

# realmd/sssds | Joining a Domain with RHEL and logging in with AD account

## Install the necessary packages and join a domain

SSSD = Authentication service from a remote source such as AD  
realmd = Active Directory service

### Install the packages

```
yum install sssd realmd oddjob oddjob-mkhomedir adcli samba-common samba-common-tools krb5-workstation  
openldap-clients python3-policycoreutils
```

### Check if can discover the domain

```
realm discover homelab.local
```

### Join Domain

```
# realm join --user=[domain user account] [domain name]  
realm join --user=aki.adm homelab.local
```

### Check if it is inside a domain after joining

```
realm list
```

---

## Further configuration

So now that the Linux server is part of the AD domain, domain users can access the server with their usual credentials. We are done, right? Wrong. "What's the problem?" I hear you say. HAHAHHAH

## Configure SSSD

Its main configuration file is located at */etc/sss/sss.conf*. As a matter of fact, this is the main configuration file we will modify.

Configure the SSSD conf to look like this. From line 17!

```
[sss]
domains = homelab.local
config_file_version = 2
services = nss, pam

[domain/homelab.local]
ad_domain = homelab.local
krb5_realm = HOMELAB.LOCAL
realmd_tags = manages-system joined-with-adcli
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 = simple
ad_hostname = lab-dc1.homelab.local
dyndns_update = true
dyndns_refresh_interval = 43200
dyndns_update_ptr = true
dyndns_ttl = 3600
dyndns_auth = GSS-TSIG
```

Once the configuration is complete, restart sssd to apply settings immediately.

```
systemctl restart sssd
```

## Managing Login Permissions for Domain Users

Shows the permitted or denied login

By default, this is the output without configurations

```
[root@lab-rhel8 ~]# realm list
homelab.local
  type: kerberos
  realm-name: HOMELAB.LOCAL
  domain-name: homelab.local
  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@homelab.local
  login-policy: allow-permitted-logins
  permitted-logins:
  permitted-groups:
```

## Deny all

Deny local login by realm accounts.

This command prevents realm accounts from logging into the local machine. Use `realm permit` to restrict logins to specific accounts.

```
realm deny --all
```

The following options can be used:

- `--all, -a`

- This option should be specified

- `--realm, -R`

- Specify the name of the realm to deny users login to.

## Permit All (Default)

Permit logins using realm accounts on the local machine according to the realm policy. This usually defaults to allowing any realm user to log in.

```
realm permit --all
realm permit -a
```

## Permit User

```
realm permit user@example.com  
realm permit DOMAIN\\User2
```

## Permit Group

```
realm permit --groups "Domain Admin"  
realm permit -g "Domain Admin"
```

## Permit Realm (if joining more than one domain)

```
realm permit --realm  
realm permit -R homelab.local
```

## Remove Permit

```
realm permit --withdraw user@example.com  
realm permit -x user@example.com
```

---

Revision #3

Created 30 December 2023 18:45:50 by aki

Updated 4 January 2024 15:15:06 by aki