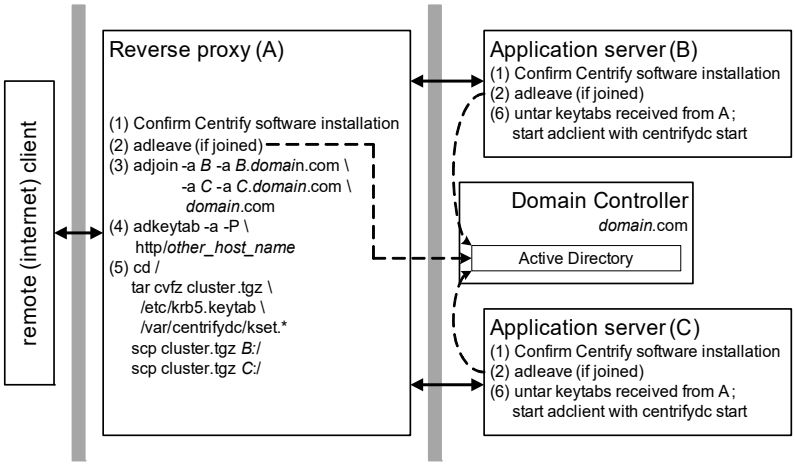
Configure a clustered environment with a reverse proxy

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`.

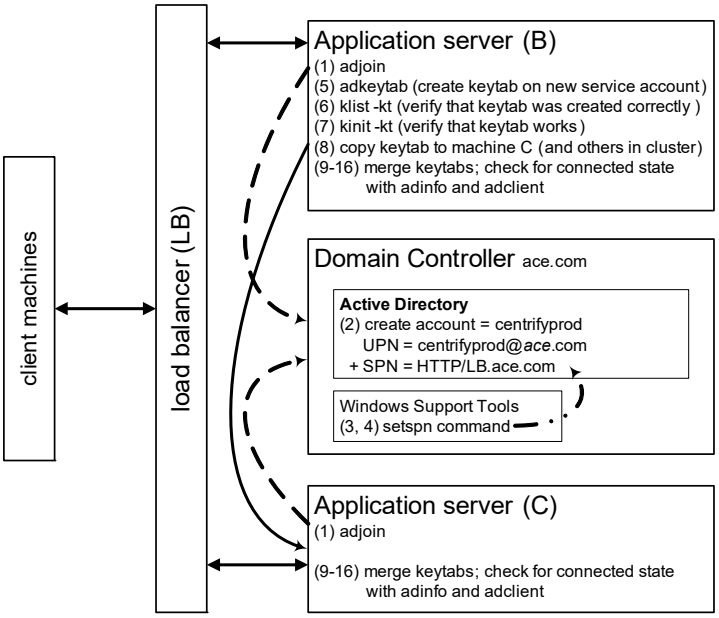
The following figure summarizes the steps for a two-server configuration. For each additional machine, perform Step 8 once more on B, and Step 9 through Step 16 on each additional machine.

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.