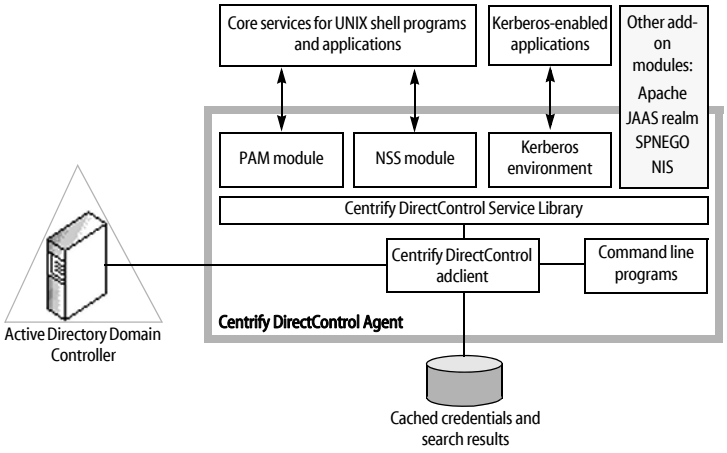
Understanding Centrify DirectControl Agents

The Centrify DirectControl Agent makes a UNIX, Linux, or Mac OS X computer look and behave like a Windows client computer to Active Directory. The Centrify DirectControl Agent performs the following key tasks:

- Joins the UNIX, Linux, or Mac OS X computer to an Active Directory domain.
- Communicates with Active Directory to authenticate users when they log on and caches credentials for offline access.
- Enforces Active Directory authentication and password policies.
- Extends Active Directory group policies to manage configuration settings for UNIX users and computers.
- Provides a Kerberos environment so that existing Kerberos applications work transparently with Active Directory.

Although the individual agents you install are platform-specific, the Centrify DirectControl Agent is a tightly integrated suite of services that work together to ensure seamless operation between existing UNIX programs and applications and Active Directory authentication, authorization, and directory service.

The following figure provides a closer look at the services provided through the Centrify DirectControl Agent:



As this figure suggests, the Centrify DirectControl Agent includes the following core components:

- The core **Centrify DirectControl Agent** is the `adclient` process that handles all of the direct communication with Active Directory. The agent contacts Active Directory when there are requests for authentication, authorization, directory assistance, or policy updates then passes valid credentials or other requested information along to the programs or applications that need this information.

- The **Centrify DirectControl Pluggable Authentication Module**, `pam_centrifydc`, enables any PAM-enabled program, such as `ftpd`, `telnetd`, `login`, and `sshd`, to authenticate using Active Directory.
- The **Centrify DirectControl NSS** module is added to the `nsswitch.conf` so that system look-up requests use the Centrify DirectControl agent to look up and validate information using Active Directory through LDAP.
- The **Centrify DirectControl command line programs (CLI)** enable you to perform common administrative tasks, such as join and leave the Active Directory domain or change user passwords for Active Directory accounts from the UNIX command prompt. These command line programs can be used interactively or in scripts to automate tasks.
- The **Centrify DirectControl Kerberos environment** generates a Kerberos configuration file (`etc/krb5.conf`) and a default key table (`krb5.keytab`) to enable your Kerberos-enabled applications to authenticate through Active Directory. These files are maintained by the Centrify DirectControl Agent and are updated to reflect any changes in the Active Directory forest configuration.
- The **Centrify DirectControl local cache** stores user credentials and other information for offline access and network efficiency.

In addition to these core components, the Centrify DirectControl Agent can also be extended with the following add-on modules:

- The **Centrify DirectControl libraries for Apache, Tomcat, JBoss, WebLogic**, or **WebSphere** plug in to the native authentication mechanisms for each Web server to enable you to configure Web applications to use Active Directory for authentication.
- The **Centrify DirectControl libraries for SAP** plug in to the native authentication mechanisms for each SAP server to enable you to configure SAP applications to use Active Directory for authentication.
- The **Centrify DirectControl Network Information Service** (`adnisd`) is a separate service that works in conjunction with the Centrify DirectControl agent to enable you to store NIS maps in Active Directory and publish that information to NIS clients through Centrify DirectControl.
- Optional utilities and programs, such as updated **Kerberos**, **OpenSSH**, **Samba**, or **PuTTY** utilities, that have been optimized to work with Centrify DirectControl and Active Directory.

Understanding the log-on process

The core Centrify DirectControl Agent components work together to identify and authenticate the user any time a user logs on to a computer using any UNIX command that

requires the user to enter credentials. The following steps summarize the interaction to help you understand the process for a typical log on request. The process is similar for UNIX commands that need to get information about the current user or group.

Note The following steps focus on the operation of the Centrify DirectControl Agent rather than the interaction between the Centrify DirectControl Agent and Active Directory. In addition, these steps are intended to provide a general understanding of the operations performed through the Centrify DirectControl Agent and do not provide a detailed analysis of a typical log-on session.

When a user starts the UNIX computer, the following takes place:

1. A `login` process starts and prompts the user to supply a user name.
2. The user responds by entering a valid local or Active Directory user name.
3. The `login` process, which is a PAM-enabled program, then reads the PAM configuration file, `/etc/pam.conf`, and determines that it should use the Centrify DirectControl PAM service, `pam_centrifydc`, for identification. The UNIX `login` process then passes the log-in request and the user name to the Centrify DirectControl Pluggable Authentication Module (PAM) service for processing.
4. The PAM service checks parameters in the Centrify DirectControl configuration file to see if the user name entered is an account that should be authenticated locally.
   - If the user should be authenticated locally, the PAM service passes the log-in request to the next PAM module in the PAM configuration file, for example, to the local configuration file `/etc/passwd`.
   - If the user is not set to be authenticated locally, the PAM service checks to see if the Centrify DirectControl agent process, `adclient`, is running. If it is, the PAM service passes the log-in request and user name to `adclient` for processing.
5. The `adclient` process connects to Active Directory and queries the Active Directory domain controller to determine whether the user name included in the request is a Centrify DirectControl user who has access to computers in the current computer's zone.
   - If `adclient` is unable to connect to Active Directory, it queries the local cache to determine whether the user name has been successfully authenticated before.
   - If `adclient` can connect to Active Directory but the user account does not have access to computers in the current zone or if the user can't be found in Active Directory or the local cache, `adclient` checks the Centrify DirectControl configuration file to see if the user name is mapped to a different Active Directory user account.
   - If the user name is mapped to another Active Directory account in the configuration file, `adclient` queries the Active Directory domain controller or local cache to determine whether the mapped user name has access to computers in the current computer's zone.

6 If the user has a UNIX profile for the current zone, `adclient` receives the zone-specific information for the user, such as the user's UID, the user's local UNIX name, the user's global Active Directory user name, the groups of which the user is a member, the user's home directory, and the user's default shell.

7 The `adclient` process checks the Centrify DirectControl authorization store to determine whether the system right for password login is enabled. If so, `adclient` goes to the next step to query NSS.

8 The `adclient` process queries through the NSS service to determine whether there are any users logged in with same UID. If there are no conflicts, the log-in request continues and `adclient` passes the request to the PAM service to have the UNIX `login` process prompt for a password.

9 The UNIX `login` process prompts the user to provide a password and returns the password to the PAM service.

10 The PAM service checks the Centrify DirectControl authorization store to verify that the user has access to the PAM login application.

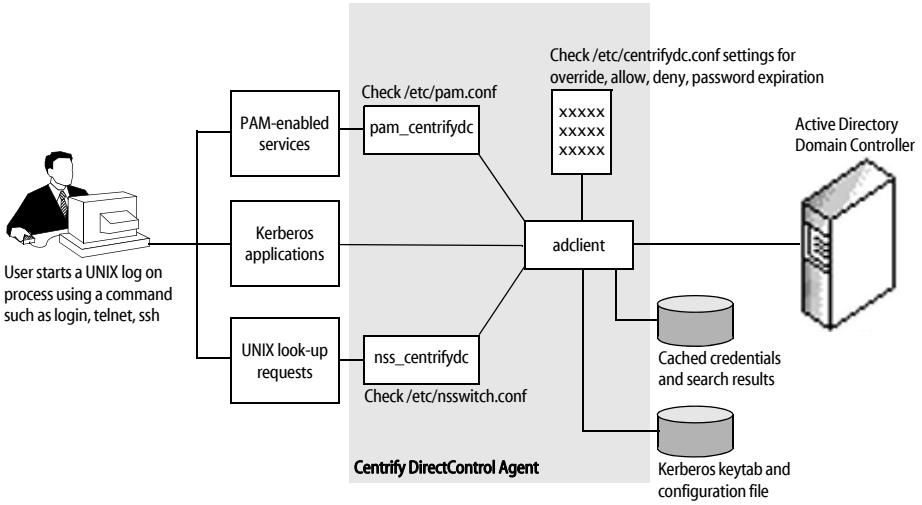
11 If the current user account is not prevented from logging on by lack of a PAM-access right, the PAM service queries `adclient` to see if the user is authorized to log on.

12 The `adclient` process queries the Active Directory domain controller through Kerberos to determine whether the user is authorized to log on to the current computer at the current time.

13 The `adclient` process receives the results of its authorization request from Active Directory and passes the reply to the PAM service.

- If the user is not authorized to use the current computer or to log in at the current time, the PAM service denies the user's request to log on through the UNIX `login` process.
- If the user's password has expired, the PAM service sends a request through the UNIX `login` process asking the user to change the password. After the user supplies the password, log-in succeeds.
- If the user's password is about to expire, the PAM service notifies the user of impending expiration through the UNIX `login` process.
- If the user is authorized to log on and has a current password, the `login` process completes successfully. If this is the first time the user has logged on to the computer through Centrify DirectControl, the PAM service creates a new home directory on the computer in the location specified in the Centrify DirectControl configuration file by the parameter `pam.homeskel.dir`.

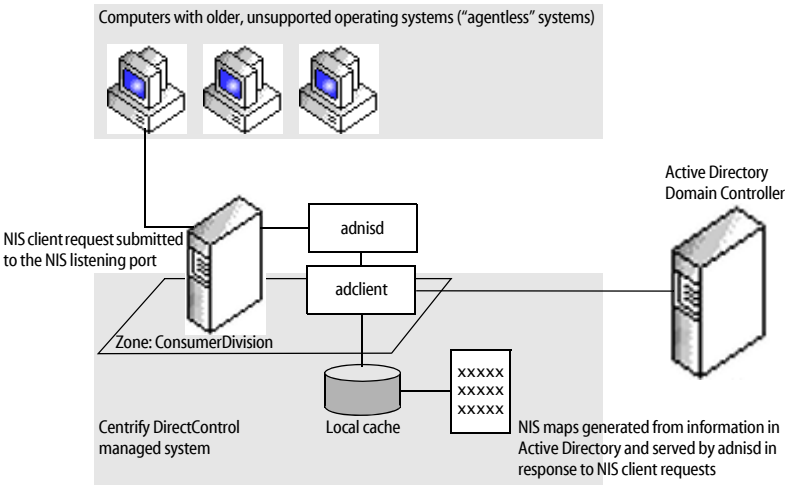
The following figure provides a simplified view of a typical log-on process when using Centrify DirectControl.



Understanding "agentless" authentication

The previous section described a typical log-on session for a Centrify DirectControl managed computer where the Centrify DirectControl Agent is installed. For computers and devices where you cannot install a Centrify DirectControl Agent, you may still be able to provide Active Directory authentication by using the Centrify DirectControl Network Information Service (`adnisd`). The Centrify DirectControl Network Information Service provides "agentless" authentication from Active Directory for computers that have older or unsupported operating systems but that can be, or already are, configured as NIS clients.

The following figure provides a simplified view of this environment.



In this scenario, the Centrify DirectControl zone acts as the NIS domain for a group of computers or devices that are configured as NIS clients. Those clients submit requests to the Centrify DirectControl Network Information Service, `adnisd`, listening on the NIS port.

The Centrify DirectControl Network Information Service periodically contacts the Centrify DirectControl Agent, `adclient`, to get updated information from Active Directory and generates a set of "maps" that it stores locally. The Centrify DirectControl Network Information Service can then use the information in these maps to respond to NIS client requests for authentication or other services.