Active Directory 参加（GUI を使った簡単な方法）

■前提

マシン	ドメイン	ホスト名	IP
AD サーバ	vmware.local	ad001	192.168.1.3
参加するマシン	--	test001	192.168.1.18

■ hosts と DNS の設定

ad のホスト名から IP が引けない場合は、hosts を編集
/etc/hosts

```
192.168.1.3 ad001.vmware.local ad001
```

■ winbind をインストール

```
yum install samba-winbind
```

■ GUI で AD 情報を設定

```
system-config-authentication &
```

または、メニューから「認証」を選択
CentOS7 の場合は、 authconfig-gtk が必要。

```
yum install authconfig-gtk
```

ユーザーアカウントデータベース
　winbind
winbind ドメイン
　VMWARE
セキュリティモデル
　ads
Winbind ADS レルム
　VMWARE.LOCAL
winbind ドメインコントローラ
　ad01
winbind ドメインコントローラが複数の場合
　ad01, ad02
テンプレートシェル
　/bin/bash

ユーザーログイン時にホームディレクトリを作成する場合は、
高度なオプションタブで

```
利用者の最初のログイン時にホームディレクトリを作成をチェックする
```

■ Winbind の設定

/etc/samba/smb.conf
すでに編集済みになっているが、一部修正したほうがいいかも

```
/etc/samba/smb.conf
winbind separator = +
template homedir = /home/%U
winbind use default domain = true
```

あたりを見直す

■ Active Directory への参加

```
setenforce 0
```

で SELinux を一時的にオフにしたほうが無難かもしれない。

```
system-config-authentication &
```

で、設定内容を確認して

```
AD（ドメイン）参加
```

を選択する。

■ Winbind の起動と確認

```
/etc/init.d/winbind start
/etc/init.d/winbind status
```

正常に動作していたら自動起動の設定

```
chkconfig winbind on
```

■ Active Directory に登録されているユーザーを取得できるかどうか確認

```
id ユーザ名
```

等で情報を取得できるか確認。

```
# wbinfo -u
Administrator
Guest
....
```

でもいいけど、wbinfo -u を使うと winbind が落ちたりすることがあるので注意。
その場合は

```
/etc/init.d/winbind restart
```

などで winbind を再起動する。

Active Directory 参加（自分で設定ファイルをいじる方法）

■前提

マシン	ドメイン	ホスト名	IP
AD サーバ	vmware.local	ad001	192.168.1.3
参加するマシン	--	test001	192.168.1.18

■ hosts と DNS の設定

/etc/hosts

```
127.0.0.1 localhost
192.168.1.3 ad001.vmware.local ad001
```

192.168.1.18 test001.vmware.local test001
(参加マシンの FQDN を設定)

/etc/resolv.conf に、
search vmware.local
nameserver 192.168.1.3

■ Kerberos の設定

レルム名は基本的に全て大文字。
/etc/krb5.conf

```
[libdefaults]
 default_realm = VMWARE.LOCAL（大文字）
 #default_tkt_enctypes = des-cbc-md5
 #default_tgs_enctypes = des-cbc-md5

 dns_lookup_realm = false
 dns_lookup_kdc = false
 ticket_lifetime = 24h
 forwardable = yes

[realms]
 VMWARE.LOCAL（大文字） = {
  kdc = ad001:88
  admin_server = ad001:749
  default_domain = vmware.local
 }

[domain_realm]
 .vmware.local = VMWARE.LOCAL（大文字）
 vmware.local = VMWARE.LOCAL（大文字）
```

AD が複数ある場合は、

```
[realms]
 VMWARE.LOCAL（大文字） = {
  kdc = ad001:88
  kdc = ad002:88
```

```
 admin_server = ad001:749
 default_domain = vmware.local
}
```

のように kdc を複数記載する。

■ Kerberos 認証の確認

```
kinit administrator@TEST.DOMAIN
```

認証されると何も表示されずにプロンプトに戻ります。

■ Winbind の設定

/etc/samba/smb.conf

```
workgroup = VMWARE
password server = ad001
realm = VMWARE.LOCAL
security = ads
idmap uid = 16777216-33554431
idmap gid = 16777216-33554431
winbind separator = +
template homedir = /home/%U
template shell = /bin/bash
winbind use default domain = true
winbind offline logon = false
```

とか

```
workgroup = VMWARE
realm = VMWARE.LOCAL
security = ads
password server = ad001
encrypt passwords = yes
winbind separator = +

winbind uid = 10000-12000
winbind gid = 10000-12000
template shell = /bin/bash
template homedir = /home/%D/%U
winbind use default domain = true
winbind offline logon = false
```

とか。何となくこんな感じ。

winbind uid と idmap uid は同じ意味。
winbind uid と idmap uid は、バージョン 3.0.25 以降は

```
idmap config VMWARE:range =  10000-12000
```

みたいに書く。
AD が複数ある場合は、

```
password server = ad001 ad002
```

のように記載する。

workgroup は AD の netbios 名。
大抵は、 ad001 か vmware　だと思う。

■アカウント取得方法の変更

/etc/nsswitch.conf

```
passwd:     files winbind
shadow:     files winbind
group:      files winbind
```

■ Active Directory への参加

```
net ads join -U AD 管理者ＩＤ
```

エラーになる場合は

```
setenforce 0
```

で SELinux を一時的にオフにする。
ファイヤーウォールも設定も切ってみる。

```
Failed to join domain: failed to find DC for domain VMWARE.local
```

とエラーが出る場合

```
net ads join -S ad001 -U AD 管理者 ID
```

で AD へ参加する。または

```
 net ads join -I IP アドレス -U AD 管理者 ID
```

でも良い。 hosts と DNS の内容に不一致があるとエラーになることがあるので注意。
参考：https://help.ubuntu.com/community/ActiveDirectoryWinbindHowto

■ Winbind の起動と確認

```
/etc/init.d/winbind start
/etc/init.d/winbind status
```

正常に動作していたら自動起動の設定

```
 chkconfig winbind on
```

■ Active Directory に登録されているユーザーを取得できるかどうか確認

```
id ユーザ名
```

等で情報を取得できるか確認。

```
# wbinfo -u
Administrator
Guest
....
```

でもいいけど、wbinfo -u を使うと winbind が落ちたりすることがあるので注意。
その場合は

```
/etc/init.d/winbind restart
```

などで winbind を再起動する。

Winbind により、ユーザー認証が行えるかどうかを確認

```
wbinfo -a 'ユーザー名%パスワード'
```

■ PAM の設定（GUI で設定する場合）

```
system-config-authentication &
```

を起動して、「ユーザー情報」と「認証」のタブの
Winbind をチェックし、「winbind の設定」を確認。
/etc/samba/smb.conf が正しく設定されていれば、その情報が表示される。
また、オプションで

```
利用者の最初のログイン時にホームディレクトリを作成
```

をチェックする。この設定で

```
/etc/nsswitch.conf
/etc/pam.d/system-auth-ac
```

が編集される

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

の session 部分が

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

や

```
session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
session     optional      pam_mkhomedir.so
```

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

などになっているはず。

■ PAM の設定（手動で書き換える場合）

```
system-config-authentication &
```

を起動して、「ユーザー情報」と「認証」のタブの
Winbind をチェックし、「winbind の設定」を確認。
/etc/samba/smb.conf が正しく設定されていれば、その情報が表示される。
この設定で

```
/etc/nsswitch.conf
/etc/pam.d/system-auth-ac
```

が編集される。設定後、

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

の最後に、SSH でログイン時にディレクトリを自動作成するために

```
session required pam_mkhomedir.so skel=/etc/skel umask=0022
```

を追加する。

手動で設定する場合は
/etc/pam.d/system-auth-ac

```
#%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        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 500 quiet
auth        sufficient    pam_winbind.so use_first_pass
auth        required      pam_deny.so

account     required      pam_unix.so broken_shadow
account     sufficient    pam_succeed_if.so uid < 500 quiet
account     [default=bad success=ok user_unknown=ignore] pam_winbind.so
account     required      pam_permit.so

password    requisite     pam_cracklib.so try_first_pass retry=3
password    sufficient    pam_unix.so md5 shadow nullok try_first_pass use_authtok
password    sufficient    pam_winbind.so use_authtok
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
session required pam_mkhomedir.so skel=/etc/skel umask=0022
```

バージョンによっては、

```
account     [default=bad success=ok user_unknown=ignore] pam_winbind.so
```

があると、ローカルユーザでログインできなかったり、AD ユーザで SSH のログインができなかったりすることがある。
その場合は、この行を削除する。

■ログインできなくなったとき

何らかの原因で AD ユーザでログインできなくなったら

```
net ads join -U AD管理者ＩＤ
```

で参加しなおしたり、OS を再起動したりするとログインできるようになる（みたい）

複数のマシンで uid を統一する

samba のバージョン 3.0.25 以降の書き方

http://phreek.org/guides/centos-6-samba-ad-member-server
http://thinkit.co.jp/cert/article/0707/7/4/2.htm
https://josephscott.org/archives/2005/11/freebsd-users-and-groups-with-samba-winbind-and-active-directory/
http://extrea.hatenablog.com/entry/2012/01/13/234810

smb.conf（抜粋）

```
[global]
idmap config *: backend = rid
idmap config *: range = 1000000-1999999
idmap config VMWARE: backend = rid
idmap config VMWARE: range = 2000000-2999999
```

複数の AD で rid を分ける場合は以下の様な指定も可能

```
[global]
security = domain
workgroup = MAIN

idmap config * : backend        = tdb
idmap config * : range          = 1000000-1999999

idmap config MAIN : backend     = rid
idmap config MAIN : range       = 10000 - 49999

idmap config TRUSTED : backend  = rid
idmap config TRUSTED : range    = 50000 - 99999
idmap config TRUSTED : base_rid = 1000
```

samba のバージョン 3.0.25 以前の書き方

http://d.hatena.ne.jp/dayflower/20070705/1183620884

```
   [2007  /06  /01     23  :32  :09  ,     0  ]     lib/module.c:do_smb_load_module(69  )     Module
‘ /usr/local/lib/samba/idmaprid.so ’ initialization failed: NT_STATUS_OBJECT_NAME_COLLISION
```

のようなエラーがログに出力される場合は、下記の新しい書き方を試す。

smb.conf（抜粋）

```
[global]
allow trusted domains = No

idmap backend = rid:HOGE=1000000-2000000
idmap uid = 1000000-2000000
idmap gid = 1000000-2000000
```

rid:HOGE の範囲は idmap uid、idmap gid の範囲を指定する

idmap backend = rid: の後ろは、

```
“AD ドメイン名（ショートネーム）”=“id map uid/idmap gid と同じ値の範囲”
```

を指定します

idmap 等の情報については /var/cache/samba か /var/lib/samba 以下に格納されているので，一度 winbind を止めて削除します。

```
# service winbind stop
# cd /var/cache/samba
# rm -f *.tdb
# service winbind start
```

正しく設定されているか確認する

http://d.hatena.ne.jp/dayflower/20070705/1183620884
http://extrea.hatenablog.com/entry/2012/01/13/234810

```
wbinfo -n ユーザ ID
S-1-5-21-299502267-436374069-1708537768-1190 User (1)
```

で SID を確認。最後の RID（ここでは 1190）を確認。

```
id ユーザ ID
```

でマップされたユーザ ID を確認し、設定した range の下限 + RID になっていることを確認。

その他の設定

AD 認証のユーザのログインを制御する

samba を利用するための認証はさせたいが、マシンに直接ログインしたり、SSH ログインをさせたくない場合は

```
template shell
```

で制御する。

```
template shell = /bin/false
```

にすると、SSH を含むログインができなくなる。

AD 認証ユーザの一部のみログインを可能にする

http://serverfault.com/questions/224340
/override-template-shell-on-linux-system-in-active-directory-domain

```
template shell = /bin/false
```

に設定して SSH 等のログインをできない状態で、一部の AD ユーザだけをログインしたい場合は

```
/etc/passwd
```

を編集することで、template shell を上書きできる。

```
getent passwd ユーザ
```

で表示された内容を /etc/passwd に追記してシェルやホームディレクトリを編集する。