xrdp sur Debian 13 avec authentification Active Directory

Nov 27, 2026 · @Serge Martins

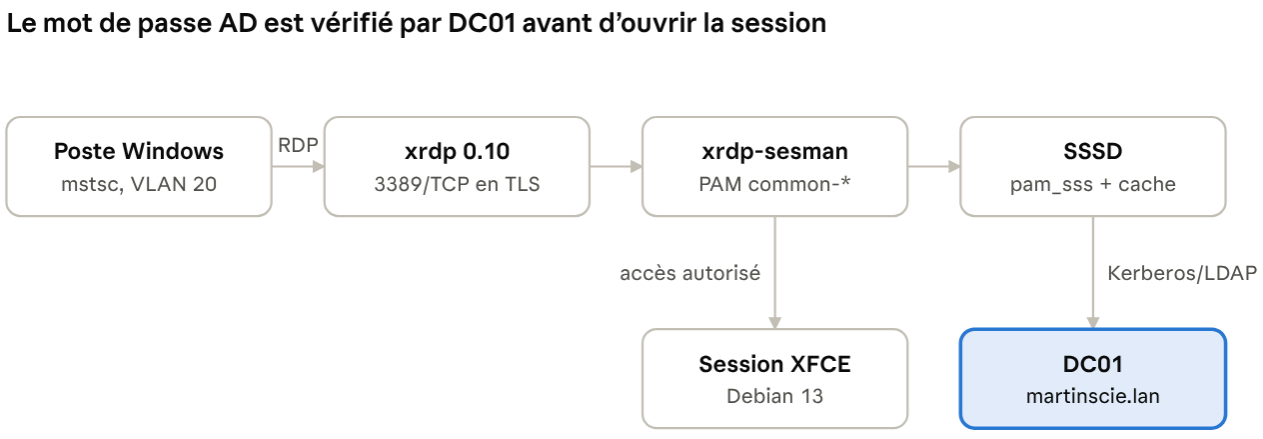
Objectif et architecture

Un utilisateur du domaine (ex. `jdupont`) ouvre une session graphique XFCE sur un serveur **Debian 13** depuis le client Bureau à distance de Windows (mstsc), avec son mot de passe AD. Debian 13 fournit xrdp **0.10.1** (branche maintenue, corrigée de toutes les failles 2026), contre 0.9.21 sur Debian 12 où une faille reste ouverte.

Briques utilisées :

- **realmd + adcli** : jonction de la machine au domaine.
- **SSSD** : utilisateurs et groupes AD, authentification Kerberos via PAM.
- **xrdp + xorgxrdp** : serveur RDP, une session Xorg par utilisateur.
- **XFCE** : bureau léger adapté au RDP.

Élément	Valeur (à adapter)
Domaine / royaume Kerberos	`martinscie.lan` / `MARTINSCIE.LAN`
Contrôleur de domaine	`DC01.martinscie.lan` – `192.168.10.10`
Serveur xrdp	`deb-rdp01.martinscie.lan` – `192.168.10.30` (Debian 13)
Groupe AD autorisé	`GG_RDP_Linux`



Flux d'authentification xrdp → PAM → SSSD → DC01

1. Prérequis

Toutes les commandes se lancent en `root`.

```
hostnamectl set-hostname deb-rdp01.martinscie.lan
```

`/etc/hosts` :

```
127.0.0.1      localhost
192.168.10.30  deb-rdp01.martinscie.lan deb-rdp01
```

`/etc/network/interfaces` (adapter `ens18`) :

```
auto ens18
iface ens18 inet static
    address 192.168.10.30/24
    gateway 192.168.10.254
    dns-nameservers 192.168.10.10
    dns-search martinscie.lan
```

```
systemctl restart networking
host -t SRV _ldap._tcp.martinscie.lan        # doit répondre DC01

# Heure synchronisée sur DC01 (Kerberos : 5 minutes d'écart maximum)
apt update && apt full-upgrade -y
apt install -y chrony
echo "server dc01.martinscie.lan iburst" > /etc/chrony/sources.d/dc01.sources
sed -i 's/^pool /#pool /' /etc/chrony/chrony.conf
systemctl restart chrony && chronyc sources
```

Côté DC01 : créer le groupe `GG_RDP_Linux` et y placer les utilisateurs autorisés.

2. Jonction au domaine

```
apt install -y realmd sssd sssd-tools libnss-sss libpam-sss adcli \
  samba-common-bin oddjob oddjob-mkhomedir packagekit krb5-user
# krb5-user : royaume MARTINSCIE.LAN

realm discover martinscie.lan
realm join -U Administrateur martinscie.lan
pam-auth-update --enable mkhomedir
```

Dans `/etc/sssd/sssd.conf`, section `[domain/martinscie.lan]`, vérifier ou ajouter :

```
use_fully_qualified_names = False
fallback_homedir = /home/%u
ad_gpo_access_control = permissive
```

`ad_gpo_access_control = permissive` évite que les GPO Windows de connexion à distance bloquent xrdp.

```
chmod 600 /etc/sssd/sssd.conf
systemctl restart sssd
id jdupont                                # UID et groupes AD, dont
gg_rdp_linux

# N'autoriser que le groupe RDP et les administrateurs du domaine
realm deny --all
realm permit -g GG_RDP_Linux
realm permit -g "Admins du domaine"
```

3. XFCE et xrdp

```
apt install -y xfce4 xfce4-goodies dbus-x11 xrdp xorgxrdp
adduser xrdp ssl-cert
systemctl enable --now xrdp
```

Session XFCE pour tous — dans `/etc/xrdp/startwm.sh`, juste avant la ligne `test -x /etc/X11/Xsession && exec /etc/X11/Xsession` :

```
unset DBUS_SESSION_BUS_ADDRESS
unset XDG_RUNTIME_DIR
exec startxfce4
```

Fenêtre « Authentification requise » (colord) — créer `/etc/polkit-1/rules.d/45-allow-colord.rules` :

```
polkit.addRule(function(action, subject) {
  if (action.id.indexOf("org.freedesktop.color-manager.") == 0 &&
      subject.isInGroup("gg_rdp_linux")) {
    return polkit.Result.YES;
  }
});
```

4. Configuration et durcissement de xrdp

`/etc/xrdp/xrdp.ini`, section `[Globals]` :

```
port=3389
security_layer=tls
crypt_level=high
```

`/etc/xrdp/sesman.ini` :

```
[Security]
AllowRootLogin=false
; refuse le shell imposé par le client RDP (protection type CVE-2026-33145)
AllowAlternateShell=false

[Sessions]
KillDisconnected=false
DisconnectedTimeLimit=0
```

Dans le bas de `xrdp.ini`, garder la session **Xorg** en premier et commenter `[Xvnc]`.

```
systemctl restart xrdp polkit

# Pare-feu local : RDP seulement depuis le VLAN 20
apt install -y ufw
ufw allow 22/tcp
ufw allow from 192.168.20.0/24 to any port 3389 proto tcp
ufw enable
```

5. Connexion depuis Windows

1. Sur un poste du VLAN 20, lancer `mstsc`.
2. Ordinateur : `deb-rdp01.martinscie.lan`, accepter le certificat.
3. Session **Xorg**, utilisateur `jdupont`, mot de passe AD : le bureau XFCE s'ouvre et `/home/jdupont` est créé.

6. Tests et dépannage

```
realm list
id jdupont
ss -tlnp | grep 3389
journalctl -u xrdp -u xrdp-sesman -f
journalctl -u sssd -f
```

Symptôme	Cause probable	Correction
`realm discover` ne trouve rien	DNS ne pointe pas sur DC01	Corriger le DNS, tester l'enregistrement SRV
`Clock skew too great`	Heure décalée	Vérifier chrony
Refusé sur xrdp mais `su - jdupont` fonctionne	GPO appliquée par SSSD	`ad_gpo_access_control = permissive`
Refusé partout	Utilisateur hors groupe autorisé	L'ajouter à `GG_RDP_Linux`, puis `sss_cache -E`
Écran noir	Clé TLS illisible ou session locale ouverte	`adduser xrdp ssl-cert` ; lignes `unset` dans `startwm.sh`
Connexion refusée par un vieux client RDP	`security_layer=tls`	Mettre à jour le client (mstsc récent)

7. Récapitulatif

```
hostnamectl set-hostname deb-rdp01.martinscie.lan
apt install -y chrony realmd sssd sssd-tools libnss-sss libpam-sss adcli \
  samba-common-bin oddjob oddjob-mkhomedir packagekit krb5-user
realm join -U Administrateur martinscie.lan
pam-auth-update --enable mkhomedir
realm deny --all && realm permit -g GG_RDP_Linux
apt install -y xfce4 xfce4-goodies dbus-x11 xrdp xorgxrdp
adduser xrdp ssl-cert
# startwm.sh : exec startxfce4 ; xrdp.ini : security_layer=tls ;
# sesman.ini : AllowRootLogin=false, AllowAlternateShell=false
systemctl restart sssd xrdp
```

Mettre à jour régulièrement (`apt update && apt full-upgrade`) : xrdp a reçu une vingtaine de correctifs de sécurité en 2026.