Windows AD ??

?? RedHat ??????? Windows AD ???

RedHat 7/8 (?????)

> ??????????????????????????????

- [Chapter 7. Configuring a RHEL host to use AD as an authentication provider Red Hat Enterprise Linux 8 | Red Hat Customer Portal]

???????

```
yum install sssd sssd-tools krb5-workstation krb5-libs
```

??????? AD ????

```
useradd AD_user
```

?? `/etc/nsswitch.conf`

```
# Add 'sss' for AD authentication
passwd:     files sss systemd
shadow:     files sss
group:      files sss systemd
```

?? `/etc/krb5.conf`

```
[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 dns_lookup_realm = false
 ticket_lifetime = 24h
 renew_lifetime = 7d
 forwardable = true
 rdns = false
 pkinit_anchors = FILE:/etc/pki/tls/certs/ca-bundle.crt
# Change this as required
 default_realm = EXAMPLE.COM
 default_ccache_name = KEYRING:persistent:%{uid}

[realms]
# Change this as required
EXAMPLE.COM = {
    kdc = ad.example.com
    dmin_server = ad.example.com
}

[domain_realm]
# Change this as required
.example.com = EXAMPLE.COM
example.com = EXAMPLE.COM
```

?? `/etc/sssd/sssd.conf`

```
[sssd]
    services = nss, pam
    domains = EXAMPLE.COM

[domain/EXAMPLE.COM]
    id_provider = files
    auth_provider = krb5
    krb5_realm = EXAMPLE.COM
    krb5_server = ad.example.com
```

?????

```
chmod 0600 /etc/sssd/sssd.conf
```

?? sssd ??

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

?? `/etc/pam.d/system-auth`

```
#%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_faildelay.so delay=2000000
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 1000 quiet_success
# AD Authentication
auth        sufficient    pam_sss.so forward_pass

auth        required      pam_deny.so


account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 1000 quiet
# AD Authentication
account     [default=bad success=ok user_unknown=ignore] pam_sss.so

account     required      pam_permit.so


password    requisite     pam_pwquality.so try_first_pass local_users_only retry=3 authtok_type$
password    sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_authtok
# AD Authentication
password    sufficient    pam_sss.so use_authtok

password    required      pam_deny.so


session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
-session     optional      pam_systemd.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
# AD Authentication
session     optional      pam_sss.so
```

?? `/etc/pam.d/password-auth` ??????????

??AD??

????

```
#> kinit AD_user
Password for AD_user@EXAMPLE.COM:

#> klist
Ticket cache: KEYRING:persistent:0:0
Default principal: AD_user@EXAMPLE.COM

Valid starting     Expires            Service principal
11/02/20 04:16:38  11/02/20 14:16:38  krbtgt/EXAMPLE.COM@EXAMPLE.COM
	renew until 18/02/20 04:16:34
```

?? SSH ??

???? AD_user (??? `@example.com`)?? SSH?

????

Displaying user authorization details

```
sssctl user-checks -a acct -s sshd AD_user
```

Display a list of available domains

```
sssctl domain-list
```

RedHat 7/8 (????)

- How to join a Linux system to an Active Directory domain | Enable Sysadmin (redhat.com)
- Windows Integration Guide Red Hat Enterprise Linux 7 | Red Hat Customer Portal
- How to join a Linux system to an Active Directory domain

??????

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

?? realmd ? Linux ???? AD ??

> NOTE: ???? /etc/krb5.conf ?????????????????? /etc/sssd/sssd.conf ???
>
> ?? AD ??????? AD ?????????? AD ?? ?? adm1?
>
> ?????????????????????????

```
realm discover ad.example.com

realm join ad.example.com -U adm1

realm list
```

???? `/etc/sssd/sssd.conf`, `/etc/krb5.conf`

```
[sssd]
domains = example.com
config_file_version = 2
services = nss, pam

[domain/example.com]
ad_server = ad.example.com
ad_domain = example.com
krb5_realm = EXAMPLE.COM
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 = ad
```

```
[libdefaults]
 dns_lookup_realm = false
 ticket_lifetime = 24h
 renew_lifetime = 7d
 forwardable = true
 rdns = false
 pkinit_anchors = FILE:/etc/pki/tls/certs/ca-bundle.crt
 default_ccache_name = KEYRING:persistent:%{uid}

 default_realm = EXAMPLE.COM
[realms]
 EXAMPLE.COM = {
 }

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

Optional: ???? AD ??

```
# □□□□ AD □ Administrator □□
realm leave ad.example.com

# □□□□□□□□□
realm leave ad.example.com -U 'EXAMPLE.COM\user'
```

??????

> ??????????????????????????? AD ??? AD ??????? /etc/sssd/sssd.conf?

?? /etc/sssd/sssd.conf

```
# ACL for AD Login
#access_provider = ad
access_provider = simple
#simple_allow_users = ad-user1, ad-user2
simple_allow_groups = ad-group
```

?? sssd ??

```
systemctl restart sssd
realm list
```

????

?? ad-user ?????

```
usermod -aG local-group aduser@ad.domain.com
getent group local-group
groups aduser@ad.domain.com
```

????

?? AD ??? uid

```
id ADDOMAIN\\aduser@ad.domain.com


getent passwd aduser@ad.domain.com
```

Revision #33
Created 20 June 2024 10:41:07 by Admin
Updated 2 December 2024 17:16:17 by Admin