Centrify Single Sign-On

Configuring Integration with SAP

April 2016

Centrify Corporation

Legal notice

Contents

About this guide

Centrify provides secure access control and centralized identity management for enterprises by seamlessly integrating UNIX, Linux, and Mac OS X computers, and J2EE and Web platforms with Microsoft Active Directory. With Centrify, organizations can improve IT efficiency, better comply with regulatory requirements, and move toward a more secure, connected infrastructure for their heterogeneous computing environment.

Centrify for SAP enables SAP Enterprise Resource Planning (ERP) and SAP R/3 users to authenticate to SAP via the SAP GUI client application on a Windows workstation, without having to type in a user ID and password. With this solution, users who has been properly configured with an SAP account can access the desired SAP business application using their Active Directory user credentials. The user gains single sign-on capability, increasing user acceptance and reducing support desk calls to reset passwords and unlock accounts. In addition, the administrator can disable the user account centrally in Active Directory and immediately remove the user's access to SAP.

Intended audience

Centrify Single Sign-On for SAP describes how to configure the SAP server and `SAPgui` to use Centrify and Active Directory for authentication. This guide is intended for SAP administrators and application developers who are responsible for managing user access to SAP ERP application resources.

This guide assumes you have a working knowledge of your SAP environment and are familiar with performing administrative tasks in that environment.

This guide also assumes you have the Centrify DirectManage package installed on at least one Windows computer in your environment and the Centrify agent installed on the SAP servers. See the *Administrator's Guide for Linux and UNIX* for the instructions about installing and working with the core Centrify components.

Using this guide

This guide is a supplement to the Centrify core documentation and should be used in conjunction with the additional documentation.

This book is organized into the following chapters:

- Chapter 1, "Using Centrify for single sign-on with SAP" provides an overview of how to integrate SAP with Active Directory using Centrify software and SAP Secure Network Communication (SNC).

- Chapter 2, "Configuring single sign-on for SAP using the Centrify agent" describes how to configure the SAP server to work with the Centrify agent.
- Chapter 3, "Configuring the SAP client" describes how to use the SAP client to work with Centrify and Active Directory.
- Chapter 4, "Advanced topics" addresses some common configuration issues faced by administrators after the basic deployment is finished.
- Appendix A, "Installing in clustered environments" describes how to configure Centrify for SAP for clusters with a load balancer or reverse proxy.
- Appendix B, "Troubleshooting SNC configuration" describes how to solve some common problems.

Conventions used in this guide

The following conventions are used in this guide:

- *sid*adm is used to indicate the SAP instance administrator's user name. In the production system, *sid* would be replaced by the instance's system identifier. For example, if the SAP instance was NWS, the SAP administrator's user name would be nwsadm; the identifier is always converted to lower case for the user name.
- `Fixed-width` font is used for sample code, program names, program output, file names, and commands that you type at the command line. When *`italicized`*, the fixed-width font indicates a variable. In addition, in command line reference information, square brackets (`[ ]`) indicate optional arguments.
- **Bold** text is used to emphasize commands, buttons, or user interface text, and to introduce new terms.
- *Italics* are used for book titles.
- For simplicity, UNIX is used in this guide to refer to all supported versions of the UNIX, Linux, and Mac OS X operating systems unless otherwise noted.
- The variable *`release`* is used in place of a specific release number in the file names for individual software packages. For example, `centrifydc-`*`release`*`-sol8-sparc-local.tgz` refers to the specific release of the Centrify agent for Solaris on SPARC. On the CD or in the download package, the file name always includes the product version number. For example, the Centrify agent version 5.1.3 package for Solaris running on the SPARC architecture would have the file name `centrifydc-5.1.3-sol8-sparc-local.tgz`.

Finding information about Centrify products

Centrify includes extensive documentation targeted for specific audiences, functional roles, or topics of interest. If you want to learn more about Centrify and Centrify products and

features, start by visiting the Centrify website. From the Centrify website, you can download data sheets and evaluation software, view video demonstrations and technical presentations about Centrify products, and get the latest news about upcoming events and webinars.

Additional resources

Before you begin, read the *Centrify for SAP Release Notes* included in the package for information on the SAP and Centrify versions supported in this Centrify for SAP release and other pertinent information.

SAP provides several documents that are useful sources of information. Depending on your interests, you may want to explore some or all of these sources further:

- *SAP SNC User's Guide* is the user's guide for using Secure Network Communication (SNC) in SAP Systems. It is intended for system administrators and describes how to use SNC to protect your SAP System communications.
- *SAP Note 150699* contains a list of the most recent kernels with SNC-related patches. In the related notes section, there are all Online Service and Support (OSS) notes relating to known problems and usages issues with SNC as well as information on how to collect trace information for investigating new problems.
- *SAP Note 595341* describes issues and problems with secure single sign-on, Kerberos and SNC. (You will need to refer to this note when you configure the SAP client on Windows in "Configure SNC for SAPgui for Java" on page 24.)
- *SAP Note 352295* provides information on the available options to use Single Sign-on from or among Microsoft Win32 platforms, as well as known problems on specific platforms.
- *SAP Note 121178* is the installation note for secure Single Sign-on on Windows platforms.

Contacting Centrify

You can contact Centrify by visiting our website, www.centrify.com. On the website, you can find information about Centrify office locations worldwide, email and phone numbers for contacting Centrify sales, and links for following Centrify on social media. If you have questions or comments, we look forward to hearing from you.

Getting additional support

If you have a Centrify account, click Support on the Centrify website to log on and access the Centrify Customer Support Portal. From the support portal, you can to search knowledge base articles, open and view support cases, connect with other Centrify users on customer forums, and access additional resources—such as online training, how-to videos, and diagnostic tools.

Using Centrify for single sign-on with SAP

This chapter provides an overview of how you use Centrify software for SAP to provide single sign-on to the SAP business application.

The following topics are covered:

Integrating Centrify with SAP

Integrating the SAP Secure Network Communication (SNC) with Centrify for SAP enables the following:

- Allows users to use their Active Directory credentials to access SAP with single sign-on (SSO).
- Enforces consistent passwords and other security policies.
- Extends SSO to internal users.
- Simplifies compliance with regulatory requirements.
- Maximizes the organization's investment in Active Directory

The Centrify agent provides an integration layer between Windows and other operating system platforms for authentication and group policy management. The main components are:

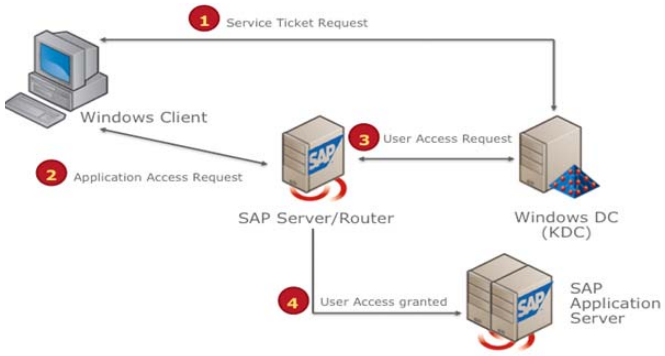
- DirectManage Access Manager is a Windows console you use to configure zones, privileges, and roles. Once you have established your zone hierarchy, privileges, and roles and assigned the roles to your Active Directory groups, day-to-day identity management can be conducted using Active Directory. Additional DirectManage tools simplify migrating UNIX users to Active Directory, deploying and maintaining the Centrify software from a central location, and centrally managing user accounts, privileges, and security policies
- Centrify agent: The Centrify agent is installed on each UNIX computer and SAP server whose users you want to migrate to Active Directory. The Centrify agent includes UNIX commands you can use to join the computer to Active Directory and to query for computer and user status.

When a UNIX computer with the Centrify agent joins the Active Directory domain, that computer essentially becomes an Active Directory client for authentication, authorization, policy management, and directory services.

To extend Active Directory authentication services to your SAP UNIX servers and Windows clients, you install an additional server-specific and client-specific library that directs client authentication requests from the SAP server through the Centrify agent to the Active Directory domain controller.

The Windows client requests a service ticket from the Kerberos Key Distribution Center (KDC). This service ticket is forwarded to the SAP application server or router. The Centrify agent on the server forwards the authentication request to Active Directory and returns the response from Active Directory back to the SAP server.

The following figure provides a simplified view of the integration between Active Directory on Windows and an SAP server hosted on a UNIX or Linux computer through Centrify.



In a standard Active Directory environment, you need to do the following before you can use Centrify for authentication in SAP:

- Prepare the Active Directory environment by installing the DirectManage tools on at least one Windows computer that is joined to the Active Directory domain.
- Install the Centrify agent on the SAP Router or SAP Application Server that has the BC-SNC module installed and join the computer to the Active Directory domain.
- Install the Centrify software package for SAP library.
- Define SAP profiles and user profiles to include the SNC mapping of the Active Directory user to the SAP user.
- Configure the `SAPgui` client to use SNC and the Centrify authentication plug in.

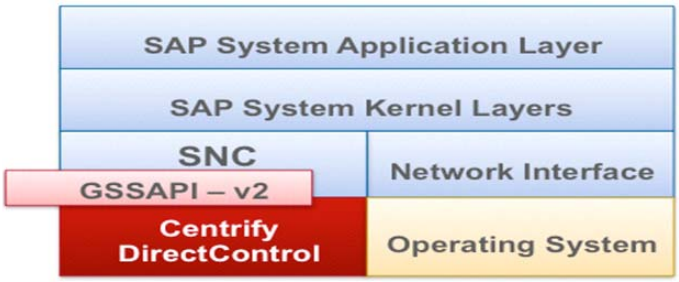
Once you have deployed the Centrify agent and configured your SAP environment to use Secure Network Communication and the Centrify modules, you can authenticate users and control access to SAP through the user's Active Directory account.

Understanding SAP Secure Network Communication (SNC)

SAP provides a standard layer for SAP R/3 and ERP called SNC (Secure Network Communication) to integrate and interface with third party security software. SNC protects the communication between SAP components (client, router, application server, and so on) and supports three protection levels:

- authentication only
- integrity protection
- confidentiality

The primary integration point for Centrify for SAP with SNC is via the GSSAPI (Generic Security Services Application Programming Interface) version 2 interface. Centrify provides authentication services for SNC as depicted in the following figure:



Understanding how Centrify integrates SAP with Active Directory

Once the SAP server has been joined to Active Directory and the SAP server and clients have been configured, users are authenticated using their Active Directory credentials. The authentication process has four stages:

1. The SAP Windows client requests a service ticket using the built-in Kerberos SSP (Security Service Provider) from the Active Directory Key Distribution Center or from the local credential cache. The `cgsskrb5.dll` library translates standard GSSAPI calls to SSP calls on the client
2. The SAP client then connects with the SAP server and presents the service ticket received in stage 1.
3. When SNC is enabled, the SAP server uses SNC to call the GSSAPI layer to authenticate the user. From this layer the call goes through the Centrify agent library to authenticate the user against her Active Directory identity. Once the request is successfully authenticated with Active Directory, the User Principal Name (UPN) is provided to the SAP server. The UPN is mapped to an SAP user as defined in the SNC tab of that user's profile.
4. When a user has logged on using an Active Directory identity, that user is mapped to the correct SAP user without having to physically provide a username or password.

Configuring single sign-on for SAP cloud-based applications

If your users access SAP servers through the SAP cloud-based applications: SAP NetWeaver Application Server ABAP or SAP NetWeaver Application Server Java, you can use Centrify Identity Service for single sign-on (SSO) as an alternative to using Centrify Server Suite as discussed in the current document.

Centrify Identify Service (CIS) is a comprehensive cloud service that secures access to cloud, mobile, and on-premises apps via single sign-on, user provisioning and multi-factor authentication.

CIS allows you to choose where to store the directory — either on-premises (within corporate control) or in the cloud. Centrify integrates the Centrify Cloud with Active Directory or LDAP without poking extra holes in the firewall or adding devices in the DMZ.

In the web-portal interface to CIS, you configure NetWeaver AS ABAP and NetWeaver AS Java for SSO by enabling SAML (Security Assertion Markup Language)-based authentication for these applications.

SAP NetWeaver ABAP and NetWeaver Java offer both IdP-initiated SAML SSO (for SSO access through the CIS web-based management portal) and SP-initiated SAML SSO (for SSO access directly through the NetWeaver ABAP or Java web application). You can configure these applications for either or both types of SSO. Enabling both methods ensures that users can log in to SAP NetWeaver ABAP or NetWeaver Java in different situations such as clicking through a notification email.

To configure the SAP NetWeaver ABAP web application for SSO, you need the following:

- A subscription to Centrify Identify Service
- SAP NetWeaver ABAP or NetWeaver Java.
- An active SAP NetWeaver ABAP or NetWeaver Java account with administrator rights for your organization.

You can find complete instructions for configuring SSO for NetWeaver ABAP and NetWeaver Java in the application configuration help included in the web-portal interface to CIS.

Configuring single sign-on for SAP using the Centrify agent

This chapter describes how to install the Centrify package for SAP and configure the SAP server for Secure Network Communication (SNC).

The following topics are covered:

- Product software
- Setting up the server environment
- Installing the host package
- Configuring SNC on Active Directory and the SAP Server

If you do not yet have the two files in the Centrify for SAP software package proceed with the next section. If you already have the host and client packages skip to Setting up the server environment.

Product software

Centrify for SAP is distributed in two files

- server package: `centrifydc-sap-`*`v.v.v-platform`*`.tar`: This file contains the software for your SAP server host. Be sure to download the package corresponding to your server platform.

  In the actual file name, *`v.v.v`* indicates the Centrify for SAP version and release number and *`platform`* indicates the SAP server host operating system.
- client package: `centrifydc_sap-`*`v.v.v`*`-win32.zip`: This file contains the Windows client software and a group policy template in the Windows Group Policy Object Editor.

If you do not have these files or you need another host package you can download them from the Centrify Customer Download Center. Go to the Centrify Customer Support Portal, login your account and go to the **Customer Download Center**. From this page, scroll down to the **SAP, Web Application & Database SSO Modules** and select the **SAP Netweaver AS ABAP SSO Module**.

The remainder of this chapter describes how to install the host package and configure your server(s). Chapter 3, "Configuring the SAP client" describes how to install the Windows client and group policy template.

Setting up the server environment

See the SAP release notes for the Centrify agent and SAP versions supported.

The Centrify agent must be installed on the UNIX host computer where the SAP ERP server has been installed or where the SAP router resides. The computer or router must be joined to an Active Directory domain controller. Use the Centrify adjoin command to join the SAP server or router computer to Active Directory. You can join in either workstation or zone mode:

- Workstation mode: Every Active Directory user and group Active Directory user and group defined in the forest (plus any users defined in a two-way trusted forest) are valid UNIX users or groups. Use this mode if you just want single sign on support based on the user's Active Directory account. For example,

  ```
  adjoin acme.com -w - u admanager
  ```

  where "acme.com" is the domain name and "admanager" is the account name of a user with sufficient rights on the Active Directory domain controller to add a computer to the specified domain and create new computer accounts. (The user will be prompted to enter the admanager password.)

- Zone mode: Only the users and groups defined in the Centrify zone are valid UNIX users and groups). Use this mode if you want to extend the use of Active Directory to include centralized management of UNIX system access control and system administrator privilege management. For example,

  ```
  adjoin acme.com -z hr -u admanager
  ```

  where "`acme.com`" is the domain name, the "`hr`" is the Centrify zone in which to put the SAP server and "`admanager`" is the account name of a user with sufficient rights on the Active Directory domain controller to add a computer to the specified domain and create new computer accounts. (The user will be prompted to enter the `admanager` password.)

Typically, the adjoin command for a "zoned" computer is a bit more complex than this example. For more information about `adjoin` and its options, see the `man` page for the `adjoin` command.

The *sid*adm (see Conventions used in this guide) must have read access privileges to the Kerberos key table (for example, /etc/krb5.keytab on most UNIX systems) on the server. See "Configure the sidadm OS profile" on page 14 for the explanation.

Installing the host package

The Centrify for SAP installation package file name is in the form

`centrifydc-sap-`*`v.v.v-platform`*`.tar`

where

- *`v.v.v`* indicates the package's current version and release numbers

- *platform* is an abbreviation for the host operating system; for example, AIX, HPUX, RHEL (Red Hat Enterprise Linux)

To install Centrify for SAP, copy the package corresponding to your host operating system to the root directory of the SAP server and use the following command to untar the file. No files, however, are placed in the root directory.

```
tar -xvf centrifydc-sap-release-platform.tar
```

Note Set permissions so that the *sid*adm has access to the directory with `snckrb5.*` file.

Configuring SNC on Active Directory and the SAP Server

This section explains how to set up the Active Directory account for SAP and configure the SAP server to use Secure Network Communications (SNC).

The `keytab` file contains entries of keys for Service Principal Names (SPNs) serviced by this server. When a computer is joined to Active Directory, Centrify updates the Kerberos `keytab` key table file. One of the entries, in the form of `hostname$`, is the sAMaccount name of the computer account. You can use this name as the SNC name of the SAP server. If you do not use the hostname$ you have to create a separate SAP service, service principal name and keytab key table.

To start, you need to confirm that the default keytab table contains a separate hostname entry. To view keytab entries use the following command:

```
/usr/share/centrifydc/kerberos/bin/klist -k
```

For example, the `klist -k` command would show the following entry for a server named `sapbox2.`The last entry, `sapbox2$CENTRIFY.SE`, is the sAMaccount name.

```
# /usr/share/centrifydc/kerberos/bin/klist -k -t
Keytab name: FILE:/etc/krb5.keytab
KVNO Timestamp         Principal
---- ----------------- --------------------------------------
   5 01/01/14 19:16:30 host/sapbox2.centrify.se@CENTRIFY.SE
   5 01/01/14 19:16:30 host/sapbox2@CENTRIFY.SE
   5 01/01/14 19:16:30 ftp/sapbox2.centrify.se@CENTRIFY.SE
   5 01/01/14 19:16:30 ftp/sapbox2@CENTRIFY.SE
   5 01/01/14 19:16:30 cifs/sapbox2.centrify.se@CENTRIFY.SE
   5 01/01/14 19:16:30 cifs/sapbox2@CENTRIFY.SE
   5 01/01/14 19:16:30 HTTP/sapbox2.centrify.se@CENTRIFY.SE
   5 01/01/14 19:16:30 HTTP/sapbox2@CENTRIFY.SE
   5 01/01/14 19:16:30 sapbox2$@CENTRIFY.SE
```

Configure the *sid*adm OS profile

Add the following `setenv` and `kinit` commands to the *sid*adm's startup file `/home/sidadm/.cshrc` to perform the following functions:

- `setenv`: Ensure that `LD_LIBRARY_PATH` is defined and set the library path to point to the Centrify for SAP library. Include the following directories in your `LD_LIBRARY_PATH`

Platform	Directories
Linux 32-bit	`/usr/share/centrifydc/kerberos/lib` `/usr/share/centrifydc/lib`
Linux 64-bit	`/usr/share/centrifydc/kerberos/lib64` `/usr/share/centrifydc/lib64`
Solaris 32-bit	`/usr/share/centrifydc/kerberos/lib` `/usr/share/centrifydc/lib`
Solaris 64-bit	`/usr/share/centrifydc/kerberos/lib/sparcv9` `/usr/share/centrifydc/lib/sparcv9`
HPUX 64-bit	`/usr/share/centrifydc/kerberos/lib/hpux64` `/usr/share/centrifydc/lib/hpux64`
AIX 64-bit	`/usr/share/centrifydc/kerberos/lib64` `/usr/share/centrifydc/lib64`

- `kinit`: obtain and cache a Kerberos ticket-granting ticket for *sid*adm when *sid*adm logs in.

Note On Linux systems, the default library load path must come before the Centrify library load path. For example, in a Linux 64-bit environment you would add the following commands:

```
if ! $?LD_LIBRARY_PATH setenv LD_LIBRARY_PATH
setenv LD_LIBRARY_PATH /usr/share/centrifydc/kerberos/
lib64:${LD_LIBRARY_PATH}:/lib64:/usr/share/centrifydc/lib64
/usr/share/centrifydc/kerberos/bin/kinit -k hostname$
```

After you update the `.cshrc` file, log in as the *sid*adm, run the `klist` command and verify that the default principal is *`hostname`*`$`. For example, a server name sapbox2 would show the following:

```
# /usr/share/centrifydc/kerberos/bin/klist
Ticket cache: FILE:/tmp/krb5cc_531
Default principal: sapbox2$@CENTRIFY.SE
Valid starting     Expires            Service principal
01/15/14 12:48:43  01/15/14 22:48:45  krbtgt/CENTRIFY.SE@CENTRIFY.SE
renew until 01/16/14 12:48:43
```

Note The *sid*adm requires read and write permissions for `/etc/krb5.keytab`. Add *sid*adm to the root group and add the appropriate permissions to the keytab file using the following command.

`chmod g+rw /etc/krb5.keytab`.

Renewing the Kerberos ticket

By default the Kerberos ticket expires every 10 hours. Set up a `cron` job to renew the ticket every 8 hours. The following instructions describe how to renew the Kerberos ticket using the sAMaccount name of the SAP server computer.

Note The `kinit` command used in the following instructions should be identical to the one configured in the `.cshrc` file (see Configure the sidadm OS profile).

Log in as *sid*adm and edit the `crontab` file to add the following lines, replacing the Kerberos principal *`hostname`*`$` with your own.

```
01 00 * * * /usr/share/centrifydc/kerberos/bin/kinit -k hostname$
01 08 * * * /usr/share/centrifydc/kerberos/bin/kinit -k hostname$
01 16 * * * /usr/share/centrifydc/kerberos/bin/kinit -k hostname$
```

For example, `crontab` file would include the following lines for SAP server name sapbox2:

```
01 00 * * * /usr/share/centrifydc/kerberos/bin/kinit -k sapbox2$
01 08 * * * /usr/share/centrifydc/kerberos/bin/kinit -k sapbox2$
01 16 * * * /usr/share/centrifydc/kerberos/bin/kinit -k sapbox2$
```

Note If you are using a cluster in a load balancing configuration, replace the *hostname$* with the UPN for the Active Directory account you created in Step 2 on page 32 of the cluster configuration instructions for a load balancer. For example, using the example UPN from those instructions, you would add the following lines.

```
01 00 * * * /usr/share/centrifydc/kerberos/bin/kinit -k
  centrifyprod@ace.com
01 08 * * * /usr/share/centrifydc/kerberos/bin/kinit -k
  centrifyprod@ace.com
01 16 * * * /usr/share/centrifydc/kerberos/bin/kinit -k
  centrifyprod@ace.com
```

Modify SAP to use Secure Network Communications

You must modify the following two SAP profiles to use Secure Network Communications (SNC) with the Centrify library.

- SAP default profile
- SAP instance profile

Note You use the SAPgui transaction RZ10 to modify both profiles. You must have SAP administrative authorization to modify the SAP profile in RZ10.

Modify the SAP default profile

The SAP default profile is called `DEFAULT.PFL` and is located in the global profile directory of the SAP system. For example, under UNIX the default location is the directory `/usr/sap/`*`SID`*`/SYS/profile` where *`SID`* is the SAP system ID.

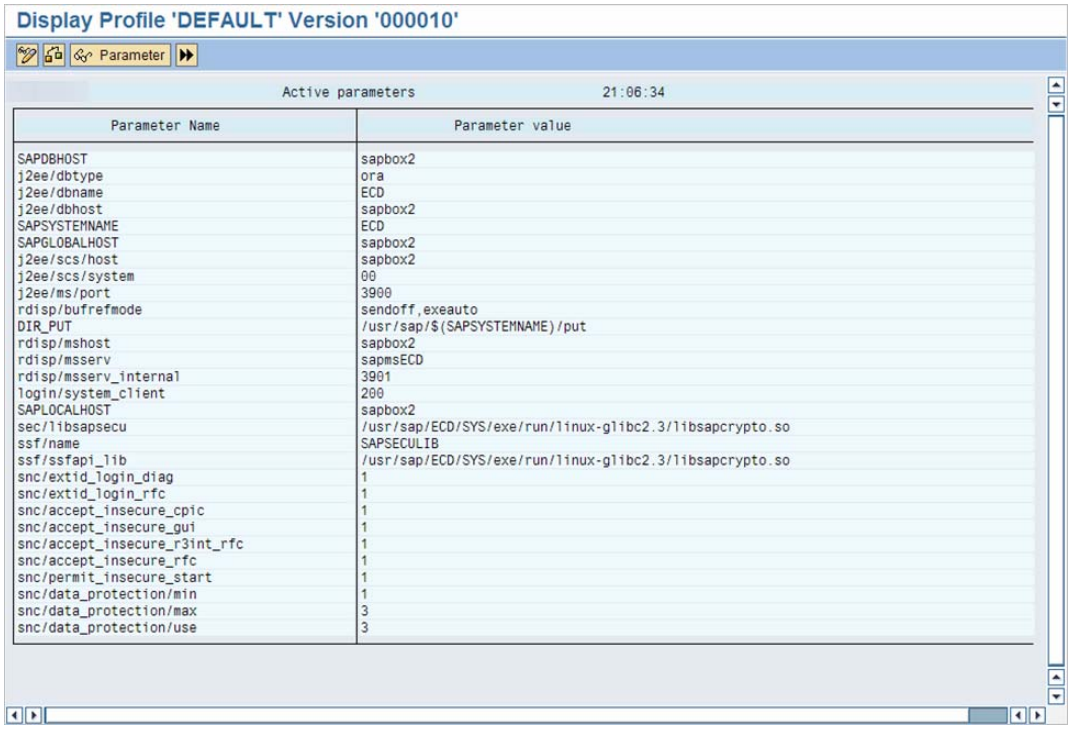
Note Try not to make profile parameter changes at the OS level. Make your profile changes using the SAP RZ10 transaction.

1 In SAP, use SAPgui transaction RZ10 (Edit Profiles).

2 In the Edit Profiles page, select the Default profile and add the following parameters:

```
snc/extid_login_diag = 1
snc/extid_login_rfc = 1
snc/accept_insecure_cpic = 1
snc/accept_insecure_gui = 1
snc/accept_insecure_r3int_rfc = 1
snc/accept_insecure_rfc = 1
snc/permit_insecure_start = 1
snc/data_protection/min = 1
snc/data_protection/max = 3
snc/data_protection/use = 3
```

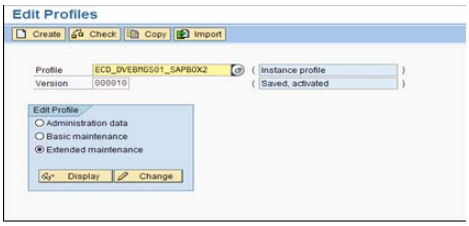
The following figure shows the profile after editing:



Modify the SAP instance profile

1 In SAPgui transaction RZ10 (Edit Profiles) select the SAP instance profile, *SID_instance_name_hostname*. For example, in the following figure and sample

commands `ECD` is the `SID`, `DVEBMGS01` is the instance name and number, and `sapbox2` is the SAP server name.



2 Add the following to this instance profile. Parameter values displayed in italics should be replaced with the correct information for your environment.

```
snc/enable = 1
snc/gssapi_lib=/usr/share/centrifydc/kerberos/lib/snckrb5.so
```

The actual location of the `snckrb5.so` (or `.a` on AIX) file depends upon your host platform. See the table in "Installing the host package" on page 13 for the exact locations.

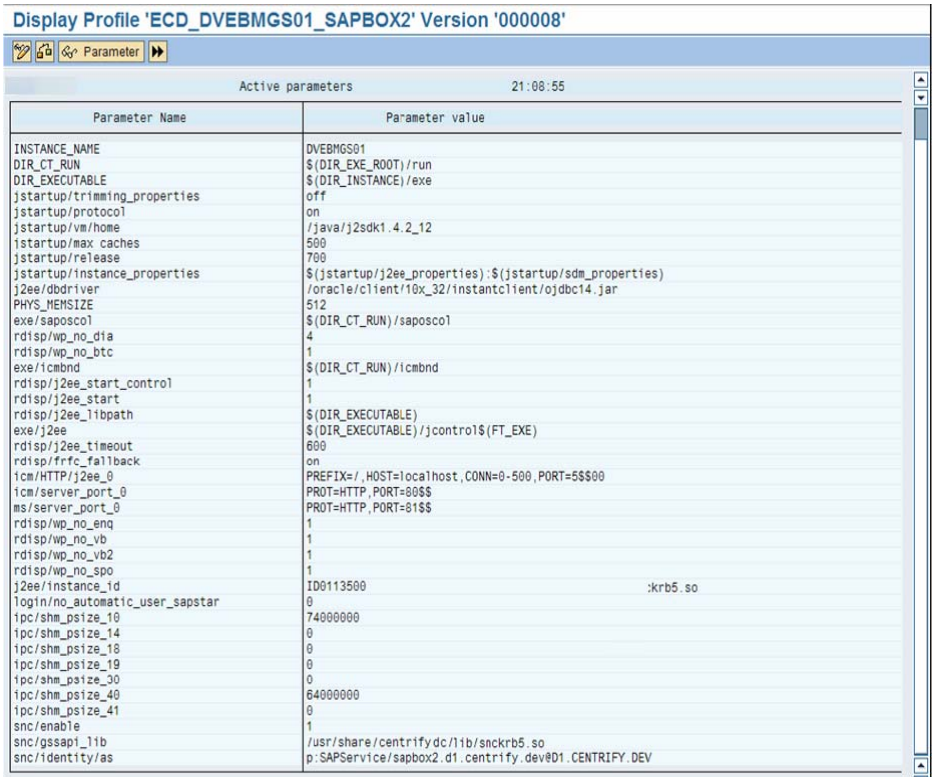
3 Add the following `snc/identify/as` to the instance profile.

```
snc/identity/as=p:hostname$@domain
```

For example, using the SNC name from previous examples the entry would be as follows:

```
snc/identity/as=p:sapbox2$@CENTRIFY.SE
```

The following figure shows the instance profile after editing and using the default location of `snckrb5.so` in a 32-bit Linux system for `snc/gssapi_lib`. The `snc/identity/as` parameter in your system will be different.



Modify the SAP instance profile to suppress prompt for password change

Once you have set up the system for single sign on using the Active Directory account, you need to suppress SAP from prompting the user for a password change. Use the SAPgui transaction RZ10 (Edit Profiles) to select the SAP instance profile and enter the following parameter:

```
login/password_change_for_SSO=0
```

This profile parameter determines precisely how SAP responds when users accesses the system using single sign-on the first time and when their password is expired. The parameter supports the following valid values:

0 = Ignore password change request, and allow access

1 = Present a pop-up window with options 2 and 3 below

2 = Require the password be changed, including old password and new password

3 = Deactivate the password

The default setting is 1, which forces the user to change the password. You can also set this parameter dynamically using RZ11 without restarting the computer. However, you must modify the profile to make the change permanent.

In addition, confirm that the `login/password_expiration_time` parameter is set to 0 (the default value). If the value is not 0, use SAPgui transaction RZ10 (Edit Profiles) to select the SAP instance profile and enter the following:

```
login/password_expiration_time=0
```

Restart SAP and verify SNC is enabled

After editing the profile on the computer running SAP, execute the following commands:

```
# su - sidadm
# stopsap
```

(wait for the SAP services to stop)

```
# startsap
```

After SAP is again running, check the `dev_w0` log file for the string `"SNC (Secure Network Communication) enabled"`. For example:

```
# cat /usr/sap/SID/instance_name_and_number/work/dev_w0 | \
grep "SNC (Secure Network Communication) enabled"
```

where *`SID`* is the SAP system ID and *`instance_name_and_number`* are the SAP instance name and instance number. For example, if in SAP 7.4 the system ID was HP2, the instance name was `DVEBMGS` and the instance number was `01` the log file would be

```
/usr/sap/HP2/DVEBMGS01/work/dev_w0
```

If this string is present in the log file, then SAP is properly configured with Secure Network Connection.

Mapping Active Directory Users to Corresponding SAP Users

To provide single sign on for SAP users you need to add and configure the domain users who require access to SAP.

In SAP, use transaction SU01.

Use Step 1 through Step 3 to add users to SAP. Skip to Step 4 for users who already have SAP accounts.

1. In the User Maintenance: Initial Screen page, enter the user name in the **User** field. Click the **Create** button or press **F8**.
2. In the Maintain User page **Address** tab, enter at least the **Last Name** (mandatory).
3. In the Maintain User page, click the **Logon Data** tab and do one of the following:
   - Enter an initial password if you want the user to have a separate password for SAP.
   - Deactivate the password if you want the user to have single sign-on to SAP via SNC.
4. In the Maintain User page, click the **SNC** tab and specify the Windows user account that is assigned to that SAP user ID as follows:
   `p:ActiveDirectoryUser@DOMAINNAME`

An example is `p:janedoe@CENTRIFY.COM`.

Note The domain name must be all uppercase letters.

5 Click **Save** to save your changes.

Configuring the SAP client

This chapter explains how to configure the SAP client environment for Secure Network Communication (SNC) to enable single sign-on (SSO) for SAP users. Perform these steps on each Windows client computer.

Note Shortcuts are typically insecure and use locally stored usernames and passwords. One benefit of Centrify for SAP is that once SSO is configured for SAP users, you can set up shortcuts for them without the need to store vulnerable passwords. You can use any password to create a shortcut, because SNC first attempts to authenticate using the Centrify GSSAPI library.

The following topics are covered:

Configure SNC for SAPgui Win32

You can configure SNC for SAP using either SAPgui Win32 as explained in this section or using SAPgui for Java; see "Configure SNC for SAPgui for Java" on page 24.

Apply the SAPSSO patch

To turn on SNC and SSO for the Win32 version of SAPgui, first apply the `sapsso.msi` patch according to *SAP Note 595341 Installation issues with Single Sign-On and SNC*. The SAP SNC patch can be downloaded as the attachment SAPSSO.ZIP to SAP note 595341 on the SAP Service Marketplace.

After the patch is applied, use the following steps to create an SNC connection.

1. Launch the **SAPLogon** Win32 program. On the **Systems** tab, click **New Item** to create a new connection to the application server where SAP is installed.
2. Enter the description, the application server where SAP is installed and the System ID and System number of your SAP instance.
3. Click the **Advanced** button to open the **Advanced Options** page.

4 Select the **Enable Secure Network Communication** check box and enter the SNC name in the form:

`p:`*`hostname$@domain`*

where *`domain`* is the kerberos_realm (in all uppercase).If *`domain`* is omitted, the SAP uses the current kerberos_realm (that is, the current domain).

5 Click **OK**.

You should now be logged onto SAP using SNC.

Configuring SNC

Before you can configure the Win32 SAPgui to turn on Secure Network Connection and single sign on, you need install the Centrify for SAP client software. The Centrify for SAP client software installation file is in the `centrifydc_sap-`*`v.v.v`*`-win32.zip` file.

To proceed, extract the files from `centrifydc_sap-`*`v.v.v`*`-win32.zip`. In this section you use the `CentrifyDC_SAPClientAgent-`*`v.v.v`*`-win32.msi` file only.

Note The `centrify_sap_settings.xml` file contains group policy templates if you want to enforce password re-prompting rather than SSO for some users. See Configuring password re-prompting in Centrify for SAP client for the installation instructions.

Use the following steps to configure an SNC connection:

1 Run `CentrifyDC_SAPClientAgent-`*`v.v.v`*`-win32.msi` to install the Centrify for SAP client package on the Windows computer (where *`v.v.v`* is the Centrify for SAP version and release numbers).

2 Launch **SAPLogon Win32**, then create a new item.

3 Enter the description, the name of the application server where SAP is installed, and the System ID and number of your SAP instance.

4 Click the **Advanced** button, and then select the **Enable Secure Network Communication** check box and enter the SNC name in the following form:

`p:`*`hostname$@domain`*

For example:

```
p:vmrhel3sap@CENTRIFY.COM
```

5 Select one of the available security levels (**Max Available** is selected by default). Click **OK**.

You are now logged into SAP using Secure Network Communication.

Note If you want, you may now create shortcuts for SAP users without needing to take security concerns into account. See "Creating shortcuts" on page 24.

Configure SNC for SAPgui for Java

Use the following steps configure SNC for SAP using the SAPgui for Java.

1 Launch the SAP Java client. Use the Add New Connection page to create a new connection.

2 Enter a description and click the **Advanced** tab.

3 Select the **use expert configuration** check box and enter the appropriate connection string, for example:

```
conn=/H/VMRHEL3SAP/S/3200/
  &sncname=p:vmrhel3sap@CENTRIFY.COM&sncon=true&sncqop=4
```

Click the **Help** button for more information.

In this example:

`conn`	=	/H/*SAP_host*/S/*service_name*
`sncname`	=	SNC name of the SAP system
`sncon`	=	Set `true` to use SNC for the connection
`sncqop`	=	1 - authentication 2 - integrity 3 - encryption 4 - all three

4 Save the connection configuration.

5 Select the saved connection and click **Connect**.

6 You are now logged into SAP using Secure Network Connection.

Creating shortcuts

Shortcuts, with locally stored usernames and passwords, are normally very insecure. However, one benefit of using single sign-on provided by Centrify for SAP is that once single sign-on is configured for SAP users, shortcuts can be set up for users without the need to store a vulnerable password.

To create a shortcut, type in any password—it does not need to be valid—to cause SNC to try to authenticate using the Centrify GSSAPI authentication mechanism.

Configuring password re-prompting in Centrify for SAP client

For some users, silent authentication via Kerberos is not acceptable policy. For example, consider the HR user who has access to sensitive compensation, benefits, and healthcare

information for employees. Many corporations have a policy that requires users to reconfirm their credentials rather than allowing silent authentication to applications that contain sensitive data.

In this case, re-prompting can be enabled for select client machines or users.When it is enabled the user is prompted with a Centrify login screen.

This scenario is also useful to log in using a different Active Directory user account. For example, an SAP administrator might want to log in to several SAP accounts mapped to different Active Directory IDs. Re-prompting allows the administrator to log in with a different user ID without having to first log out of the current Windows session.

There are two ways to enable re-prompting:

- Set a group policy
- Modify the registry entries on each computer

Both methods provide the same results; however, using a group policy is much easier.

Set a group policy

Note To use a group policy to enable re-prompting, you need to be able to set group policy on the Active Directory domain controller. The following instructions assume that you have sufficient permissions to run the group policy object editor and add the Centrify for SAP template.

There are three policies for enabling and managing re-prompting:

- **Reprompt Kerberos Credentials Dialog**: Enable this policy to reprompt the user to enter a password when accessing the SAP service. The default is **Not configured**.
- **Allowed password entry attempts**: Enable this policy to set the number of retries. The default is **Not configured**.
- **Disable remember password**: Enable this policy to force the user to enter the password. The default is **Not configured**. When this policy is set to **Not configured** or **Disabled**, the user can choose to have the password remembered.

To use these policies you have to add the `centrify_sap_settings.xml` template to the group policy editor. Use the following procedure to add the template file and then enable the **Reprompt Kerberos Credentials Dialog** policy.

1. Move the `entrify_sap_settings.xml` file you extracted from the `CentrifyDC_SAPClientAgent-`*`v.v.v`*`-win32.msi` file in Configuring SNC to the `C:\Program Files\Centrify\Centrify\group policy\policy` directory. (This is the same folder that contains all of the other Centrify Suite group policy templates.)
2. Next, open the Windows Group Policy Editor to add the template. Right click the **Centrify Settings** node and select **Add/Remove Templates**.

Note The Group Policy Editor might contain other Centrify group policy templates that were previously loaded. See the *Group Policy Guide* for a description of the other Centrify policies.

3 Click **Add** and then select `centrify_sap_settings`. Click **Open**.

4 In the Add/Remove Templates window, `centrify_sap_settings.xml` is now in the list. Click **OK**.

This completes adding the template. The Centrify SAP Settings policies are now listed in the Centrify Settings node in the Group Policy Editor. To enable a policy, right click the policy and then select Properties.

Modify the registry entries

To configure the use of credential re-prompting, you can also use the following registry entries. You need to modify the registry on each client machine.

Registry Entry	Options
`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Centrify\SAP\DoRepromptCred`	When this key equals 0 (zero) re-prompting is turned off unless a valid Kerberos ticket is not available (default value). When this key equals 1 (one) re-prompting is performed every time regardless of the validity of Kerberos ticket.
`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Centrify\SAP\KerberosPasswordRetry`	This key may have a value of 1-9999 depending on the number of retries you want to allow a user to have before an error is returned.
`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Centrify\SAP\AllowPassSave`	When this key equals 1 (one) a user is allowed to save his/her password for re-prompting When this key equals 0 (zero) a user is NOT allowed to save his/her password for re-prompting (default value).

Advanced topics

While the previous chapters provide the basics to integrating SAPgui to a SAP server instance via SNC and providing single sign on using the user's Active Directory credentials, this chapter addresses the following advanced topics for your consideration on an as needed basis.

- Configuring SNC for logon groups
- Pattern based mapping of Active Directory users to SAP users
- Central deployment of Centrify for SAP client library

Configuring SNC for logon groups

A common configuration is to deploy several SAP instances to provide adequate load balancing and failover. Typically, this involves defining a logon group with multiple SAP instances. You can use SAP transaction SMLG to manage logon groups and verify the SNC status of the servers in each group.

Each instance in the logon group should be SNC enabled. When a logon entry is created using Logon Groups instead of Server Selection, the SAP instance is selected dynamically at logon time. As a result the message server will provide the SNC name dynamically when the logon request is received. For this reason, do not enter an SNC name at the time the logon entry is configured; instead, select the checkbox to enable SNC and the level of desired protection.

Pattern based mapping of Active Directory users to SAP users

One of the challenges of deploying a single sign on solution for SAP is the mapping of individual SAP user accounts to their network identity (Active Directory user/ SNC name).

If the majority of the users already have the same user name in SAP as in Active Directory, SAP has a transaction that may be of help. Transaction SNC1 generates an SNC user name for each user in an SAP instance.

This can be done with a prefix and postfix as in the following screenshot:

Note The Active Directory user name (UPN) must match exactly, including the same character case, with the SNC user name of the SAP user.

All of the SNC name mappings are held in a single table in SAP (USRACL) that you can access using transaction SM30.

Central deployment of Centrify for SAP client library

The client library, `CentrifyDC_SAPClientAgent-release-win32.msi`, can be centrally deployed and installed using group policy in Active Directory or through other third party deployment or desktop management tools. In order to successfully deploy the product it may be helpful to understand what the installer does so that it can be replicated as part of the deployment process.

First, the file cgsskrb5.dll is installed, typically in `c:\windows\system32`.

Second, a system environment variable needs to be set to point to this file. For example:

```
SNC_LIB=c:\windows\system32\cgsskrb5.dll
```

Most desktop management tools can distribute either the .msi or perform the previous steps to deploy the client to the appropriate client machines.

Installing in clustered environments

This appendix explains how to install the Centrify for SAP package in a clustered environment.

The following topics are covered:

Centrify software requirements

When you set up SAP servers in a cluster, each server and, if you are using a reverse proxy the reverse proxy computer as well, must have the following Centrify software installed:

- All UNIX-based systems: The Centrify agent (`adclient`) must be installed. Run `adinfo` on each server to confirm that the Centrify agent is installed. (Windows-based servers do not require Centrify agent.)
- All UNIX- and Windows-based systems: The Centrify for SAP software must be installed.

Note A load balancer is an exception to this rule. If you are using a load balancer, do not install the Centrify agent or the Centrify for SAP software on the load balancer.

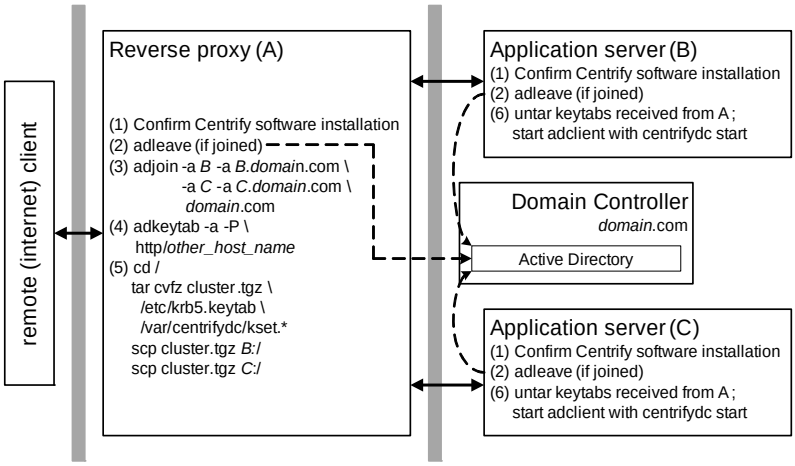
In addition, the Kerberos keytabs for each server must be the same. The following instructions tell you how to copy the keytab across systems.

The next two sections provide sample, step-by-step instructions you can customize for your environment to set up Active Directory authentication in a clustered environment with a reverse proxy and then with a load balancer.

Configure a clustered environment with a reverse proxy

This section assumes that you are installing the Centrify for SAP package in a cluster that has a reverse proxy with multiple servers on the back end.

In the following example, the reverse proxy is running on a machine named A, internal back-end SAP servers are running on machines named B and C, and the domain is *domain*.com. The figure summarizes the steps and where they are carried out.



1. Confirm that you have the Centrify agent (`adclient`) and the Centrify for SAP package installed as required.
2. If the servers are joined to the domain controller (run `adinfo` to find out), run `adleave` on each UNIX machine to "unjoin."
3. On machine A, run the following command to join machine A to the domain with aliases for B and C:

   ```
   adjoin -a B -a B.domain.com -a C -a C.domain.com domain.com
   ```

   Add another -a (--alias) option for each additional application server.
4. If A has more than one host name, use the following command to add host names:

   ```
   adkeytab -a -P http/other_host_name
   ```
5. On machine A, run the following commands to replicate the keytabs from machine A onto machines B and C:

   ```
   cd /
   tar cvfz cluster.tgz /etc/krb5.keytab /var/centrifydc/kset.*
   scp cluster.tgz B:/
   scp cluster.tgz C:/
   ```

   If you have additional servers, run `scp` to copy `cluster.tgz` to each one.

6 On machines B and C (and each additional server), run the following commands to install the keytabs from machine A and to start `adclient`:

```
cd /
tar xvfz cluster.tgz
/usr/share/centrifydc/bin/centrifydc start
```

Note If the password for machine A is changed, run Step 5 and Step 6 after every change. This password is changed transparently in a protocol initiated by Active Directory; that is, Active Directory prompts the Centrify agent for a new account password on an interval defined in the `adclient.krb5.password.change.interval` configuration parameter. The Centrify agent then automatically generates a new password for the computer account and issues the new password to Active Directory. The default interval is 28 days.

Configure a clustered environment with a load balancer

This section describes how to configure a clustered environment with a load balancer. To provide authentication across all of the servers, you need to create a service account for the load balancer on the domain controller, create a new keytab based on that account, and then merge that keytab on each application server.

Note To create new service accounts, you need permission for the container in which you are creating the account. For information about using `adkeytab` to manage service accounts, see the `man` page for the `adkeytab` command.

In this demonstration:

- the Centrify agent and the Centrify for SAP software are already installed on servers B and C (do not install either software package on the load balancer)
- the load balancer hostname is `LB`
- the servers behind the load balancer are named B and C
- the domain is `ace.com`.

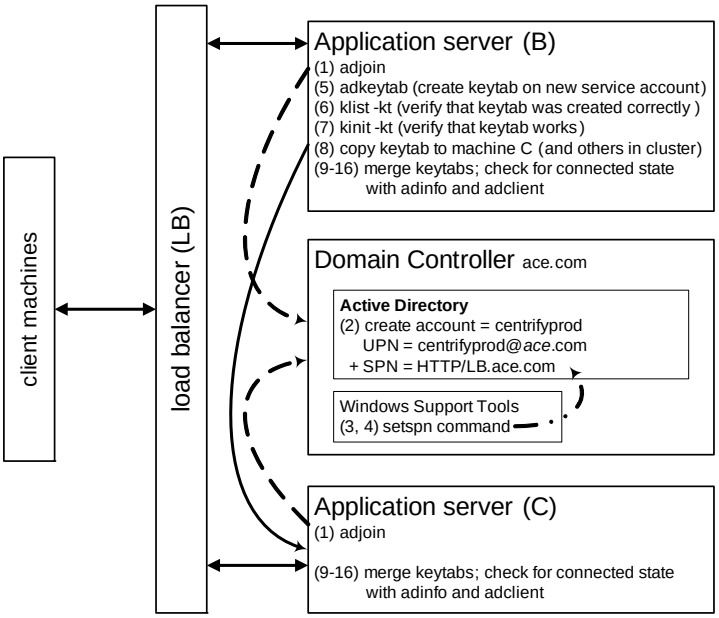
The following figure summarizes the steps for a two-server configuration. For each additional machine, perform Step 8 once more on B, and Step 9 through Step 16 on each additional machine.

This procedure requires users who have the following permissions:

- Create user account on Active Directory on the domain controller
- Add a new service principal name to the user account on the domain controller
- Change service account password from the UNIX computer.

1 Confirm that you have the Centrify agent (`adclient`) and the Centrify for SAP package installed as required.

Unless they are already joined to the domain controller, run `adjoin` on machines B and C (and all other application servers) to join them to the domain controller.



2 Create a new Active Directory account called `centrifyprod`. Verify that the user principal name (UPN) is `centrifyprod@ace.com`.

Note To have `setspn` available to run in Step 3 and Step 4, you need to install Windows Support Tools

3 From a Windows system with Windows Support Tools installed, run the `setspn` command to add a new service principal name (SPN) to the user account:

```
setspn -a HTTP/LB.ace.com centrifyprod
```

4 Confirm that the SPN was created correctly:

```
setspn -l centrifyprod
```

You should see the SPN `HTTP/LB.ace.com`.

Perform Step 5 through Step 8 on machine B *only*.

5 Use the following `adkeytab` command with the `--adopt` option to create the keytab for the new `centrifyprod` account and have Centrify take over the management of the keytab:

```
adkeytab --adopt --principal HTTP/LB.ace.com \
--encryption-type arcfour-hmac-md5 \
--encryption-type des-cbc-md5 \
--encryption-type des-cbc-crc \
--keytab /etc/krb5/centrifyprod.keytab centrifyprod
```

To run the `adkeytab` command above, you must have permission to change the password for the service account and read and write permission for the `userAccountControl` attribute on the Active Directory domain controller. If this is *not* the case, use the following steps to work around this problem:

- Have the Active Directory administrator create a new Active Directory account and add the SPN to the account as above, then provide the password to the UNIX administrator.
- Have the UNIX administrator use the following `adkeytab` command instead of the command in Step 5. In this example, the new user created by the Active Directory administrator is `centrifyprod@ace.com` and the password is `ABC123xyz`:

```
adkeytab --adopt --user centrifyprod@ace.com \
--local --newpassword ABC123xyz \
--encryption-type arcfour-hmac-md5 \
--encryption-type des-cbc-md5 \
--encryption-type des-cbc-crc \
--keytab /etc/krb5/centrifyprod.keytab centrifyprod@ace.com
```

The `--user` option specifies the new account created by the Active Directory administrator, and the `--local` option updates the keytab file on computer B without changing the password in Active Directory, and `--newpassword` option specifies the new password required by the `--local` option.

This work around requires the UNIX administrator to know and expose the password in the command line. The alternative would be to give the Active Directory administrator `root` privileges on the UNIX computer or the UNIX administrator password reset privileges on the domain controller.

6 Verify that the keytab was created correctly:

```
/usr/share/centrifydc/kerberos/bin/klist \
  -kt /etc/krb5/centrifyprod.keytab
```

You should see the SPN `http/`*`LB`*`.`*`domain`*`.com`.

7 Verify that the keytab works:

```
/usr/share/centrifydc/kerberos/bin/kinit \
  -kt /etc/krb5/centrifyprod.keytab centrifyprod
```

You should see no output if everything worked correctly.

8 Copy the keytab `/etc/krb5/centrifyprod.keytab` to machine C.

Perform Step 9 through Step 16 on both machine B and machine C.

9 Disable Centrify to prepare for merging keytabs:

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

10 Back up the existing keytab:

```
cp /etc/krb5/krb5.keytab \
  /etc/krb5/krb5.keytab.todaysdate
```

11 Merge the keytabs; for example:

```
#/usr/bin/ktutil
ktutil:rkt /etc/krb5/krb5.keytab
ktutil:rkt /etc/krb5/centrifyprod.keytab
ktutil:wkt /etc/krb5/krb5.keytab.new
ktutil:q
```

12 Verify that the new keytab was created correctly:

```
/usr/share/centrifydc/kerberos/bin/klist \
  -kt /etc/krb5/krb5.keytab.new
```

13 Copy the new keytab to the default location with the appropriate name:

```
cp /etc/krb5/krb5.keytab.new /etc/krb5/krb5.keytab
```

14 Verify that the new keytab works:

```
/usr/share/centrifydc/kerberos/bin/kinit -kt centrifyprod
```

You should see no output if everything worked correctly.

15 Enable Centrify:

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

16 Run `adinfo` and check that `adclient` goes into a connected state. If `adclient` reports that it is `disconnected`, something has gone wrong in the setup.

If the password for the `centrifyprod` Active Directory account is changed, run Step 5 through Step 16 after every change. This password is changed transparently in a protocol initiated by Active Directory; that is, Active Directory prompts for a new account password on an interval defined in the `adclient.krb5.password.change.interval` configuration parameter. The Centrify agent then automatically generates a new password for the computer account and issues the new password to Active Directory. The default interval is 28 days.

Troubleshooting SNC configuration

If SAP does not restart after configuring SNC, there are typically three causes

- Centrify for the SAP server is not available: The `snckrb5.so` library cannot be found.
- Kerberos accepting credentials are not available: The keytab file does not have an entry for the configured principal name.
- Kerberos initiating credentials are not available: The SAP *sid*adm user does not have, or has an incorrect, cached Kerberos ticket with a default principal name that matches the configured principal name.

Centrify for the SAP server is not available

Typically, this is caused by one of the following errors

- The Centrify for SAP package was not "un-tarred" or the `snckrb5.so` library is in the wrong location.

  See the table in "Setting up the server environment" on page 13 for the `snckrb5.so` (`.a` on AIX) files for various platforms.

- You have the wrong path or filename for snc/gssapi_lib in the SAP instance profile. If this is the case and you are not able to connect to SAP via SAPgui, you may have to edit the instance profile text file directly (the profile files can typically be found in the `/usr/sap/`*`SID`*`/SYS/profile` directory).

  See "Modify the SAP instance profile" on page 17 for the instance profile configuration instructions.

Kerberos accepting credentials are not available

Typically, this occurs because the supplied service principal name does not exist in the default `keytab` file. This can be caused when:

- The system is not joined to Active Directory through the Centrify agent (and therefore, no keytab file exists at all).

  Use the `adinfo` command to determine if you are joined. If you are not joined, see "Setting up the server environment" on page 13 for the `adjoin` command options. For the full list of `adjoin` options, see the `adjoin` man page.

- You have supplied the wrong service principal name (SPN) to SAP in the `snc/identity/as` instance profile parameter.

If this is the case, and you are not able to connect to SAP via SAPgui, you may have to edit the instance profile text file directly (the profile files can typically be found in the `/usr/sap/SID/SYS/profile` directory). See "Modify the SAP instance profile" on page 17 for the instructions.

Kerberos initiating credentials are not available

Typically, this occurs because the supplied principal name does not exist in the cached Kerberos tickets for the *sid*adm user for SAP. This can be caused when the `kinit` command in the `.cshrc` file of the *sid*adm user does not execute correctly, is for the wrong principal name or is not executed before SAP is restarted. See "Configure the sidadm OS profile" on page 14 for the `.cshrc` file instructions.

Ensure that the default principal name in the cached credential matches the principal name supplied to SAP.

Index

T

U

W

Z