered to the first password module in the stack as the new password for this module. If the new password fails, the module prompts the user for a new password. If the user’s password has expired, the account management module saves this information, and the password management module retrieves this information to determine whether or not to force the user to update the user password.

EXAMPLES

The following example illustrates how to configure settings for the Centrify DirectControl PAM module, pam_centrifydc.so, in the /etc/pam.conf configuration file on a Solaris computer:

```
rlogin auth     sufficient  pam_centrifydc.so debug
rlogin auth     requisite   pam_centrifydc.so deny debug
login  auth     sufficient  pam_centrifydc.so debug
login  auth     requisite   pam_centrifydc.so deny debug
passwd auth     sufficient  pam_centrifydc.so try_first_pass debug
passwd auth     requisite   pam_centrifydc.so deny debug
other  auth     sufficient  pam_centrifydc.so debug
other  auth     requisite   pam_centrifydc.so deny debug
cron   account  sufficient  pam_centrifydc.so debug
other  account  sufficient  pam_centrifydc.so debug
other  session  sufficient  pam_centrifydc.so debug homedir
other  password sufficient  pam_centrifydc.so debug
```

The specific settings supported and how and where they are defined by default for Active Directory users can vary depending on your operating environment. For more information about using and configuring PAM, see the documentation for your operating environment.

AUTHOR

Centrify Corporation

SEE ALSO

For related information, see the appropriate reference section for your operating environment, for example, see pam(5) or pam_unix(5).

NAME

dzdo − execute privileged commands as a specified user on the local computer.

SYNOPSIS

dzdo −K|−k|−l|−V|−v|

dzdo [−b] [−H] [−P] [−S] [−b]| [−p *prompt*] [−u *username|#uid*] {−i | −s | *command* }

dzdo −e [−S] [−p *prompt*] [−u *username|#uid*] file

DESCRIPTION

The **dzdo** program allows a permitted user to execute a command as the superuser or another user in the Active Directory authorization store.

Note The **dzdo** command requires that you are running Centrify software with a valid license.

The **dzdo** program provides functionality that is similar to the UNIX **sudo** command, except its privileged commands are defined using Access Manager, adedit, or Centrify PowerShell cmdlets and stored in an Active Directory authorization store. In addition, only Active Directory users with a profile in the zone where DirectAuthorize rights and roles are enforced can use **dzdo** to run commands. You can, however, use **dzdo** to run privileged commands with either an Active Directory or local user as the target user. If you do not specify a user, **dzdo** attempts to execute the command as the "root" user.

The real and effective uid and gid are set to match those of the target user as specified in the user’s UNIX profile. You can configure privileged commands to require that users authenticate themselves by typing their own account password or the target user’s account password. For example, if a privileged command right is configured in DirectAuthroize to run as the root user and to authenticate using the target user’s password, running the command requires the user to know and enter root password.

Once authenticated, the user may then run **dzdo** privileged commands without re−entering a password for a short period of time. By default, the password timeout is 5 minutes but can be modified by specifying a different value with the **dzdo.password_timeout** configuration parameter in the centrifydc.conf file. You can use the **−v** option with **dzdo** to update the time stamp without running a command. The password prompt itself will also time out if the user’s password is not entered within the password timeout interval.

The **dzdo** program determines who is an authorized user by consulting the Active Directory authorization store maintained by Access Manager or Centrify command−line tools. If a user who is not authorized tries to run a privileged command using **dzdo** , a warning message is displayed except in the case where unauthorized users try to run **dzdo** with the **−l** or **−v** flags. This allows users to determine for themselves whether or not they are allowed to use **dzdo.** commands.

The **dzdo** program logs both successful and unsuccessful command execution attempts to the syslog authpriv facility or the auth facility if the authpriv facility is not supported on the platform (typically to /var/log/secure). Unsuccessful command executions are logged as errors and include the name of the user who attempted the execution, the user the unsuccessful execution ran as, and the command the user attempted to run.

You can configure **dzdo** to log only unsuccessful command execution attempts by setting the configuration parameter **dzdo.log** to false.

OPTIONS

You can use the following options with this command:

−A Gets the password from a helper program rather than from the terminal. The command will exit with an error if a helper program cannot be found.

−b Runs the specified command in the background. Note that if you use the −b option, you cannot use shell job controls to manipulate the process.

−C fileDescriptor
Does not close file descriptors before the specified number when **dzdo** exits. Normally, **dzdo** closes all open file descriptors except standard input, standard output, and standard error. This option allows you to specify a starting point above standard error (file descriptor 3). Values less than 3 are not allowed.

−e Edits one or more specified files rather than running a command.

−g group/gid
Specifies the primary group to set for the specified command.

Note: The definition for a command right contains a list of valid groups that can be used with this option; it could be restricted to certain groups or may include all valid groups. If you are uncertain about the group to specify, or see an error when running the command, check with your Centrify zone administrator.

To specify a group by GID instead of the group name, use ’#gid’. For example, to run adquery as a privileged command and set the primary group as the group with the numeric GID of 101, you could type a command similar to the following:

```
dzdo −g ’#101’ adquery
```

Note: Be certain to put single quotes around #gid.

−H
Sets the HOME environment variable to the home directory of the target user (root by default) as specified in the user’s UNIX profile. By default, **dzdo** does not modify HOME, but you can change the default behavior by setting the **dzdo.always_set_home** or **dzdo.set_home** configuration parameters in the centrifydc.conf configuration file.

Note This option has no effect if you select the Reset environment variables option for a privileged or restricted environment command in Access Manager.

−h host
Specifies a remote host on which to execute the command. The user must be authorized for the remote computer. For example:

```
dzdo −h qa1.acme.com <command>
```

When using this option, you can pass parameters to ssh for the remote connection by using the −W option.

−i Runs the login shell for the user the command is being run as. This option simulates an initial login by changing to the target user’s home directory, invoking a shell, setting the HOME, SHELL, USER, LOGNAME, and PATH environment variables, and unsetting all other environment variables.

−K Removes the user’s login timestamp entirely. This option does not require a password. After using this option, however, the next time the user attempts to run **dzdo** , it will require a password.

−k Invalidates the user’s timestamp by setting the time on it to the epoch. This option does not require a password. After using this option, however, the next time the user attempts to run **dzdo** , it will require a password. This option allows a user to revoke **dzdo** permissions from a .logout file.

−l

Lists the allowed and forbidden commands for the current user on the local host computer.

−n Prevents **dzdo** from prompting for a password.

−o opID

The **opID** (operation ID), when used in conjunction with the active role specified with the **−R** parameter, creates a secret handshake between **dzdo** and **dzsh.**

−P

Preserves the user’s group membership unaltered. By default, **dzdo** will set the group membership to the list of groups the target user is in. The real and effective group IDs, however, are still set to match the target user.

Note This option overrides the Preserve group membership option for a privileged or restricted environment command if that option is selected in Access Manager.

−p prompt

Allows you to override the default password prompt and use a custom one. The following percent (‘%’) escapes are supported:

%u Expanded to the invoking user’s login name.

%U Expanded to the login name of the user the command will be run as (defaults to root)

%h Expanded to the local host name without the domain name.

%H Expanded to the local host name including the domain name.

%p Expanded to the user whose password is asked for.

%% Two consecutive % characters are collapsed into a single % character. You can use this option with dzdo or dzedit.

−r role

Causes the new (SE Linux) security context to have the role specified by role.

−R activeRole

The **activeRole,** when used in conjunction with the operation ID specified with the **−o** parameter, creates a secret handshake between **dzdo** and **dzsh.**

−S

Reads the password from standard input instead of the terminal device. You can use this option with dzdo or dzedit.

−s

Runs the shell specified by the SHELL environment variable if it is set or the shell as specified in the user’s UNIX profile.

−t type

Causes the new (SE Linux) security context to have the type specified by type.

−T timeout

Used to set a timeout for the command. If the timeout expires before the command has exited, the command will be terminated. By default, **dzdo** does not allow timeout setting, but you can change the default behavior by setting the **dzdo.user.command.timeout** configuration parameters in the centrifydc.conf configuration file.

−u username|uid

Runs the specified command as a user other than root.

Note The **dzdo command will recognize any user name that is an equivalent of the user** name specified for the command to be run. For example, if permission is given to bob.smith (the Active Directory name) to run adinfo as a privileged command, and if bob.smith has a UNIX profile name of bsmith, you can specify either bob.smoth or bsmith when you use dzdo to run adinfo. For example:

```
dzdo −u bsmith adinfo
```

To specify a uid instead of a username, use ’#uid’. Note that you must put single quotation marks around #uid (’#uid’). You can use this option with dzdo or dzedit.

−V Displays version information for the installed software, including the version of the UNIX sudo program that dzdo is based on.

−v Validates and updates the user’s login timestamp. The option will prompt for the user’s password, if necessary. Using this option extends the **dzdo** password timeout for another 5 minutes or the timeout period set in the centrifydc.conf configuration file. This option does not run a command.

−W, sshOption

Specifies a comma−separated list of parameters to pass to ssh when executing a command on a remote host with the **−h** option. For example:

```
dzdo −h host−W,−v,−i"identityFile" "ls −la"
```

to show verbose output (−v) and specify an identity file (−i) for ssh while executing the ls −la command on the remote host.

VAR=value

Enables you to pass environment variable values to the command you are running as part of the **dzdo** command line.

Note This option has no effect if you select the "Reset environment variables" option for a privileged or restricted environment command in Access Manager.

−−

Indicates that the **dzdo** program should stop processing command line arguments. It is most useful in conjunction with the **−s** option.

RETURN VALUES

Upon successful execution of a program, the return value from **dzdo** will simply be the return value of the program that was executed.

Otherwise, **dzdo** quits with an exit value of 1 if there is a configuration or permission problem or if **dzdo** cannot execute the given command. In the latter case, the error string is printed to stderr. If **dzdo** cannot stat(2) one or more entries in the user's PATH, an error is written to stderr. (If the directory does not exist or if it is not really a directory, the entry is ignored and no error is printed.) This should not happen under normal circumstances. The most common reason for stat(2) to return "permission denied" is if you are running an auto−mounter and one of the directories in your PATH is on a computer that is currently unreachable.

SECURITY NOTES

By default, **dzdo** executes commands with a minimal set of environment variables that includes TERM, PATH, HOME, SHELL, LOGNAME, USER and USERNAME, and removes environment variables that contain special characters. You can check the default list of environment variables that **dzdo** checks by running **dzdo −V** as root. You can modify the default list of environment variables to preserve or remove using the **dzdo.env_keep** and **dzdo.env_delete** configuration parameters in the centrifydc.conf configuration file.

For security purposes, the dynamic linker on most operating systems will remove variables that can control dynamic linking from the environment for all setuid executables, including the **dzdo** program. Depending on the operating system, environment variables such as _RLD*, DYLD_*, LD_*, LDR_*, LIBPATH, SHLIB_PATH, and others are removed from the environment before **dzdo** begins execution and cannot be preserved.

To prevent command spoofing, **dzdo** checks the current directory last when searching for a command in the user's PATH. You should note, however, that the actual PATH environment variable is not modified and is passed unchanged to the program that **dzdo** attempts to execute.

The **dzdo** program will check the ownership of its timestamp directory (/var/run/dzdo by default) and ignore the directory's contents if it is not owned by root or if it is writable by users other than root. On computers that allow non−root users to give away files via chown(2), if the timestamp directory is located in a directory writable by anyone (e.g.: /tmp), it is possible for a user to create the timestamp directory before **dzdo** is run. However, because **dzdo** checks the ownership and mode of the directory and its contents, the only damage that can be done is to "hide" files by putting them in the timestamp dir. This is unlikely to happen since once the timestamp directory is owned by root and inaccessible by any other user. Any user placing files there would be unable to get them back out. To get around this issue, you can use a directory that is not world−writable for the timestamps (/var/adm/dzdo for instance) or create /var/run/dzdo with the appropriate owner (root) and permissions (0700) in the system startup files.

The **dzdo** program will not honor timestamps set far in the future. Timestamps with a date greater than current_time + 2 * TIMEOUT will be ignored and **dzdo** will log the issue and complain. This is done to keep a user from creating his/her own timestamp with a bogus date on computers that allow users to give away files.

Note that **dzdo** will only log the command it explicitly runs. If a user runs a command such as **dzdo su** or **dzdo sh** , subsequent commands run from that shell will not be logged, and **dzdo** access controls will not affect those commands. The same is true for commands that offer shell escapes (including most text editors). Because of this, you should use caution when giving users access to privileged commands through **dzdo** to verify that the command does not inadvertently give the user an effective root shell.

The administrator can ensure that only the authentic executable is executed in **dzdo** by specifying the digest in the command attribute using adedit or Access Manager.

EXAMPLES

To get a file listing of an unreadable directory:

```
% dzdo ls /usr/local/protected
```

To edit the index.html file as user webmaster:

```
% dzdo −u webmaster vi ~www/htdocs/index.html
```

To shut down a computer:

```
% dzdo shutdown −r +15 "quick reboot"
```

To make a usage listing of the directories in the /home partition:

```
% dzdo sh −c "cd /home ; du −s * | sort −rn > USAGE"
```

Note that this command line runs commands in a sub−shell to make the cd command and file redirection work.

ENVIRONMENT CONFIGURATION PARAMETERS

The following configuration parameters can be set in the centrifydc.conf file to control **dzdo** operation.

Use this parameter To do this

audittrail.dz.command.with.args

Specify whether to show command parameters in the audit log for **dzdo** and **dzsh** or just the command name. The default (false) is to show only the command name. For example, to keep passwords entered on the command line out of the log, leave this parameter set to false. Set to true to show the command parameters as well as the command name.

dzdo.always_set_home

Set the HOME environment variable to the home directory of the target user (which is root unless the −u option is used). This effectively means that the −H flag is always implied. The parameter value can be true or false. The default value is false.

dzdo.badpass_message

Specify the message displayed if a user enters an incorrect password. The parameter value can be any text string enclosed by quotation marks. The default value is "Sorry, try again."

dzdo.env_check

List the environment variables to check for % or / characters in the value and remove them from the user's environment. Variables with % or / characters are removed regardless of whether you have selected the Reset environment variables option for the command in Access Manager. The default list of variables to check is displayed when you run **dzdo −V as root. You can customize the list by modifying this configuration** parameter in the centrifydc.conf file. The parameter value can be a comma−separated list of environment variable names.

dzdo.env_delete

Specify the default list of environment variables to be removed from the user's environment. This configuration parameter only applies if you have selected the Remove unsafe environment variables option for the command in Access Manager. The variables specified with this parameter are removed in addition to the default list of variables which is displayed when you run **dzdo −V** as root. The parameter value can be a comma−separated list of environment variable names.

dzdo.env_keep

Specify the default list of environment variables to preserve in the user's environment. This configuration parameter only applies if you have selected the Reset environment variables option for the command in Access Manager. The variables specified with this parameter are preserved in addition to the default list of variables which is displayed when you run **dzdo −V** as root. The parameter value can be a comma−separated list of environment variable names.

dzdo.lecture

Control whether **dzdo** displays a warning message about using the program before displaying the password prompt. The valid parameter values are:

once To display the warning message only the first time the command is run.

never To never display a warning message.

always To display the warning message every time the program is invoked.

The default value is once.

dzdo.lecture_file

Specify the full path to a file containing the warning message you want displayed. If this parameter is not set, a default message is displayed.

dzdo.log_good

Specifies whether you want to log messages for successful command execution. By default, the **dzdo** program logs both valid and invalid command execution. If you only want to log information about invalid command execution, you can setting this parameter to false. The default value for this parameter is true. The **dzdo** program typically logs messages to the file /var/log/secure.

dzdo.passprompt

Specify the password prompt displayed. This parameter serves the same function as the **dzdo −p** command and accepts the same escapes.

dzdo.passwd_timeout

Specify the number of minutes before the dzdo password prompt times out. The default parameter value is 5 minutes.

dzdo.path_info

Specifies whether the dzdo program should inform the user when it cannot find a command in the user's PATH. By default, the parameter value is true and the program will display an error statement indicating that the command could not be found in the user's PATH. You can set this configuration parameter to false if you want to prevent **dzdo** from indicating whether a command was not allowed or simply not found.

dzdo.set_home

Set the HOME environment variable to the home directory of the target user when the −s option is used. The parameter value can be true or false. The default value is false.

dzdo.timestampdir

Specify the directory where **dzdo** stores user timestamp files. The default is directory is /var/run/dzdo.

dzdo.timestamp_timeout

Specify the number of minutes between operations during which a user need not re−authenticate. The default parameter value is 5 minutes.

dzdo.tty_tickets

Require authentication once per−tty rather than once per user. The parameter value can be true or false. The default value is false.

dzdo.validator

Specifies the full path to a script that is executed each time the **dzdo** command is run. The script is run synchronously under the user's Active Directory name.

The **dzdo** command always runs the /usr/share/centrifydc/sbin/dzcheck script before it executes the command specified. However, the distribution package does not include a dzcheck script.

You do not need to create a dzcheck script to use dzdo. You only need to create a script if you want to modify dzdo behavior. For example, if you want to prompt the user to enter some information, such as a trouble ticket number, before executing a command, you could write a script to prompt and store the information, name the script "dzcheck" and put it in the /usr/share/centrifydc/sbin directory.

Use the dzdo.validator command only if you need to specify a different path or file name. If you name your script "dzcheck" and store it at the default location, you do not need to use dzdo.validator. For example, if you want to name the script "myvalidator" and store it in the /etc/centrifydc directory, you would add the following line in the centrifydc.conf file: dzdo.validator: /etc/centrifydc/myvalidator

The **dzdo** command sets three environment variables:

DZDO_USER: the Active Directory name of the user invoking the command.

DZDO_COMMAND: the command.

DZDO_RUNASUSER: the user name under which the command is executed.

The script should return one of the following values:

0 = Success. dzdo will continue and run the command

non−zero = Failure: dzdo will not run he command. In this event, dzdo does NOT show a message on the console. If you want to notify the user of the failure, include the message in the script.

When the logging level is set to DEBUG, the call to the script and the return value are logged in var/log/centrifydc.log. If DEBUG is off, the call to the script and return value are logged in /var/log/messages.

dz.system.path

Specifies the list of common system paths for locating commands in the local operating environment. The paths specified for this parameter define the program locations searched when the System match path option is selected for **dzdo** and **dzsh** commands. This configuration parameter enables an administrator to define rights to run commands found in the user's path, the system path, or a specific location, even though the default or most commonly−used paths may be different in different operating environments. The default value for this parameter lists the most common locations for finding command line programs in the system path.

dz.user.path

Specifies the list of common user paths for locating commands in the local operating environment. The paths specified for this parameter define the program locations searched when the User match path option is selected for **dzdo** and **dzsh** commands. This configuration parameter enables an administrator to define rights to run commands found in the user's path, the system path, or a specific location, even though the default or most commonly−used paths may be different in different operating environments. The default value for this parameter lists the most common locations for finding command line programs in the user's path.

FILES

/var/run/dzdo Directory containing timestamps

AUTHOR

Centrify Corporation

SEE ALSO

For related information, see the following command reference sections: dzinfo(1), dzsh(1), adlicense(1)