Connecter Linux à un AD

Redhat IDM et sssd

Par Nicolas Zin – architecte technologique – Savoir-faire Linux

Agenda

- Rappel sur kerberos
- Active Directory et Redhat IDM
- Les différentes facons de connecter une machine Linux à un Active Directory
  - Connection directe
  - Trust AD-Redhat IDM

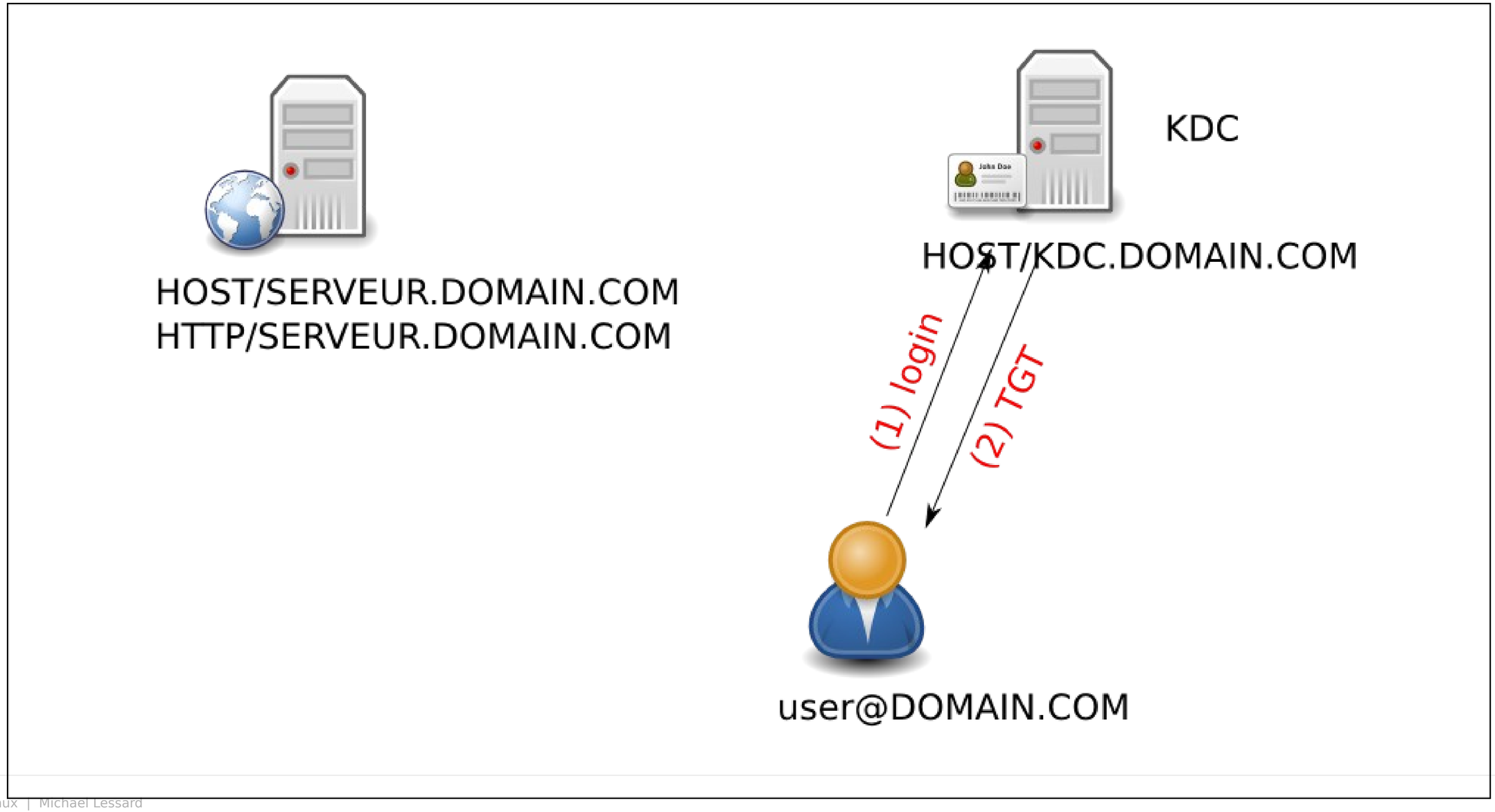
Rappel sur kerberos

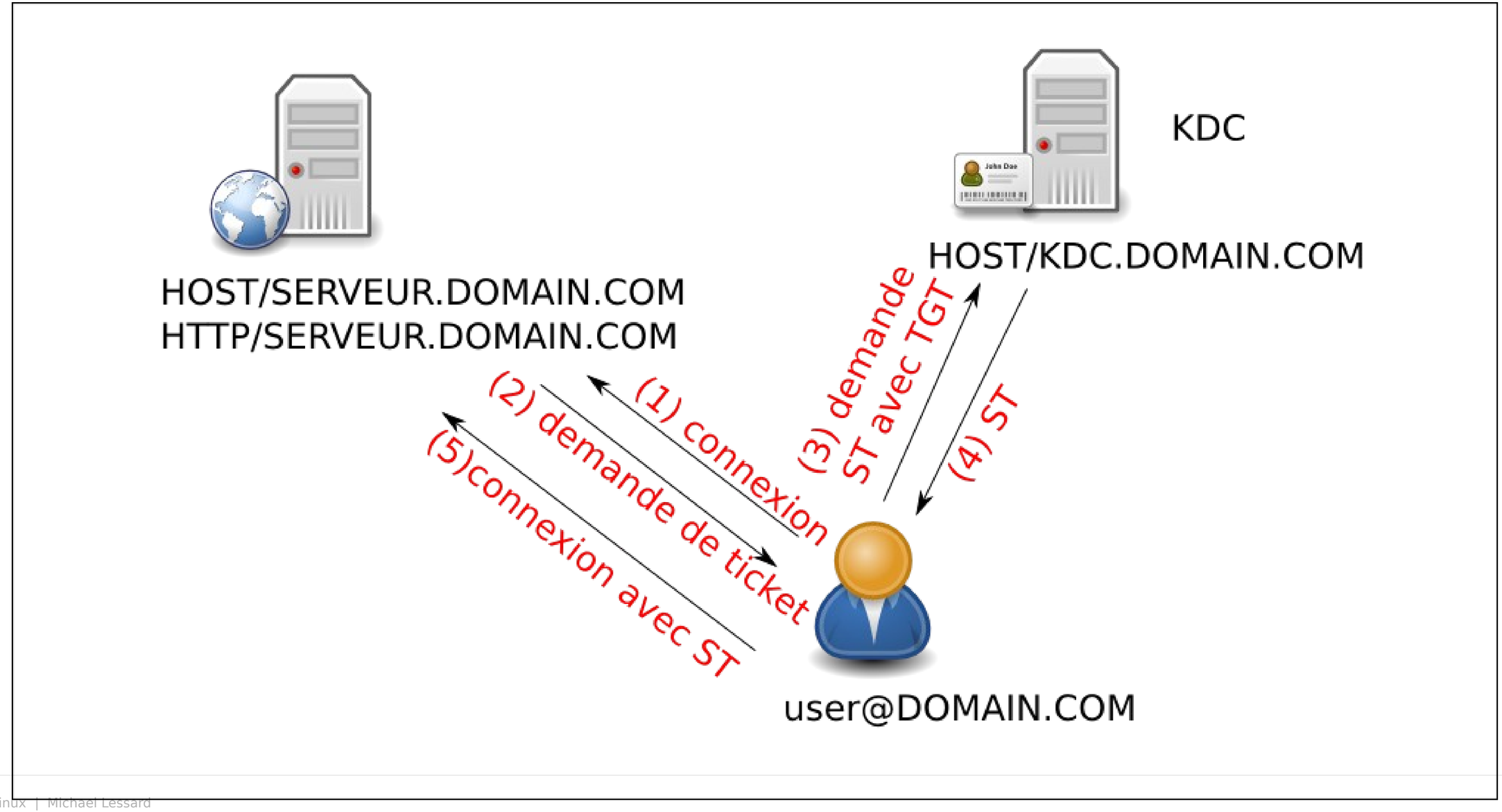
HOST/SERVEUR.DOMAIN.COM
HTTP/SERVEUR.DOMAIN.COM

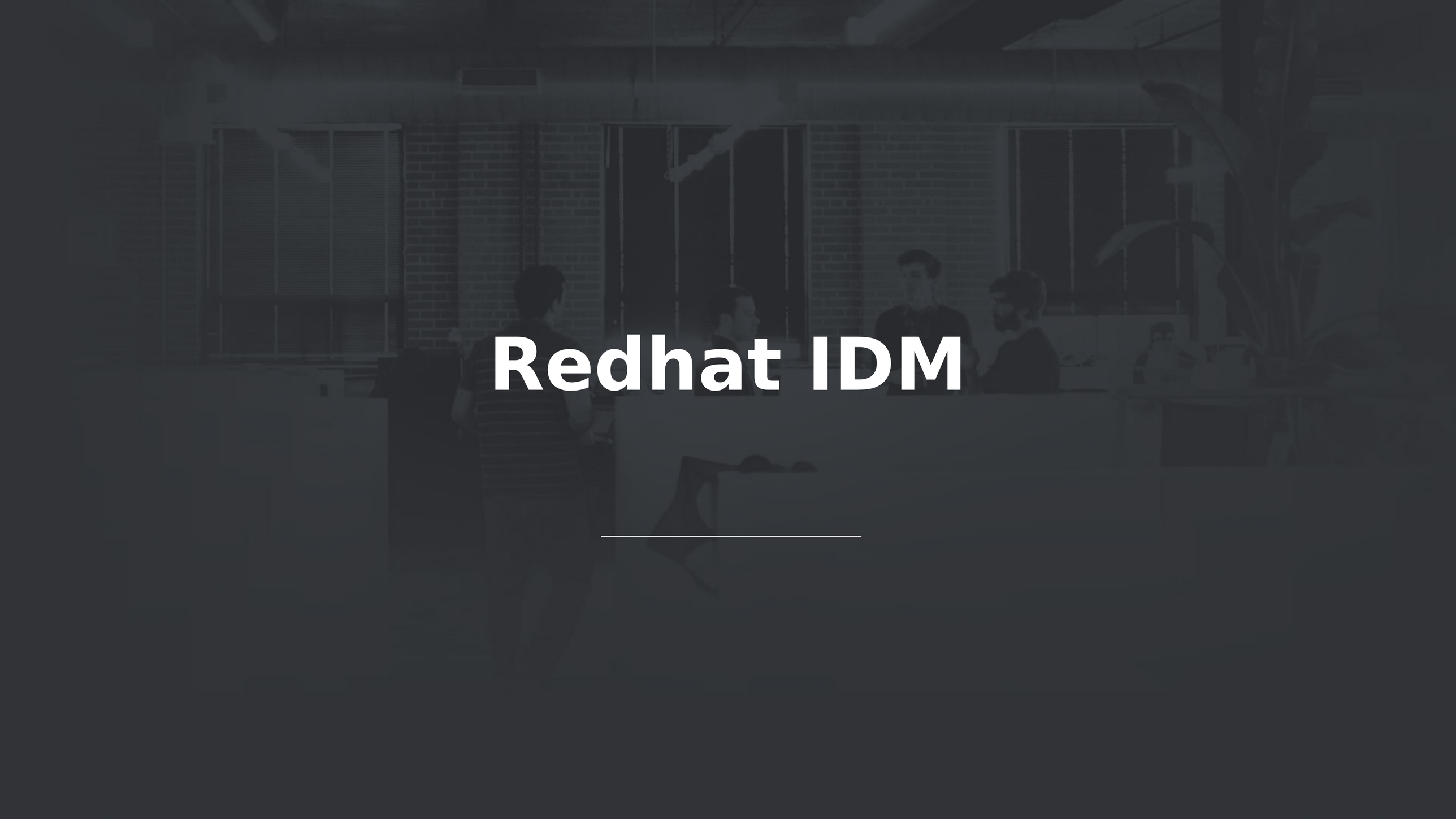
KDC

HOST/KDC.DOMAIN.COM

user@DOMAIN.COM


KDC
HOST/KDC.DOMAIN.COM
HOST/SERVEUR.DOMAIN.COM
HTTP/SERVEUR.DOMAIN.COM
(1) login
(2) TGT
user@DOMAIN.COM


KDC
HOST/KDC.DOMAIN.COM
HOST/SERVEUR.DOMAIN.COM
HTTP/SERVEUR.DOMAIN.COM
(1) connexion
(2) demande de ticket
(3) demande ST avec TGT
(4) ST
(5)connexion avec ST
user@DOMAIN.COM



Redhat IDM

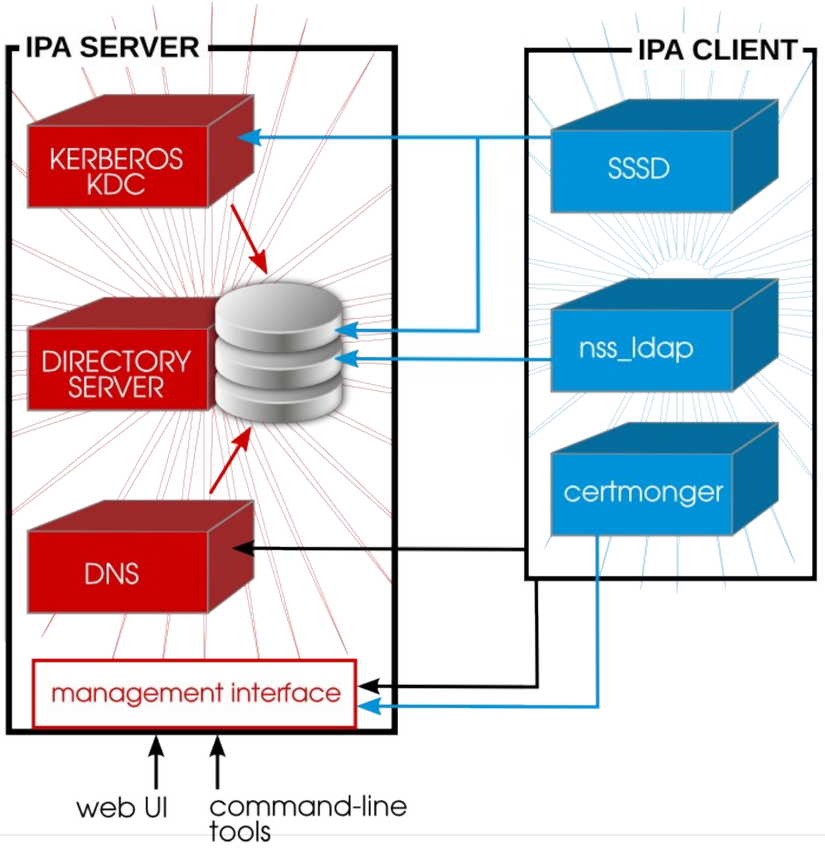
Structure interne

Active Directory =

- Kerberos (+ntp)
- Ldap
- MSRPC (via SMB)

Redhat IDM / FreeIPA =

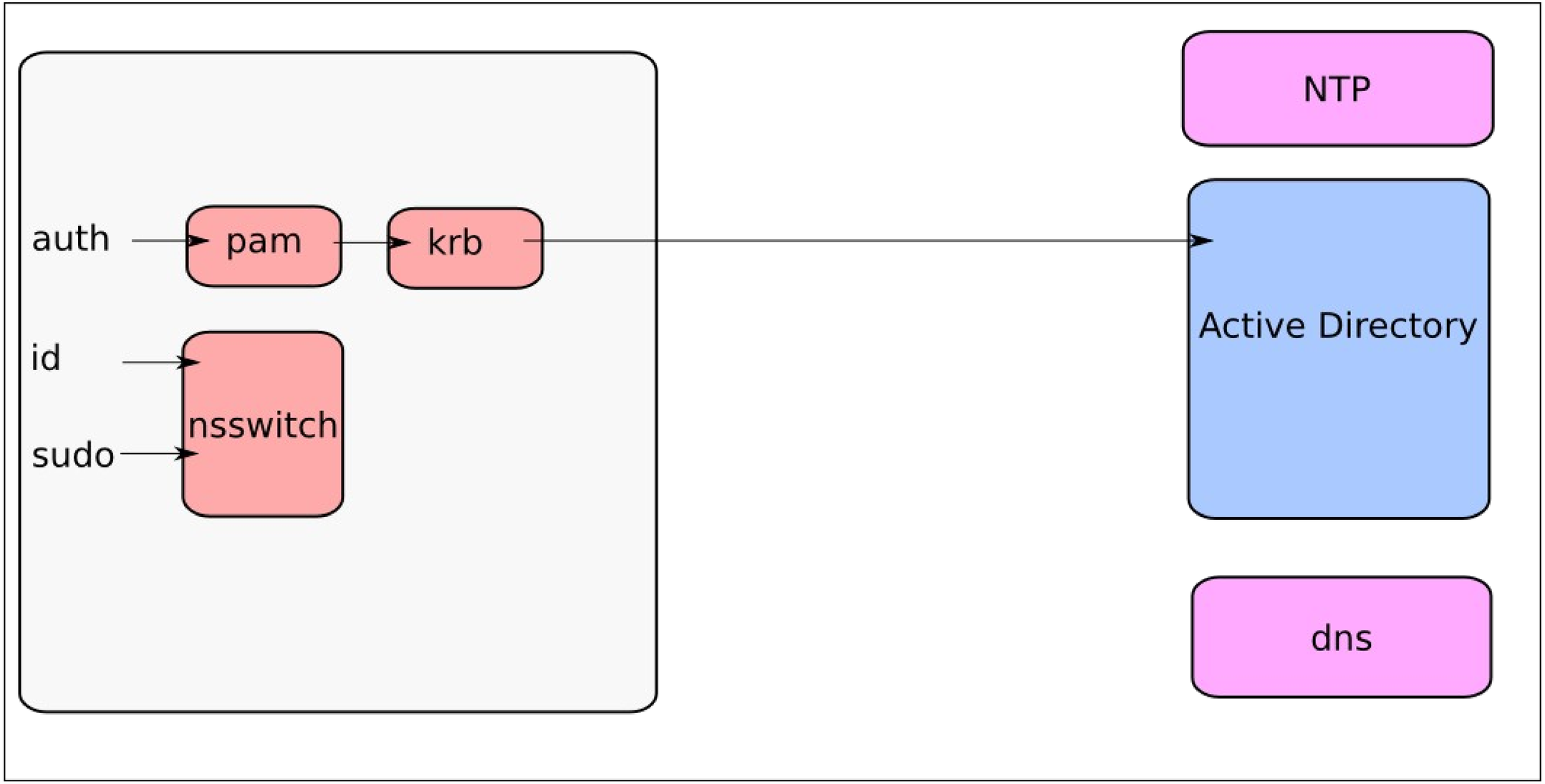
- Kerberos (+ntp)
- Ldap
- dogtag

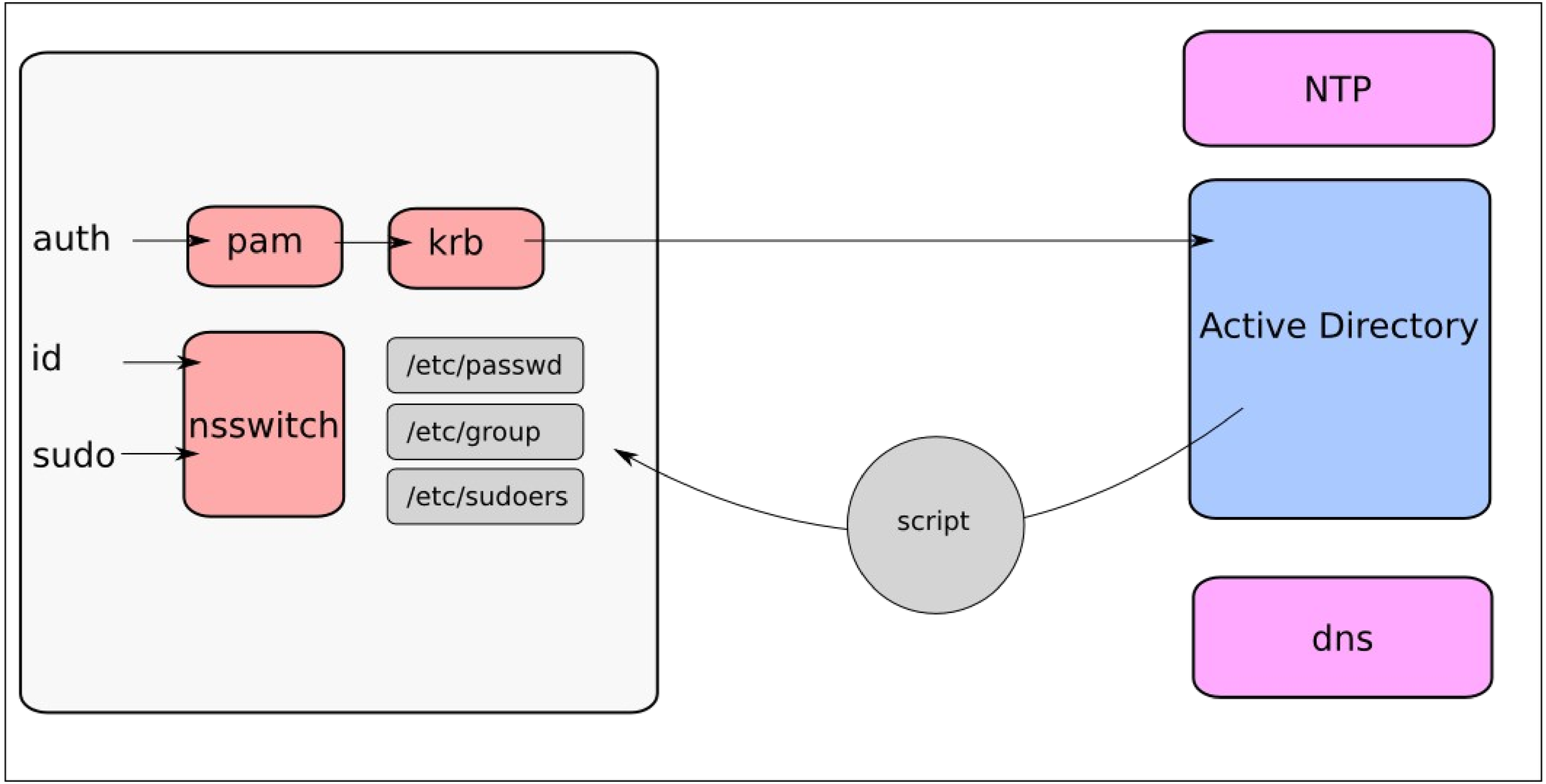


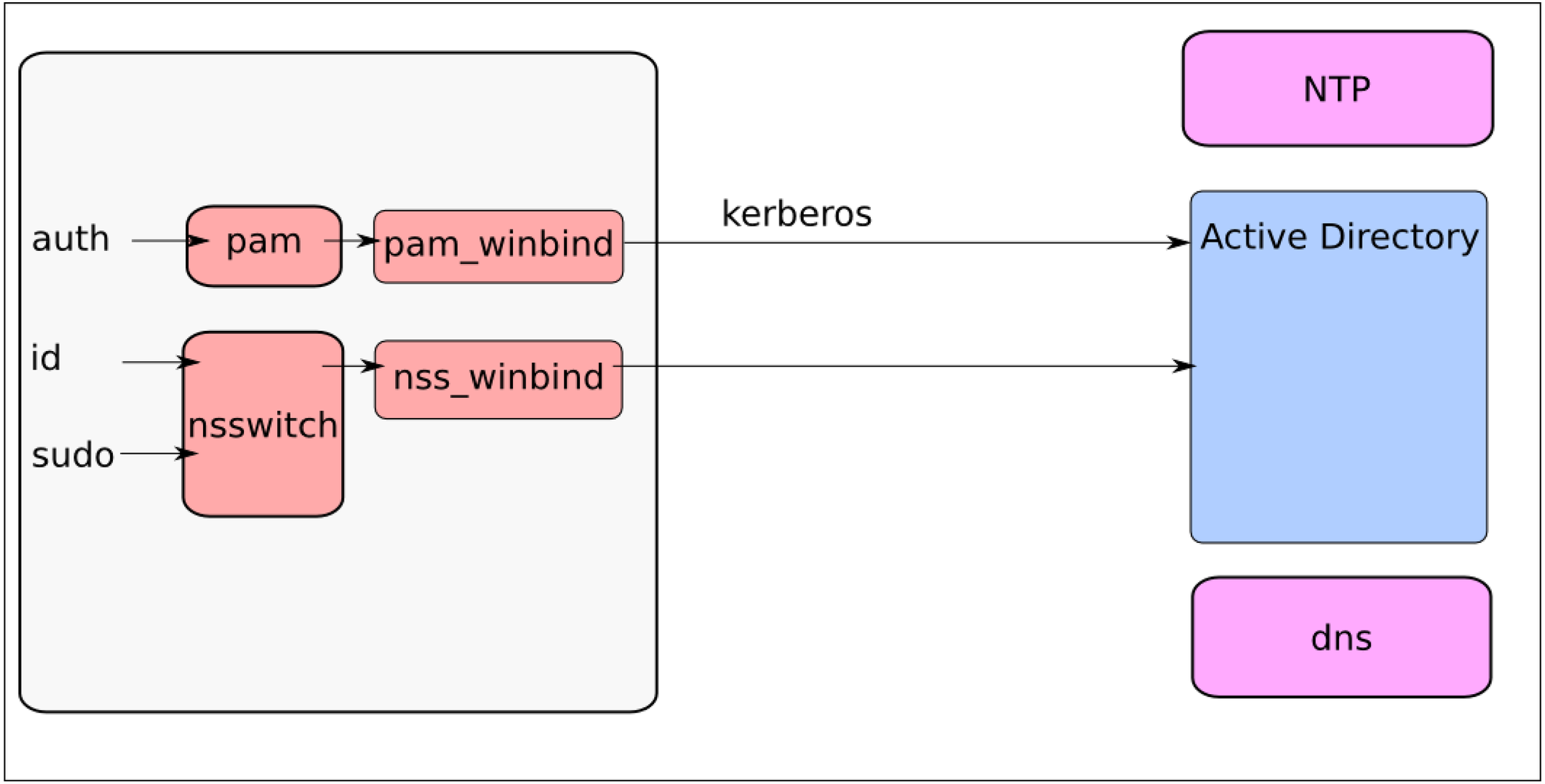
Connection Linux - AD

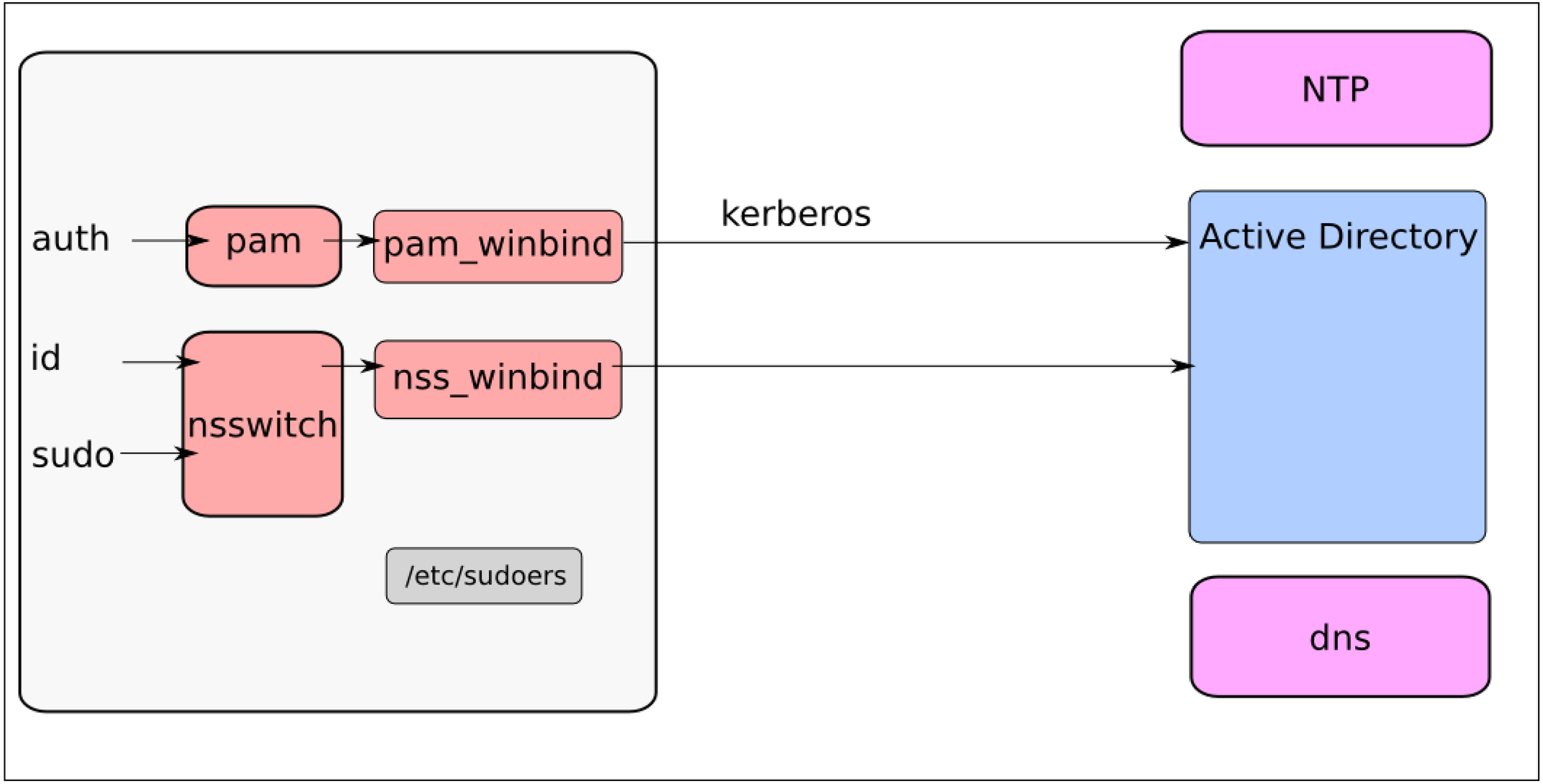
But

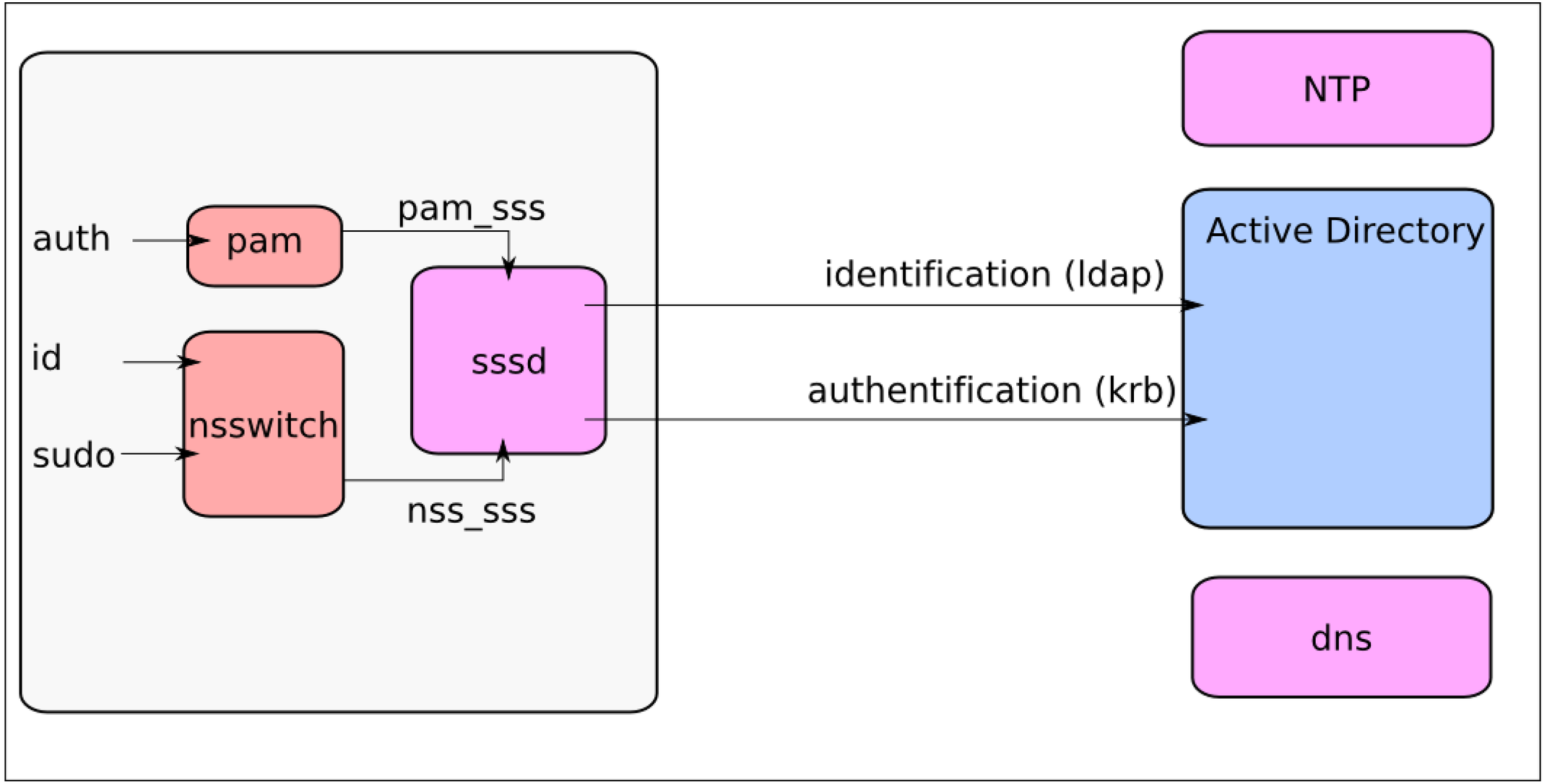
- Des utilisateurs windows doivent pouvoir se connecter aux machines Unix avec leurs login/password
- Si possible on centralise les règles sudo

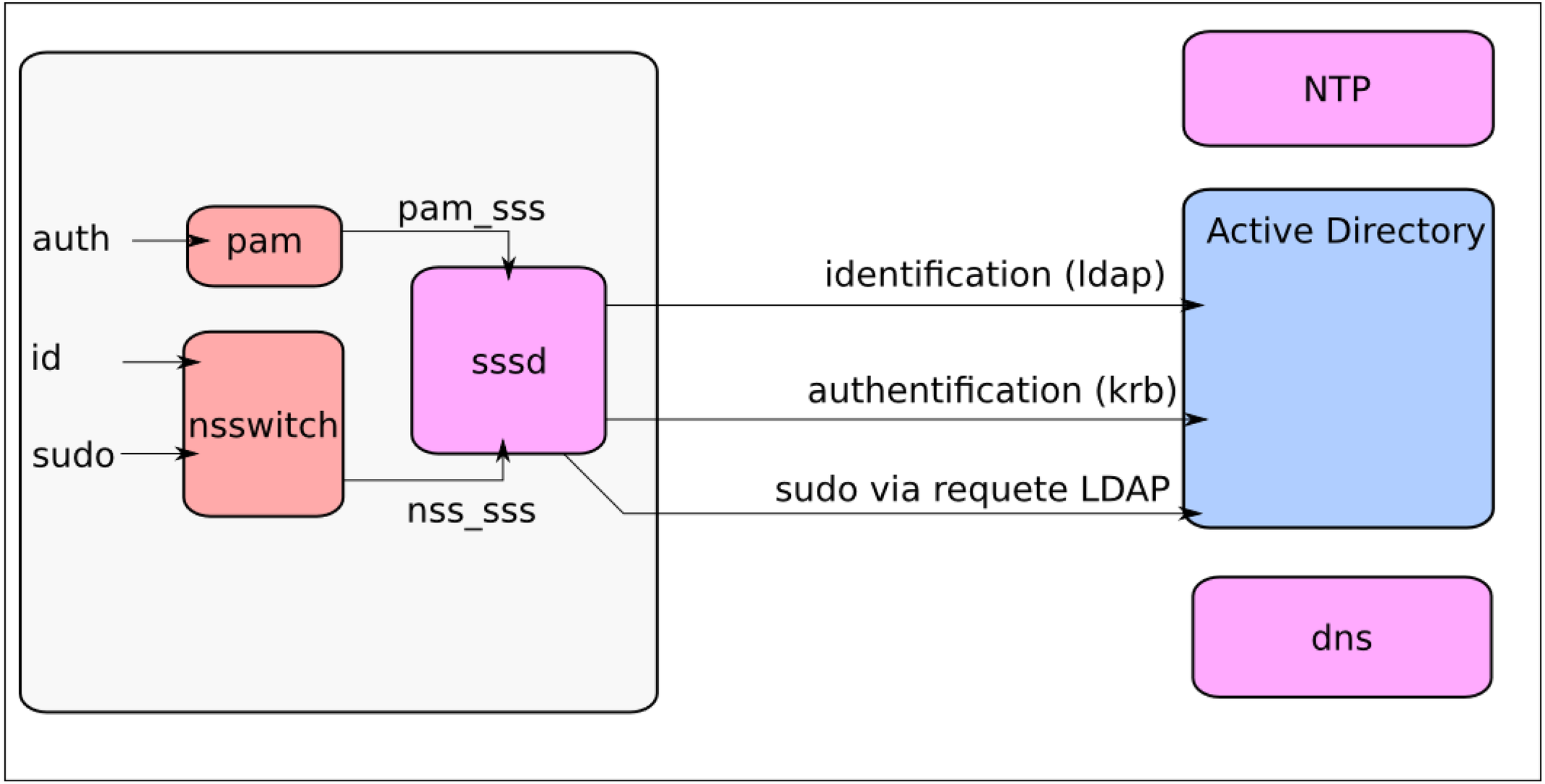

NTP
auth
pam
krb
Active Directory
id
nsswitch
sudo
dns

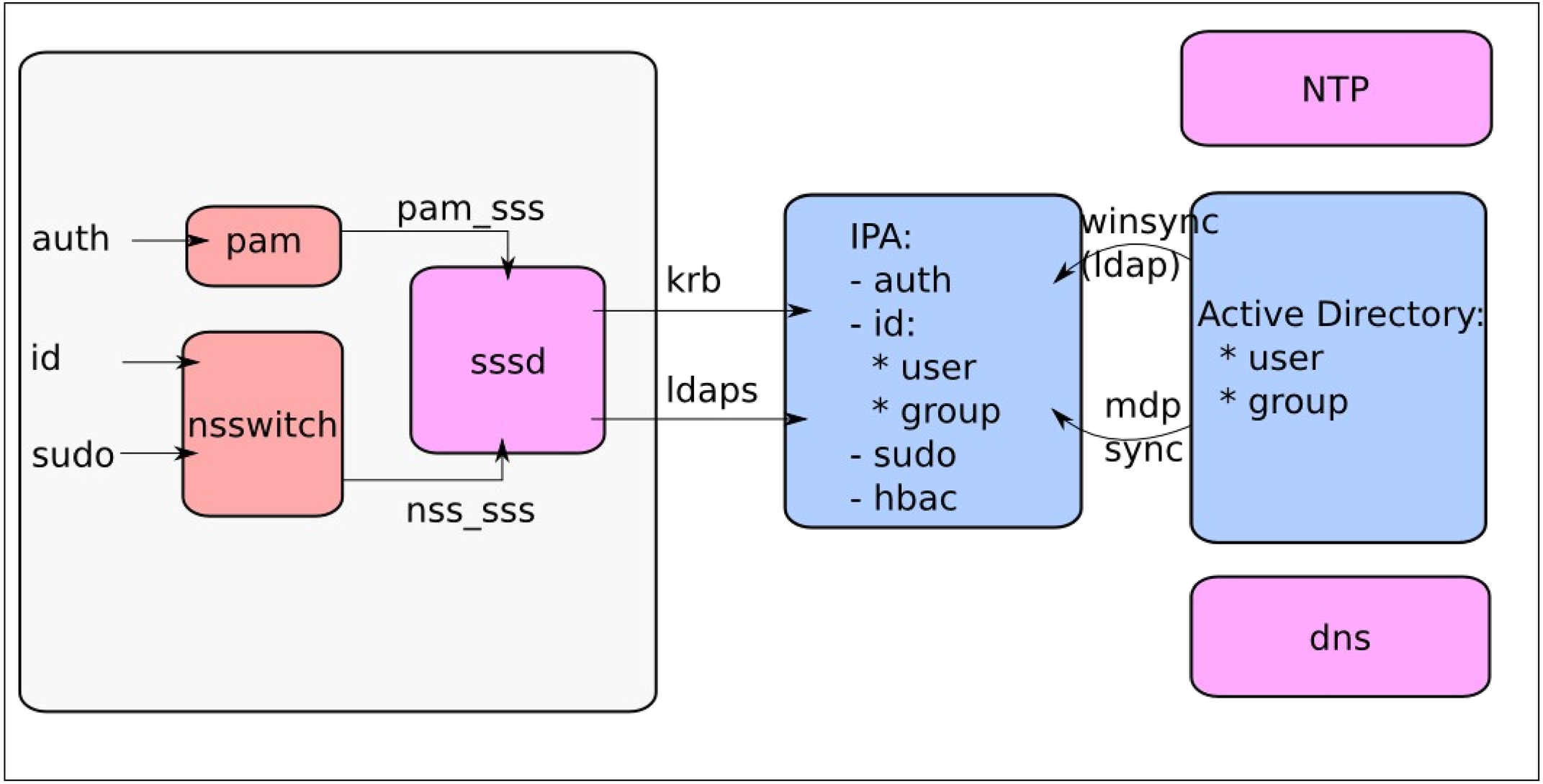

NTP
auth
pam
krb
Active Directory
id
nsswitch
/etc/passwd
/etc/group
/etc/sudoers
sudo
script
dns

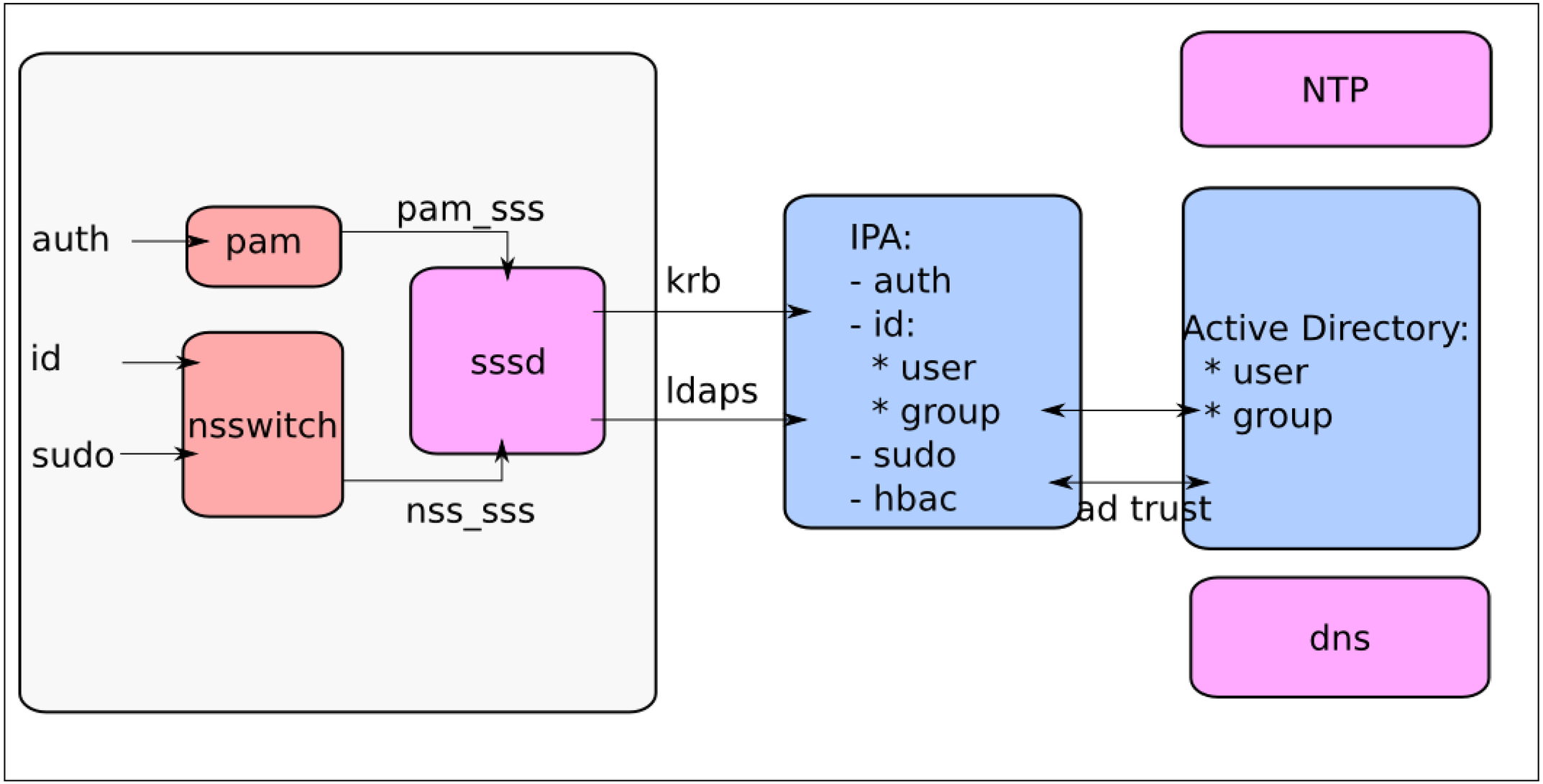

NTP
auth
pam
pam_winbind
kerberos
Active Directory
id
nss_winbind
nsswitch
sudo
dns


NTP
auth
pam
pam_winbind
kerberos
Active Directory
id
nsswitch
nss_winbind
sudo
/etc/sudoers
dns


NTP
Active Directory
dns
auth
pam
pam_sss
id
sudo
nsswitch
sssd
nss_sss
identification (ldap)
authentification (krb)


NTP
Active Directory
auth
pam
pam_sss
id
sudo
nsswitch
sssd
identification (ldap)
authentification (krb)
sudo via requete LDAP
nss_sss
dns


NTP
auth
pam
pam_sss
id
nsswitch
sudo
sssd
krb
ldaps
nss_sss
IPA:
- auth
- id:
* user
* group
- sudo
- hbac
winsync
(ldap)
mdp
sync
Active Directory:
* user
* group
dns


NTP
auth
pam
pam_sss
id
nsswitch
sudo
sssd
krb
ldaps
nss_sss
IPA:
- auth
- id:
* user
* group
- sudo
- hbac
ad trust
Active Directory:
* user
* group
dns

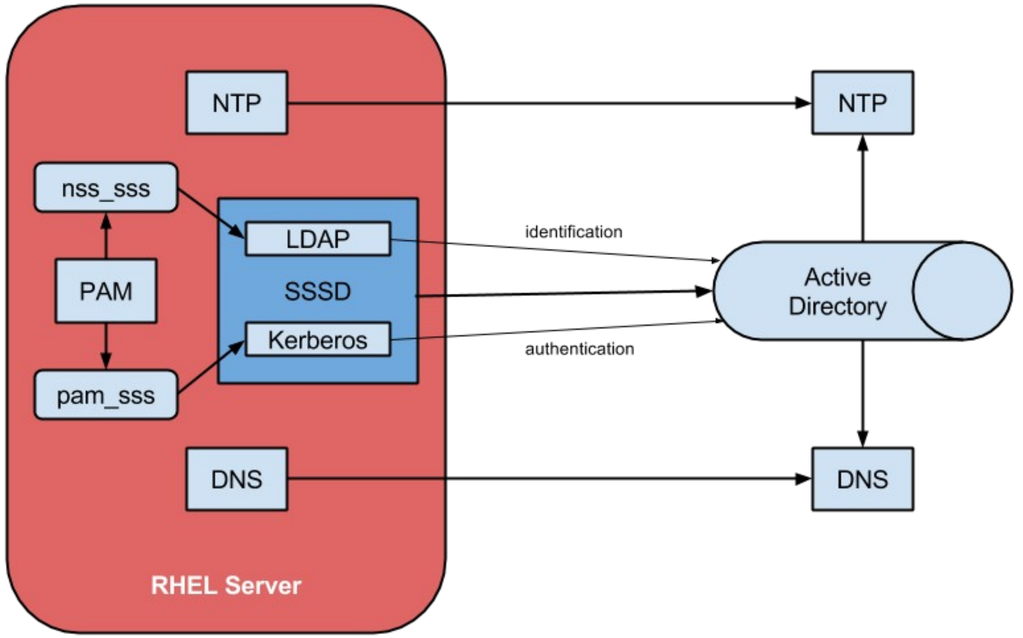
Connection Linux – AD avec sssd

serveur Linux - AD

- - installation des Service For Unix dans l'Active Directory (schema avec uid,gid…)

- yum install sssd sssd-client krb5-workstation samba openldap-clients policycoreutils-python
  kinit Administrator@AD.EXAMPLE.COM
  net ads join createupn=host/client.ad.example.com@AD.EXAMPLE.COM –k
  net ads keytab create
  net ads keytab add host/client.ad.example.com@AD.EXAMPLE.COM

- Configure sssd



- Cf http://www.chriscowley.me.uk/blog/2013/12/16/integrating-rhel-with-active-directory/

Connection via IDM

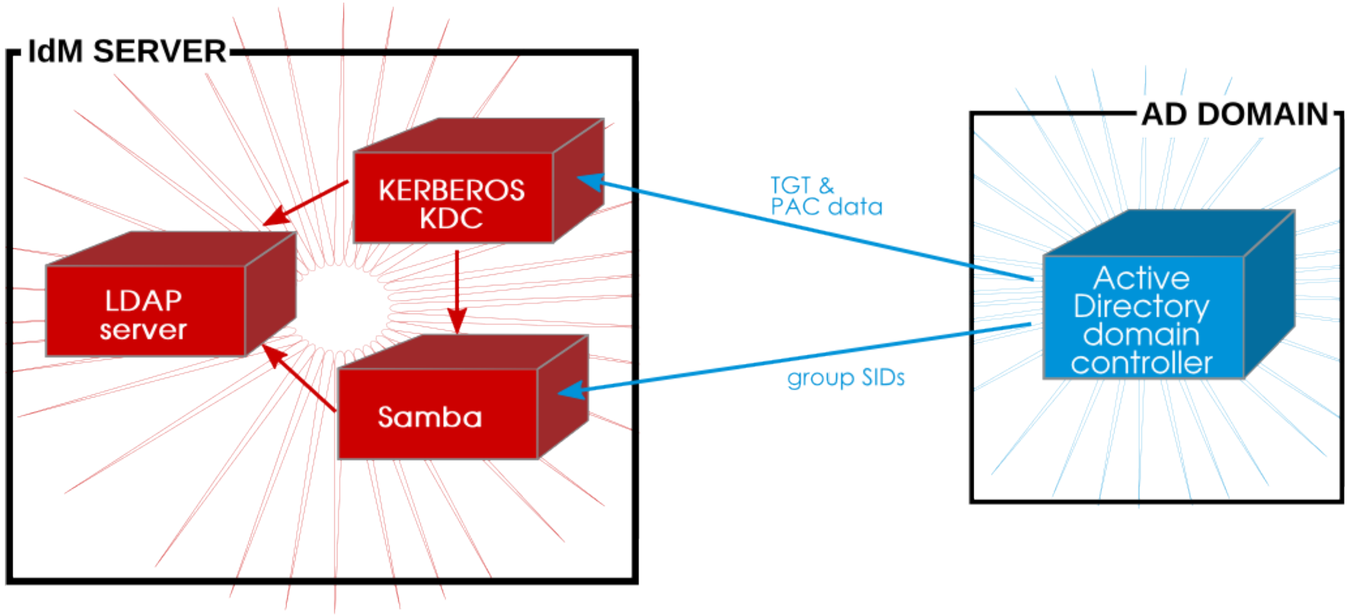
Pré-requis

- Windows 2008 ou 2012
- Redhat 7.1+ sur les serveurs
- Sssd >=1.9 : Redhat 6.4+ pour avoir toutes les fonctionnalités
- Sssd <1.9 : Redhat 5.8+, Redhat 6 à 6.3 : avec des fonctionnalités réduites (hbac, support par couche de compatibilité sur le serveur IDM)

Redhat IDM - AD

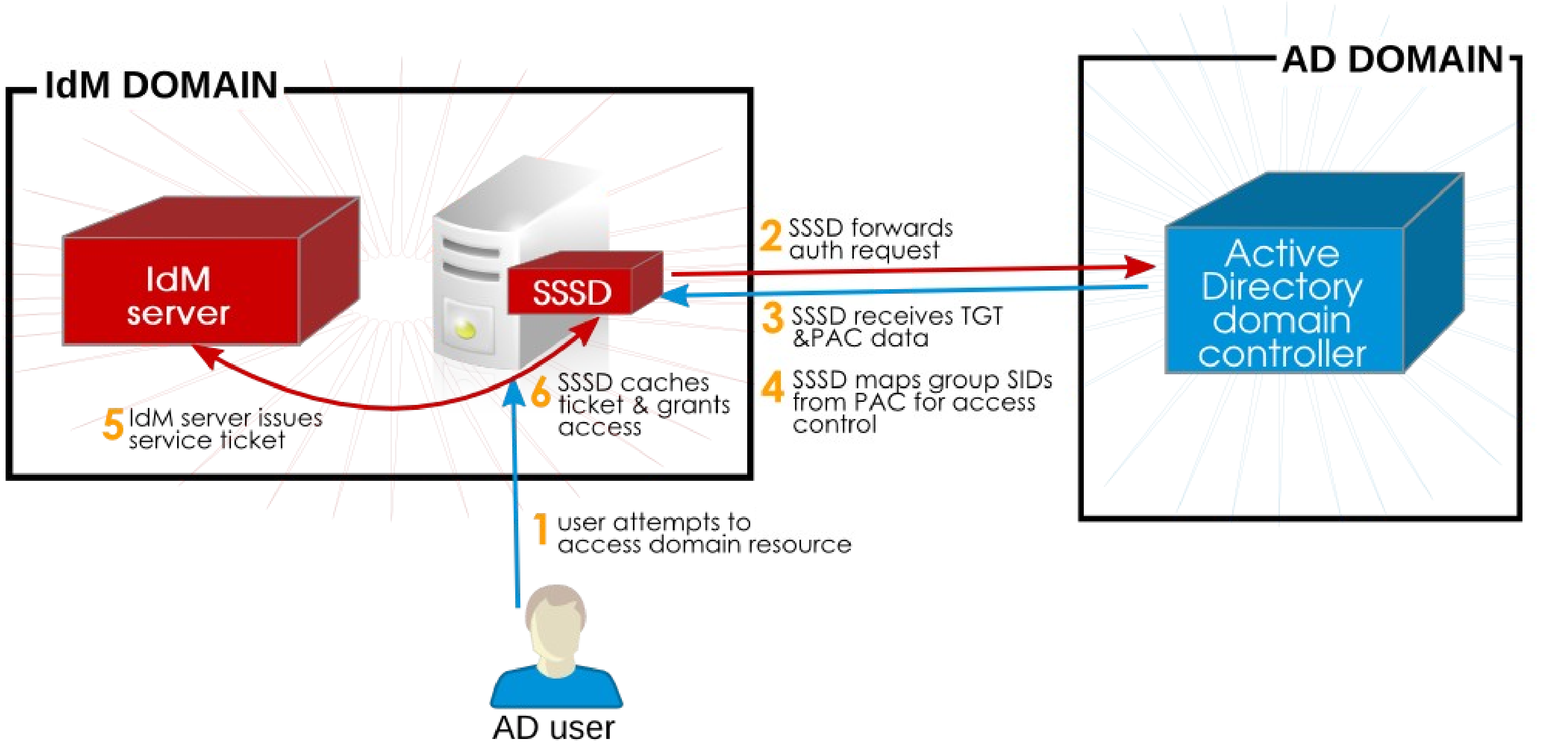
- - installation des Service For Unix dans l'Active Directory optionnel

- ipa-adtrust-install --enable-compat –netbios-name=LINUX
- ipa trust-add --type=ad ipawindows.mtl.sfl --admin Administrator --password



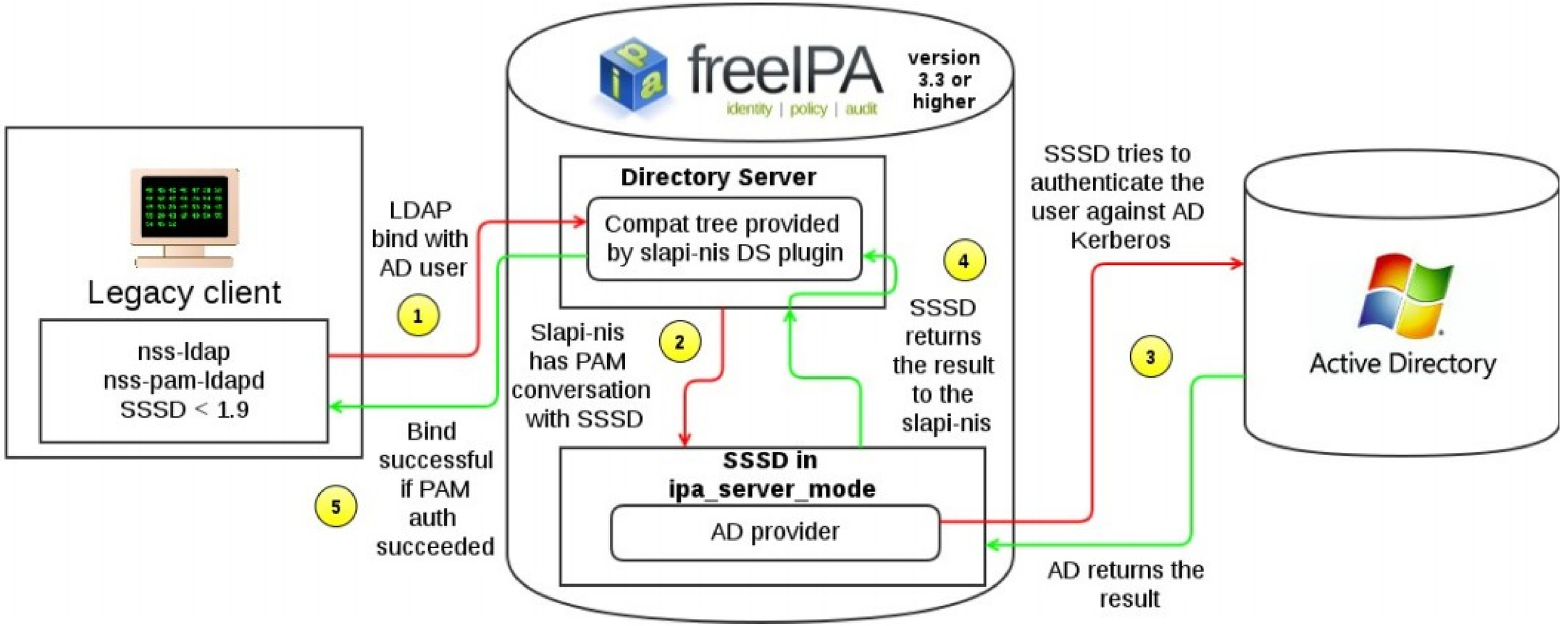
Linux server – Redhat IDM

- yum install ipa-client -y
- Ipa-client-install



Sssd < 1.9

- Redhat5.x et < RHEL 6.4 :



Démonstration

Configuration

- Réseau 10.0.10x
- Domaine Windows : rhugw.local
- Domaine Linux : rhug.local