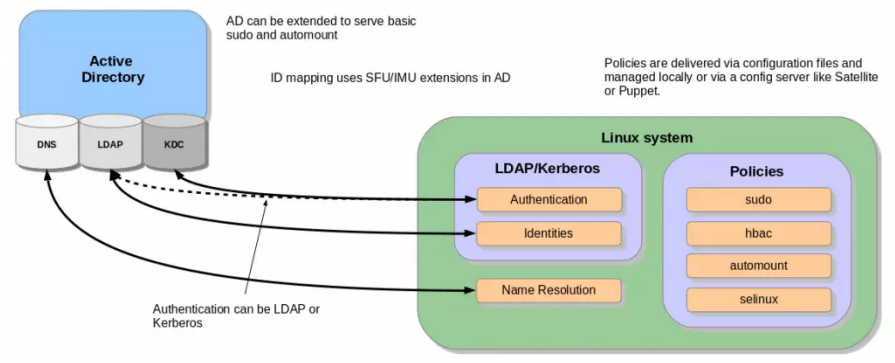
How To Join CentOS 8 / RHEL 8 System to Active Directory (AD) domain

By **Josphat Mutai** - October 18, 2019

Question: How do I join a CentOS 8 / RHEL 8 system to Windows Active Directory domain?. In this guide, we'll discuss how to use **realmd** system to join a CentOS 8 / RHEL 8 server or workstation to an Active Directory domain. Realmd provides a clear and simple way to discover and join identity domains to achieve direct domain integration.



In most Enterprise environments, Active Directory domain is used as a central hub for storing user information. In this integration, realmd configures underlying Linux system services, such as SSSD or Winbind, to connect to the domain. Linux systems are connected to Active Directory to pull user information for authentication requests.

This guide will illustrate how to configure SSSD to retrieve information from domains within the same Active Directory Resource Forest. if you're working with more than one AD forest, this guide may not work for you.

Step 1: Install required packages

A number of packages are required for CentOS 8 / RHEL 8 AD integration. Install them on your system by running the following commands:

```
sudo dnf install realmd sssd oddjob oddjob-mkhomedir adcli samba-cor
```

Accept installation prompt.

```
Last metadata expiration check: 0:19:18 ago on Fri 27 Sep 2019 09:4
Package realmd-0.16.3-16.el8.x86_64 is already installed.
Package sssd-2.0.0-43.el8_0.3.x86_64 is already insta
Package adcli-0.8.2-2.el8.x86_64 is already installe
Package samba-common-4.9.1-8.el8.noarch is already i
```

```
Dependencies resolved.
================================================================================
 Package                                 Arch
================================================================================
Installing:
 oddjob                                  x86_64
 oddjob-mkhomedir                        x86_64
 samba-common-tools                      x86_64
Installing dependencies:
 samba-libs                              x86_64

Transaction Summary
================================================================================
Install  4 Packages

Total download size: 773 k
Installed size: 1.7 M
Is this ok [y/N]: y
```

Step 2: Discover Active Directory domain on CentOS 8 / RHEL 8

Before doing AD integration, ensure the CentOS/RHEL 8 machine can resolve and discover AD domain.

Verify your DNS settings.

```
$ cat /etc/resolv.conf
```

Check if AD domain discovery is successful.

```
$ realm  discover example.com
example.com
  type: kerberos
  realm-name: EXAMPLE.COM
  domain-name: example.com
  configured: no
  server-software: active-directory
  client-software: sssd
  required-package: oddjob
```


```
  required-package: oddjob-mkhomedir
  required-package: sssd
  required-package: adcli
  required-package: samba-common-tools
```

Step 3: Join CentOS 8 / RHEL 8 Linux machine in Active Directory domain

An AD administrative user account is required for integrating CentOS 8 / RHEL 8 machine with Windows Active Directory domain.

Make sure you have admin username and password. Then run the command below to join CentOS 8 / RHEL 8 Linux system to an Active Directory domain.

```
$ realm join example.com -U Administrator
Password for Administrator:
```

Replace `Administrator` with your AD admin account, and input password when asked. Confirm that the join was successful.

```
 $ sudo realm list
example.com
  type: kerberos
  realm-name: EXAMPLE.COM
  domain-name: example.com
  configured: kerberos-member
  server-software: active-directory
  client-software: sssd
  required-package: oddjob
  required-package: oddjob-mkhomedir
  required-package: sssd
  required-package: adcli
  required-package: samba-common-tools
  login-formats: %U@example.com
  login-policy: allow-realm-logins
```

Your **sssd.conf** configuration file should look like below,

```
 $ cat /etc/sssd/sssd.conf
[sssd]
domains = example.com
```


```
config_file_version = 2
services = nss, pam
default_domain_suffix = example.com

[nss]
homedir_substring = /home

[pam]

[domain/example.com]
ad_domain = example.com
krb5_realm = EXAMPLE.COM
realmd_tags = manages-system joined-with-samba
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = True
fallback_homedir = /home/%u@%d
access_provider = ad
```

When a change is made in the config file, service restart is required.

```
sudo systemctl restart sssd
```

Status should be running.

```
$ systemctl status sssd
 ● sssd.service - System Security Services Daemon
    Loaded: loaded (/usr/lib/systemd/system/sssd.service; enabled; v
    Active: active (running) since Fri 2019-09-27 22:30:25 EAT; 37mi
  Main PID: 32474 (sssd)
    CGroup: /system.slice/sssd.service
            ├─32474 /usr/sbin/sssd -i --logger=files
            ├─32478 /usr/libexec/sssd/sssd_be --domain example.com -
            ├─32479 /usr/libexec/sssd/sssd_nss --uid 0 --gid 0 --log
            └─32480 /usr/libexec/sssd/sssd_pam --uid 0 --gid 0 --log
.....................................................................
```

If the integration is working, it should be possible to get an AD user in

```
$ id jmutai
uid=1783929917(jmutai@example.com) gid=1784800513(domain users@examp
```

Step 4: Control Access – Limit to user/group

Access to the server enrolled can be limited by allowing only specific users/ and groups.

Limit to users

To permit a user access via SSH and console, use the command:

```
$ realm permit user1@example.com
$ realm permit user2@example.com user3@example.com
```

Permit access to group – Examples

```
$ ream permit -g sysadmins
$ realm permit -g 'Security Users'
$ realm permit 'Domain Users' 'admin users'
```

This will modify *sssd.conf* file.

If instead you like to allow all users access, run:

```
$ sudo realm permit --all
```

To deny all Domain users access, use:

```
$ sudo realm  deny --all
```

Step 5: Configure Sudo Access

By default Domain users won't have permission to escalate privilege to root. Users have to be granted access based on usernames or groups.

Let's first create sudo permissions grants file.

```
$ sudo vi /etc/sudoers.d/domain_admins
```

Add single user:

```
user1@example.com        ALL=(ALL)       ALL
```


Add another user:

```
user1@example.com      ALL=(ALL)    ALL
user2@example.com      ALL=(ALL)    ALL
```

Add group

```
%group1@example.com      ALL=(ALL)    ALL
```

Add group with two or three names.

```
%security\ users@example.com        ALL=(ALL)        ALL
%system\ super\ admins@example.com ALL=(ALL)        ALL
```

Step 6: Test SSH Access

Access the server remotely as user on AD allowed to login.

```
$ ssh jmutai@localhost
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is SHA256:wmWcLi/lijm4zWbQ/Uf6uLMYzM7g1AnBwxzo
ECDSA key fingerprint is MD5:10:0c:cb:22:fd:28:34:c6:3e:d7:68:15:02:
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known
```

This is a confirmation that our configuration was successful. Visit realmd and sssd wiki pages to learn more.

More:

How To Manage CentOS 8 With Cockpit Web Admin Console

How To Change SSH Port on CentOS / RHEL & Fedora With SELinux Enforcing

How To Check SSL Certificate Expiration with OpenSSL

Founder of Computingforgeeks. Expertise in Virtualization, Cloud Computing, Linux/UNIX systems, Programming,Storage systems,HA, Server Clustering e.t.c.