Identify. Simplify. Centrify.

Centrify

WHITE PAPER

CENTRIFY CORP.

NOV 2010

DirectControl and RSA SecurID

Enabling Active Directory users to authenticate to Unix/Linux using SecurID tokens

ABSTRACT

This document describes the steps necessary to install and configure DirectControl and RSA SecurID to enable two factor authentication for Unix/Linux environments.

Centrify Corporation
444 Castro Street, Suite 1100
Mountain View, CA 94041

TEL (650) 961-1100
FAX (650) 962-0307
URL www.centrify.com

[WP-001-2006-03-30]

Contents

1 First Steps

1.1 Overview

Once installation of the two agents is complete, user authentication can occur for locally defined UNIX users or for Active Directory users who have UNIX profiles in the appropriate zone. In addition, specific groups of AD users can be prompted for password authentication or two factor authentication.

1.1.1 Installing the two agents

Installation of the agents for the two products is simple. The installation process for each agent does not interfere with or touch any configuration file used by the other product. Follow the standard installation steps for each product.

The products may be installed in either order. After the Centrify DirectControl agent is installed the machine must be joined to Active Directory and placed in a DirectControl Zone.

1.1.2 Configuring the system-auth file for Linux.

After the installation of the two products you will need to configure the /etc/pam.d/system-auth file:

Notice that pam_securid is first in the list.

#/etc/pam.d/system-auth file

```
# lines inserted by Centrify Direct Control (CentrifyDC 4.4.1-203)
auth       required       pam_securid.so
auth       sufficient     pam_centrifydc.so
auth       requisite      pam_centrifydc.so deny
account    sufficient     pam_centrifydc.so
account    requisite      pam_centrifydc.so deny
session    required       pam_centrifydc.so homedir
password   sufficient     pam_centrifydc.so try_first_pass
password   requisite      pam_centrifydc.so deny
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        required      pam_tally.so onerr=fail no_magic_root deny=5
auth        sufficient    pam_unix.so  try_first_pass
auth        requisite     pam_succeed_if.so uid >= 500 quiet
auth        required      pam_deny.so

account     required      pam_unix.so
account     sufficient    pam_succeed_if.so uid < 500 quiet
account     required      pam_tally.so deny=5 reset no_magic_root
account     required      pam_permit.so

password    requisite     pam_cracklib.so minlen=8 dcredit=0 ucredit=0
lcredit=0 ocredit=0 try_first_pass retry=3
```

```
#password    sufficient    pam_unix.so md5 shadow  try_first_pass
use_authtok remember=8
password    sufficient    pam_unix.so remember=8 use_authtok md5 shadow

password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond
quiet use_uid
session     required      pam_unix.so
```

1.1.3 Configuring the pam.conf file for Solaris and AIX

After the installation of the two products you will need to configure the /etc/pam.conf file.

Notice the sshd-kbdint lines at the bottom of the file.

#etc/pam.conf file

```
# lines inserted by Centrify Direct Control (CentrifyDC 4.4.1-203)
login        auth sufficient         pam_centrifydc.so unix_cred
login        auth requisite          pam_centrifydc.so deny
krlogin      auth sufficient         pam_centrifydc.so unix_cred
krlogin      auth requisite          pam_centrifydc.so deny
krsh         auth sufficient         pam_centrifydc.so unix_cred
krsh         auth requisite          pam_centrifydc.so deny
ktelnet      auth sufficient         pam_centrifydc.so unix_cred
ktelnet      auth requisite          pam_centrifydc.so deny
ppp          auth sufficient         pam_centrifydc.so unix_cred
ppp          auth requisite          pam_centrifydc.so deny
other        auth sufficient         pam_centrifydc.so unix_cred
other        auth requisite          pam_centrifydc.so deny
passwd       auth sufficient         pam_centrifydc.so try_first_pass
passwd       auth requisite          pam_centrifydc.so deny
cron         account sufficient      pam_centrifydc.so unix_cred
cron         account requisite       pam_centrifydc.so deny
other        account sufficient      pam_centrifydc.so unix_cred
other        account requisite       pam_centrifydc.so deny
other        session required        pam_centrifydc.so
other        password sufficient     pam_centrifydc.so try_first_pass
#
#ident     "@(#)pam.conf    1.31  07/12/07 SMI"
#
# Copyright 2007 Sun Microsystems, Inc.  All rights reserved.
# Use is subject to license terms.
#
# PAM configuration
#
# Unless explicitly defined, all services use the modules
# defined in the "other" section.
#
# Modules are defined with relative pathnames, i.e., they are
# relative to /usr/lib/security/$ISA. Absolute path names, as
# present in this file in previous releases are still acceptable.
#
# Authentication management
#
```

```
# login service (explicit because of pam_dial_auth)
#
login auth requisite        pam_authtok_get.so.1
login auth required         pam_dhkeys.so.1
login auth required         pam_unix_cred.so.1
login auth required         pam_unix_auth.so.1
login auth required         pam_dial_auth.so.1
#
# rlogin service (explicit because of pam_rhost_auth)
#
rlogin      auth sufficient      pam_rhosts_auth.so.1
rlogin      auth sufficient      pam_centrifydc.so unix_cred
rlogin      auth requisite       pam_centrifydc.so deny
rlogin      auth requisite       pam_authtok_get.so.1
rlogin      auth required        pam_dhkeys.so.1
rlogin      auth required        pam_unix_cred.so.1
rlogin      auth required        pam_unix_auth.so.1
#
# Kerberized rlogin service
#
krlogin    auth required         pam_unix_cred.so.1
krlogin    auth required         pam_krb5.so.1
#
# rsh service (explicit because of pam_rhost_auth,
# and pam_unix_auth for meaningful pam_setcred)
#
rsh        auth sufficient       pam_rhosts_auth.so.1
rsh        auth sufficient       pam_centrifydc.so unix_cred
rsh        auth requisite        pam_centrifydc.so deny
rsh        auth required         pam_unix_cred.so.1
#
# Kerberized rsh service
#
krsh  auth required         pam_unix_cred.so.1
krsh  auth required         pam_krb5.so.1
#
# Kerberized telnet service
#
ktelnet    auth required         pam_unix_cred.so.1
ktelnet    auth required         pam_krb5.so.1
#
# PPP service (explicit because of pam_dial_auth)
#
ppp   auth requisite        pam_authtok_get.so.1
ppp   auth required         pam_dhkeys.so.1
ppp   auth required         pam_unix_cred.so.1
ppp   auth required         pam_unix_auth.so.1
ppp   auth required         pam_dial_auth.so.1
#
# Default definitions for Authentication management
# Used when service name is not explicitly mentioned for authentication
#
other auth requisite        pam_authtok_get.so.1
other auth required         pam_dhkeys.so.1
other auth required         pam_unix_cred.so.1
other auth required         pam_unix_auth.so.1
#
# passwd command (explicit because of a different authentication module)
#
passwd     auth required         pam_passwd_auth.so.1
#
# cron service (explicit because of non-usage of pam_roles.so.1)
#
```

```
cron  account required pam_unix_account.so.1
#
# Default definition for Account management
# Used when service name is not explicitly mentioned for account
management
#
other account requisite     pam_roles.so.1
other account required pam_unix_account.so.1
#
# Default definition for Session management
# Used when service name is not explicitly mentioned for session
management
#
other session required pam_unix_session.so.1
#
# Default definition for Password management
# Used when service name is not explicitly mentioned for password
management
#
other password required     pam_dhkeys.so.1
other password requisite    pam_authtok_get.so.1
other password requisite    pam_authtok_check.so.1
other password required     pam_authtok_store.so.1
#
# Support for Kerberos V5 authentication and example configurations can
# be found in the pam_krb5(5) man page under the "EXAMPLES" section.
sshd-kbdintauth       required              pam_securid.so
sshd-kbdint           auth sufficient       pam_centrifydc.so unix_cred
sshd-kbdint           auth requisite        pam_centrifydc.so deny
sshd-kbdint           account sufficient    pam_centrifydc.so unix_cred
sshd-kbdint           account requisite     pam_centrifydc.so deny
sshd-kbdint           session required      pam_centrifydc.so
sshd-kbdint           password sufficient   pam_centrifydc.so try_first_pass
sshd-kbdintauth       requisite             pam_authtok_get.so.1
sshd-kbdintauth       required              pam_dhkeys.so.1
sshd-kbdintauth       required              pam_unix_cred.so.1
sshd-kbdintauth       required              pam_unix_auth.so.1
sshd-kbdintaccount    requisite             pam_roles.so.1
sshd-kbdintaccount    required              pam_unix_account.so.1
sshd-kbdintsession    required              pam_unix_session.so.1
sshd-kbdintpassword   required              pam_dhkeys.so.1
sshd-kbdintpassword   requisite             pam_authtok_get.so.1
sshd-kbdintpassword   requisite             pam_authtok_check.so.1
sshd-kbdintpassword   required              pam_authtok_store.so.1
```

1.1.4 Requiring token authentication for specific groups.

RSA supports the ability to require Token authentication for specific groups of users.

This feature is supported when using Centrify, and Active Directory groups can be specified as the required group. Local groups work as well.

PLEASE NOTE THAT THIS FEATURE DOES NOT WORK WITH AIX. There is a bug in the AIX OS that prevents the SecurID agent from iterating AD groups.

The sd_pam.conf file should be configured as so:

```
#VAR_ACE ::  the location where the sdconf.rec, sdstatus.12 and securid
files will go
VAR_ACE=/opt/RSA


#ENABLE_GROUP_SUPPORT :: 1 to enable; 0 to disable group support
ENABLE_GROUP_SUPPORT=1

#INCL_EXCL_GROUPS :: 1 to always prompt the listed groups for securid
# authentication (include)
#                  :: 0 to never prompt the listed groups for securid
# authentication (exclude)
INCL_EXCL_GROUPS=1

#LIST_OF_GROUPS :: a list of groups to include or exclude...Example
#LIST_OF_GROUPS=other:wheel:eng:othergroupnames
LIST_OF_GROUPS=sampleadgroup

#PAM_IGNORE_SUPPORT :: 1 to return PAM_IGNORE if a user is not SecurID
# authenticated due to their group membership
#                    :: 0 to UNIX authenticate a user that is not SecurID
# authenticated due to their group membership
PAM_IGNORE_SUPPORT=1

#AUTH_CHALLENGE_USERNAME_STR :: prompt message to ask user for their
# username/login id
AUTH_CHALLENGE_USERNAME_STR=Enter USERNAME :

#AUTH_CHALLENGE_RESERVE_REQUEST_STR :: prompt message to ask administrator
# for their System password
AUTH_CHALLENGE_RESERVE_REQUEST_STR=Please enter System Password for root :

#AUTH_CHALLENGE_PASSCODE_STR :: prompt message to ask user for their
# Passcode
AUTH_CHALLENGE_PASSCODE_STR=Enter PASSCODE :

#AUTH_CHALLENGE_PASSWORD_STR :: prompt message to ask user for their
# Password
AUTH_CHALLENGE_PASSWORD_STR=Enter your PASSWORD :
```

1.1.5 Configuring SSH to require SecurID.

When setting up the SecurID product you must make some configuration changes to the sshd configuration files.

If you are using the Centrify openSSH product you must make some configuration changes to support token authentication. The Centrify openSSH is configured to attempt Kerberos single signon whenever a user logs in. This means that the user is not prompted for their username or password. This capability must be disabled if you want to prompt users for token authentication.

Make the following changes to /etc/centrifydc/ssh/ssh_config:

```
# Configuration for Centrify DirectControl:
Host *
#GSSAPIAuthentication yes
```

```
#GSSAPIKeyExchange yes
#GSSAPIDelegateCredentials yes
```

Make the following changes to /etc/centrifydc/ssh_sshd_config:

```
# Configuration for Centrify DirectControl:
ChallengeResponseAuthentication yes
Banner /etc/issue
#GSSAPIKeyExchange yes
#GSSAPIAuthentication yes
#GSSAPICleanupCredentials yes
PrintMotd no
UsePAM yes
```

Restart sshd to ensure the changes take effect.

2 Confirming the Installation

Once the agents have been installed, you can confirm the installation is working by configuring a local UNIX user on the RSA Administration Server and confirming authentication with a SecurID Token.

Next you can enable an Active Directory user by creating a UNIX Profile for that user in the zone where the UNIX machine is registered. After the user is created, you must register the user on the RSA Administration Server to have a SecurID token.

The user must enter their unix UserID (not their AD name) in order for authentication with SecurID to occur.

3 Controlling Machine Access with DirectControl

You can disable user access by 3 methods

- Disabling the user's Active Directory Account
- Removing the user from the DirectControl Zone
- Unchecking the "Enable user access to this zone" check box in the user's Centrify Profile tab.

4 Known Issues

- For sshd_config, you should explicitly set the following parameter to Yes. Even though the parameter is defaulted to this value, it sometimes is not correctly set. Without this parameter, you will not receive prompts for events like New Pin, etc.

```
ChallengeResponseAuthentication Yes
```

- Even though the user authenticates with their SecurID token, they may be prompted to reset their Active Directory password if it has expired in the domain. After the user logs in, they will be presented with the "Change Password" prompts from Active Directory
- When a user authenticates with a SecurID token, they are granted access to the UNIX machine, but they are not authenticated to the Active Directory Domain. As a result, they will not have Kerberos Credentials or Single Signon capability to other systems. After signing on, the user may type

```
>kinit
```

- and enter their Active Directory password to properly authenticate to Active Directory.

5 How to Contact Centrify

North America
(And All Locations Outside EMEA)

Centrify Corporation
785 N. Mary Avenue., Suite 200
Sunnyvale, CA 94085
United States

Sales: +1 (408) 542-7500

Enquiries: info@centrify.com
Web site: www.centrify.com

Europe, Middle East, Africa
(EMEA)

Centrify EMEA
Asmec Centre
Merlin House
Brunel Road
Theale, Berkshire, RG7 4AB
United Kingdom

Sales: +44 118 902 6580