[TIPS] A Centrify Server Suite Cheat Sheet

AD-bridging commands ("ad" commands)

adcheck - check OS, network and AD readiness for Centrify DirectControl

To check the system with domain (e.g. corp.contoso.com)

```
$ adcheck corp.contoso.com
```

To only perform OS checks

```
$ adcheck --test os
```

To only perform network-related tests

```
$ adcheck --test net corp.contoso.com
```

To only perform AD-related tests

```
$ adcheck --test ad corp.contoso.com
```

To check the system with a service domain controller (e.g. dc1)

```
$ adcheck --servername dc1 corp.contoso.com
```

To check connectivity only with DCs within the site

```
$ adcheck --siteonly corp.contoso.com
```

To check only on 3 (or n) DCs in a large domain

```
$ adcheck --bigdommain 3 corp.contoso.com
```

To check trust relationships (e.g. with hq.fabrikam.com)

```
$ adcheck --xdomain corp.contoso.com
```

To skip NTP checking (if you are not doing sync with AD DCs)

```
$ adcheck --skip-ntp corp.contoso.com
```

adinfo: provides information about the status of the agent

Looking-up Basic Information

To check the general status of the client

```
$ adinfo
```

To see the current domain controller the client is using

```
$ adinfo --server
```

To see the current domain the agent is joined to

```
$ adinfo --domain
```

To see the status (mode) of the agent (connected to ad or in offline mode)

```
$ adinfo --mode
```

To see the version of the installed client

```
$ adinfo --version
```

To see the corresponding Centrify Suite Version

```
$ adinfo --suite-version
```

To view Active Directory connectivity to the current domain

```
$ adinfo --test
```

To view the current Active Directory site

```
$ adinfo --site
```

To see the current joined Centrify zone

```
$ adinfo --zone
```

`$ adinfo --zonedn` (in distinguishedName format)

Advanced/Troubleshooting Information

DNS

To check for the "joined-as" name (local host name and joined as name may be different)

```
$ adinfo --name
```

To check the status of the DNS cache and stats

```
$ adinfo --diag dns
```

Connectivity

To check connectivity with an AD domain

```
$ adinfo --test [domain.name]
```

To check network connectivity statistics

```
$ adinfo --sysinfo neststate
```

To test connectivity against a specific domain controller

```
$ adinfo --T --servername [dc-name]
```

Active Directory

To see the current AD Global Catalog

```
$ adinfo --gc
```

To see the domain/forest map

```
$ adinfo --sysinfo domain
```

To see the status of the AD computer trust relationship

```
$ adinfo --sysinfo adagent
```

Testing Credentials

```
$ adinfo -A --user [username]
```

this will prompt you for a password, the output is:

```
Password for user "username" is correct/incorrect
```

Configuration

To parse the contents of the centrify.conf file

```
$ adinfo --config
```

To show the client's in memory configuration parameters

```
$ adinfo --sysinfo config
```

To show Centrify name service configuration

```
$ cat /etc/nsswitch.conf | grep centrifydc
```

Kerberos

To view Kerberos information like supported encryption types, key version and registered SPNs

```
$ adinfo --computer
```

To view the updated Kerberos configuration in the local system

```
$ cat /etc/krb5.conf
```

To list the principals in the system's krb5.conf file

```
$ dzdo /usr/share/centrifydc/kerberos/bin/klist -kt /etc/krb5.keytab
```

To determine the encryption types of the system's cached ticket

```
$ dzdo /usr/share/centrifydc/kerberos/bin/klist -fe /etc/krb5.ccache
```

PKI

adcert - a CLI-based MS PKI client

To perform auto-enrollment of Computer PKI certificates (requires elegible template and communications)

Using the computer object to authenticate

```
$ dzdo /usr/share/centrifydc/sbin/adcert --enroll --machine
```

Using a user to authenticate

```
$ dzo /usr/share/centrifydc/sbin/adcert --enroll --user [ADusername]
```

Dynamic DNS

addns - a dynamic DNS client for AD DNS or RFC 2136-compliant servers

To renew DNS using machine credentials

```
$ sudo addns --update --machine
```

To renew DNS using user credentials

```
$ sudo addns --update --user [ADusername]
```

To renew DNS only on a specific interface (e.g. eth0)

```
$ sudo addns --update --machine --interface eth0
```

Multi-factor Authentication Readiness

For MFA to work you need:

- A Centrify Identity or Privilege Service SaaS tenant or Privilege Service On Premises
- At least one Centrify Connector (multiple for redundancy)
- Your UNIX/Linux systems must trust the IWA Root Cert of the tenant OR Enterprise/Public trust is setup
- Your UNIX/Linux systems must be able to communicate to the Centrify Connector via HTTPS and the IWA port

adcdiag - performs a readiness check for Centrify Identity Platform's MFA

To check against the default tenant published in Active Directory (requires Centrify connector)

```
$ dzdo adcdiag
```

To specify the tenant URL

```
$ dzdo adcdiag --cloudurl example.my.centrify.com
```

To list the Centrify Connectors in your environment / Instance names

```
$ dzdo adcdiag --list connectors
$ dzdo adcdiag --list instance
```

To list the Centrify Connectors for a specific instance URL

```
$ dzdo adcdiag --list instance example.my.centrify.com
```

Querying Centrify-enabled AD Users and Groups

adquery: provides information about Active Directory users and groups that are UNIX-enabled by Centrify

To view all Centrify UNIX-enabled users

```
$ adquery user
```

will show all AD users in Express mode / Only authorized in Zone mode

To view all Centrify UNIX-enabled groups

```
$ adquery group
```

will show all AD groups in Express mode / Only unix-enabled in Zone mode

To view a user's entry (passwd style)

```
$ adquery user [username]
```

To view a group entry (group style)

```
$ adquery group [groupname]
```

To view only the user or group's AD group memberships

```
$ adquery user [user] --adgroup
```

To view all information about a user or group (including AD object attributes)

```
$ adquery user|group [user or group] -A
```

To view the distinguishedName a user or group

```
$ adquery user|group [user or group] --dn
```

To view all information and include password expiration, account lockout/enabled state

```
$ dzdo adquery user [user] -A
```

To view information about a computer

```
$ adquery user [computername]$ -A
```

To get results from cache (instead of fetching from AD)

```
$ adquery user|group [options] --cache-first
```

Centrify Cache Commands

adobjectrefresh - refreshes a specific user or group (requires DirectControl 5.3 and above)

To refresh a specific user object (by unix name, samaccountname, dn, upn, canonicalname)

```
$ dzdo adobjectrefresh --user fred.thomas
```

To force-refresh a specific user object (by unix name, samaccountname, dn, upn, canonicalname)

```
$ dzdo adobjectrefresh --user fred.thomas@centrif.vms --force
```

To refresh a specific group (by unix name, samaccountname, canonicalname)

```
$ dzdo adobjectrefresh --group admins
```

To refresh a specific group, but ignore members (not recursively refresh member user/groups)

```
$ dzdo adobjectrefresh --group admins --ignoremembers
```

adflush - clears the Centrify cache in the local computer (dc, gc, credential & dns)

To flush the authorization cache

```
$ dzdo adflush --auth
```

To rebind and force a new DC selection

```
$ dzdo adflush --bindings
```

To flush the DNS cache

```
$ dzdo adflush --dns
```

To expire the information from domain controllers and global catalogs

```
$ dzdo adflush --expire
```

To force complete removal/expiration even when disconnected (use carefully)

```
$ dzdo adflush --force
```

To refresh the krb5.conf file

```
$ dzdo adflush --trusts
```

To clear the health history

```
$ dzdo adflush --health
```

To clear the cloud connectors (in MFA scenarios)

```
$ dzdo adflush --connectors
```

Group Policy-related Commands

adgpupdate - triggers the group policy refresh interval

To refresh the GPOs in the system

```
$ adgpupdate
```

To refresh only computer GPOs

```
$ adgpupdate --target Computer
```

To refresh only user GPOs

```
$ adgpupdate --target User
```

adgpresult - to view a RSOP (resultant set of policy) to the local system or user

To view the report for computer and user

```
$ adgpresult
```

To view the report for the computer

```
$ adgpresult --computer
```

To view the report for the current

```
$ adgpresult --user
```

To view the report for a particular user

```
$ dzdo adgpresult --user [user.name]
```

Joining Active Directory

adjoin - joins an Active Directory domain

To run adjoin successfully, you need:

- to be root or have sudo (root-like) rights
- to have the credentials (or the keytab) of an AD user that can join computers to a container (NOT Domain Admin)
- to know the Distinguished Name (e.g. "ou=servers,ou=unix") of the container that you will place the system in AD
- to know the domain name you're joining (e.g. corp.contoso.com)
- to have a clear network path to the DC or DCs you're using (dns, global catalog, kerberos, ldap, cifs, ntp)

Sample Join Operations

To join AD in workstation/express mode (AD user must be able to add computers to "ou=workstations,ou=unix")

```
$ sudo adjoin --workstation --container "ou=workstations,ou=unix" --user
[AuthorizedADUser] --verbose [domain.name]
```

To join AD in Self-Service mode (AD/Centrify admin pre-created the machine ahead of time using Access Manager console or Centrify PowerShell)

```
$ sudo adjoin --selfserve [domain.name]
```

To join AD in zone mode (e.g. Global zone)

```
$ sudo adjoin --zone Global --container "ou=servers,ou=unix" --user [AuthorizedADUser]
--verbose [domain.name]
```

To join AD in zone mode and don't initialize (precache)

```
$ sudo adjoin --noinit --zone Global --container "ou=servers,ou=unix" --user
[AuthorizedADUser] --verbose [domain.name]
```

To join AD and trust the Computer for Delegation (must know what you're doing - security implications)

```
$ sudo adjoin --trust Global --container "ou=servers,ou=unix" --user
[AuthorizedADUser] --verbose [domain.name]
```

To join AD in workstation mode and specify a workstation license

```
$ sudo adjoin --licensetype "workstation"--workstation --container
"ou=workstations,ou=unix" --user [AuthorizedADUser] --verbose [domain.name]
```

To use an specific domain controller to join (e.g. dc1.hq.fabrikam.com)

```
$ sudo adjoin --server dc1.hq.fabrikam.com Global --container "ou=servers,ou=unix" --
user [AuthorizedADUser] --verbose [domain.name]
```

To join a Mac in Workstation mode and instruct Centrify to use the Apple algorighm to generate UID/GID scheme

```
$ sudo adjoin --enableAppleIDGenScheme --container "ou=macs,ou=unix" --user
[AuthorizedADUser] --verbose [domain.name]
```

To join AD and provide a different "AD name" than the local system name (e.g. adserver vs. localhost)

```
$ sudo adjoin --name adserver --container "ou=servers,ou=unix" --user
[AuthorizedADUser] --verbose [domain.name]
```

To join AD using keytab (kinit Authorized AD user keytab first, then run adjoin without the --user option)

```
$ env KRB5_CONFIG=[/path/to/krb5.conf] /usr/share/centrifydc/kerberos/bin/kinit -kt
/path/to/keytab [principal]
$ sudo adjoin --zone Global --container "ou=servers,ou=unix" --verbose [domain.name]
```

Leaving Active Directory

adleave - leaves an Active Directory domain

adleave by default will disable the computer account in AD (if the --remove option is not used) and will roll-back the Kerberos, PAM and NSS configuration to the state it was prior to running adjoin.

To run adjoin successfully, you need:

- to be root or have sudo (root-like) rights
- for an ″online″ leave operation, you need the credentials or an authorized AD user (or keytab)

Leave the domain and disable the computer object (orphan object left behind)

```
$ dzdo adleave --user [Authorized ADUsername]
```

Leave the domain and remove computer object (frees license)

```
$ dzdo adleave --user [Authorized ADUsername] --remove
```

Offline/forced leave (no AD connectivity required, must clean-up in AD)

```
$ dzdo adleave --force
```

Privilege Elevation ("dz" commands)

dzinfo - displays information of the user's access controls

To view self access (all)

```
$ dzinfo
```

To view the properties of the role(s), including effectiveness

```
$ dzinfo --roles
```

To view how you can access the system (PAM rights)

```
$ dzinfo --pam
```

To view the commands you can run

```
$ dzinfo --commands
```

To view the computer roles that apply to the system (requires elevation)

```
$ dzinfo --computer-role
```

To view authorization information about about another user (requires elevation)

```
$ dzdo dzinfo [user.name]
```

To test a command against the role

```
$ dzinfo --test [path/to/binary] [options]
```

Centrify-enhanced sudo

dzdo - centrify-enhanced sudo. Uses Centrify zone data in AD for commands, otherwise identical to sudo.

To view version information (as of 2015, based on sudo 1.8.10p3)

```
$ dzdo -V
```

DirectAudit Commands ("da" commands)

dainfo - shows information about the status of the audit agent

To view the audit agent status

```
$ dainfo
```

To view status with verbose output

```
$ dainfo --diag  (or dadiag)
```

To view contents of the configuration file

```
$ dainfo --config
```

To view audited status of another user (must elevate)

```
$ dzdo dainfo --username lisa.simpson
```

dacontrol - controls the status/configuration of the directaudit client (requires elevation)

To set the installation (if not set by Group Policy)

```
$ dzdo dacontrol --installation [installation-name]
```

To check if the audit agent is enabled

```
$ dzdo dacontrol --query
```

To enable direct audit

```
$ dzdo dacontrol --enable
```

To disable direct audit

```
$ dzdo dacontrol --disable
```

What happens when adjoin is run succesfully?

This activates the DirectControl agent (adclient/CentrifyDC service).

1. Creates a computer object in AD and sets SPNs for http, host, nfs, cifs, afpserver
2. Establishes a secure communication channel between the system and Active Directory
3. A forest/domain/site map is created to locate the nearest DCs
4. The Kerberos environment (krb5.conf, krb5.keytab) are maintained by Centrify (configurable). A backup is created.
5. Network time is synchronized with AD DCs (configurable)
6. The PAM (Pluggable Authentication Modules) are modified to include Centrify auth, account, password, session modules. A back-up of the previous configuration is made.
7. The NSS (Name Service Switch) providers for users and groups defaults to AD first, then other methods (e.g. files, ldap, etc). A backup of the previous configuration is made.

Note: in the OS X platform, the PAM/NSS functions are channeled via the Directory Services Plugin API.

8. An Access Control Model is enforced depending on the zone mode:

- In zone mode (licensed): Authorization (RBAC) follows zone rules (defaults to closed, only authorized users can access and enabled groups are visible)

- In express/workstation mode: Only Authentication is facilitated. The system is open for all AD users and all groups are visible.

9. Privilege Elevation: Centrify-enhanced sudo (dzdo) becomes active based on the roles/rights defined.
10. User/Group identity (RFC2307) data in AD is stored within the Centrify zone, NOT with the user/group object.
11. The virtual registry is initialized and group policies are enforced.

What happens when adleave is run succesfully?

1. Online the --remove object: The object in AD is removed from the container and from the zone (frees license)
2. Online the without --remove object: The object in AD is marked as disabled. Must be ovewritten to rejoin.
2. Offline: The object in AD is left orphaned. Cleanup must happen via API (AM, PowerShell, adedit)
3. The UNIX environment is reset and rolled back (Kerberos, PAM, NSS)
4. The Centrify adclient (CentrifyDC) service is disabled.

Important Locations

`/usr/share/centrifydc/`

bin > contains user binaries, including centrify-enhanced openldap tools like ldapsearch
sbin > contains system binaries, including adcert and centrify-enhanced OpenSSH
samples > sample files for hadoop, adedit and local account management
kerberos/bin > this is the location of the Centrify-provided MIT Kerberos tools

`/etc/centrifydc`

centrifydc > config files for the DirectControl agent
centrifyda > config files for the DirectAudit agent
ssh > config files for Centrify-enhanced OpenSSH