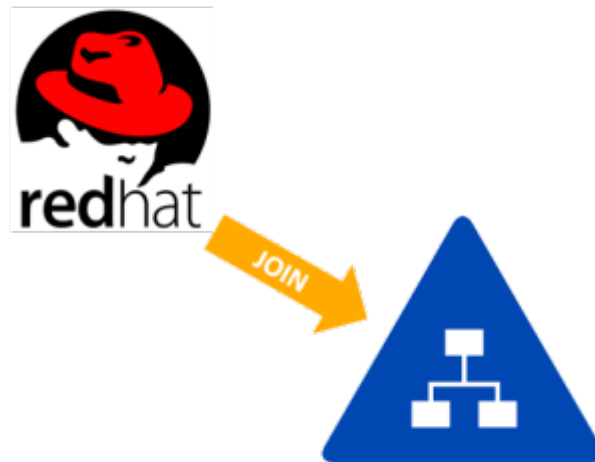


How to join RHEL system to Active Directory



Voraussetzungen:

- Red Hat Enterprise Linux 7 / 6
- Vorhandenes und funktionierendes - Active Directory

Konfigurationsablauf

Before you start: Make Sure RHEL machine is able to resolve Active Directory servers!

1. **Install adcli package** along with **sssd**:

```
# yum install adcli sssd authconfig
```

2. Then **discover** the **AD domain**:

```
adcli info ad.example.com
```

3. **adcli** will show few details about the AD domain. now, **join RHEL system to AD domain using adcli**

```
# adcli join ad.example.com
```

```
Password for Administrator@AD.EXAMPLE.COM: <---- Enter Admin password
```

4. The join operation creates a keytab the machine will authenticate with. When inspect the with `klist -kt`, should show several entries that contain client hostname in some form:

```
# klist -kte
```

5. **Configure /etc/krb5.conf** to use AD domain:

```
# vim /etc/krb5.conf
```

```
[libdefaults]
default_realm = AD.EXAMPLE.COM
dns_lookup_realm = true
dns_lookup_kdc = true
ticket_lifetime = 24h
renew_lifetime = 7d
forwardable = true

[realms]
AD.EXAMPLE.COM = {
kdc = server.ad.example.com
admin_server = server.ad.example.com
}

[domain_realm]
.ad.example.com = AD.EXAMPLE.COM
ad.example.com = AD.EXAMPLE.COM`
```

6. Use authconfig to **set up** the **Name Service Switch**(/etc/nsswitch.conf) and **PAM stacks**(password-auth and system-auth):

```
# authconfig --enablesssd --enablesssdauth --update
```

Above command will modify and add necessary entries in /etc/nsswitch.conf, /etc/pam.d/password-auth and /etc/pam.d/system-auth files.

7. **The final step** is to configure the **SSSD** itself. Open /etc/sss/sss.conf and define a single domain:

```
# vim /etc/sss/sss.conf
```

```
[sss]
services = nss, pam, ssh, autofs
config_file_version = 2
domains = AD.EXAMPLE.COM

[domain/AD.EXAMPLE.COM]
id_provider = ad
# Uncomment if service discovery is not working # ad_server =
server.win.example.com
```

8. Start the SSSD and make sure it's up after reboots:

```
# systemctl start sssd  
# systemctl enable sssd
```

After you are done, fetch user information for AD user and try to login:

```
# id Administrator  
# ssh Administrator@localhost
```

Last update: **2017/09/06 09:15**