CPAM Ardèche / Greta Ardèche-Drôme

Procédure Teleport

Ferme

Collet Valentin
BTS SIO-SISR / Session 2026

SOMMAIRE

Cahier des charges

Descriptifs de l'existant

Infra réseau :

Deux pfsenses en redondance

- Vlan 10 : serveur
  - (AD/DNS + DHCP + GLPI)
- Vlan 20 : prod
- Vlan 30 : serveur redondant
  - (AD/DNS 2 + DHCP 2)
- Vlan 99 : gestion
- Les serveurs AD DNS sont déjà prêts, le service CS est installé sur l'AD ; les serveurs DHCP fonctionnent en load balancing sous debian 13 avec adresse PC management (seul poste du vlan 20 pouvant accéder au teleport via port 443) réservé sur son adresse MAC.

Besoins

Le besoin principal est la mise en place d'un bastion d'accès sécurisé (PAM — Privileged Access Management) au sein de la ferme informatique. Cette solution doit permettre à l'équipe informatique d'accéder de manière centralisée, sécurisée et auditée aux serveurs Linux (SSH) et aux postes Windows (RDP), sans exposer directement ces ressources sur le réseau.

J'ai besoin d'une VM Debian 13 avec les caractéristiques suivantes :

- 2 vCPU minimum (4 en production)
- 4 Go de RAM minimum (8 Go en production)
- 30 Go disque OS + 20 Go pour /var/lib/teleport (stockage des sessions enregistrées)

Fonctionnalités attendues :

- Accès SSH aux serveurs Linux via le client tsh ou l'interface web
- Accès RDP aux postes Windows via l'interface web (sans client lourd)
- Authentification multi-facteurs (OTP/TOTP) pour tous les comptes

- Enregistrement et relecture des sessions pour l'audit
- Gestion fine des droits par rôles (RBAC) avec intégration Active Directory
- Interface web HTTPS sécurisée avec certificat signé par l'AD CS interne

Ports nécessaires ouverts sur le firewall LAN :

- 443/tcp — Interface Web Teleport (HTTPS)
- 3022/tcp — SSH sur les nodes enregistrés
- 3023/tcp — Proxy SSH pour les clients tsh
- 3024/tcp — Tunnel inverse Proxy vers Nodes
- 3025/tcp — Auth Server (restreindre au LAN uniquement)
- 3028/tcp — Windows Desktop Service (RDP via Teleport)

Contraintes

La contrainte principale est la « contrainte temps » : je dispose d'un temps limité pour réaliser l'installation et la configuration complète du bastion afin de pouvoir le présenter dans ma ferme à la fin de l'année scolaire.

Contraintes techniques :

- Intégration obligatoire avec l'Active Directory existant (MySocVCt.fr) pour la gestion des comptes et l'accès RDP via LDAPS
- Le certificat HTTPS doit être signé par l'AD CS interne (MySocVCt-CA) afin que les navigateurs et agents acceptent la connexion sans avertissement
- Synchronisation NTP strictement nécessaire : un décalage d'horloge invalide les certificats Teleport et empêche l'enrôlement des nodes
- Le FQDN du serveur Teleport (teleport.mysocvct.fr) doit être résolu en interne par le DNS de l'AD
- Compatibilité avec l'infrastructure réseau existante : VLANs 10/20/30/99 et pfSense en redondance

Contraintes organisationnelles :

- Le compte de service svc-teleport créé dans l'AD doit suivre le principe du moindre privilège

- Les GPO déployées par le script bootstrap doivent être vérifiées via gpmc.msc avant mise en production

Ressources

Accès à la ferme (hyperviseur proxmox)

Documentation : https://goteleport.com/docs/get-started/deploy-community/

Analyse

Descriptif des solutions

Teleport (open-source) :

Teleport est une plateforme PAM (Privileged Access Management) open-source développée par Gravitational. Elle permet un accès sécurisé, centralisé et entièrement audité aux infrastructures : serveurs Linux (SSH), bureaux Windows (RDP), clusters Kubernetes, bases de données et applications web, le tout depuis une interface web unifiée ou via le client CLI tsh. Teleport intègre nativement l'authentification multi-facteurs (OTP, WebAuthn), un RBAC granulaire, l'enregistrement et la relecture des sessions, une PKI interne automatisée ainsi qu'une intégration LDAP/AD. La solution s'appuie sur des certificats à durée de vie courte en lieu et place de mots de passe statiques, réduisant considérablement la surface d'attaque. L'édition Community est gratuite et open-source ; une édition Enterprise existe avec un support professionnel.

Apache Guacamole :

Apache Guacamole est une passerelle d'accès à distance open-source, sans client (« clientless »), accessible entièrement depuis un navigateur web en HTML5. Elle supporte les protocoles RDP, SSH et VNC et permet ainsi d'accéder à des machines distantes sans installer de logiciel sur le poste utilisateur. Guacamole s'appuie sur un serveur guacd qui traduit les protocoles et les transmet au navigateur. L'outil s'intègre avec LDAP/AD pour la gestion des comptes, propose un enregistrement de session basique et peut être couplé à un fournisseur d'identité externe (OpenID, SAML). En revanche il ne dispose pas de RBAC natif avancé ni de PKI intégrée, et son architecture (Tomcat + guacd) est plus complexe à maintenir.

Comparaison des solutions :

	Teleport	**Apache Guacamole**
Protocoles supportés	SSH, RDP, Kubernetes, BDD, apps web	SSH, RDP, VNC
Interface utilisateur	Web (HTTPS) + CLI tsh	Web uniquement (HTML5)
Client requis	Optionnel (tsh pour SSH avancé)	Aucun (100 % navigateur)
Authentification MFA	Native : OTP, WebAuthn, SSO SAML/OIDC	Extérieures uniquement (SAML/OIDC)
Gestion des rôles (RBAC)	Granulaire natif par ressource et label	Basique (groupes de connexion)
Intégration AD/LDAP	Oui, via LDAPS avec compte de service	Oui, via LDAP
Enregistrement de sessions	Complet : SSH, RDP, rejouable en web	Basique (vidéo RDP uniquement)
PKI / certificats	PKI interne automatisée + compatible AD CS	Dépend d'une PKI externe
Audit & traçabilité	Journal d'audit complet	Journaux Apache basiques
Architecture	Service unique (Auth + Proxy + SSH)	Tomcat + guacd + base de données
Complexité d'installation	Modérée (binaire + YAML)	Importante (Java, Tomcat, guacd)
Licence	Open-source (Apache 2) + Enterprise payant	Open-source (Apache 2)
Points forts	Sécurité Zero Trust, RBAC avancé, PKI auto	Sans client, simple pour RDP/VNC

Limite principale	Nécessite un agent sur chaque node	Pas de RBAC fin, pas de PKI native

Choix d'une solution

Dans le contexte de la ferme informatique, la solution retenue est Teleport.

Guacamole présente l'avantage d'être entièrement accessible depuis un navigateur sans installation de client, ce qui peut être séduisant pour un accès RDP rapide. Cependant il ne propose pas de RBAC natif granulaire, pas de PKI intégrée, et son enregistrement de sessions reste limité. Sa pile technique (Tomcat, guacd, base de données) est également plus lourde à maintenir.

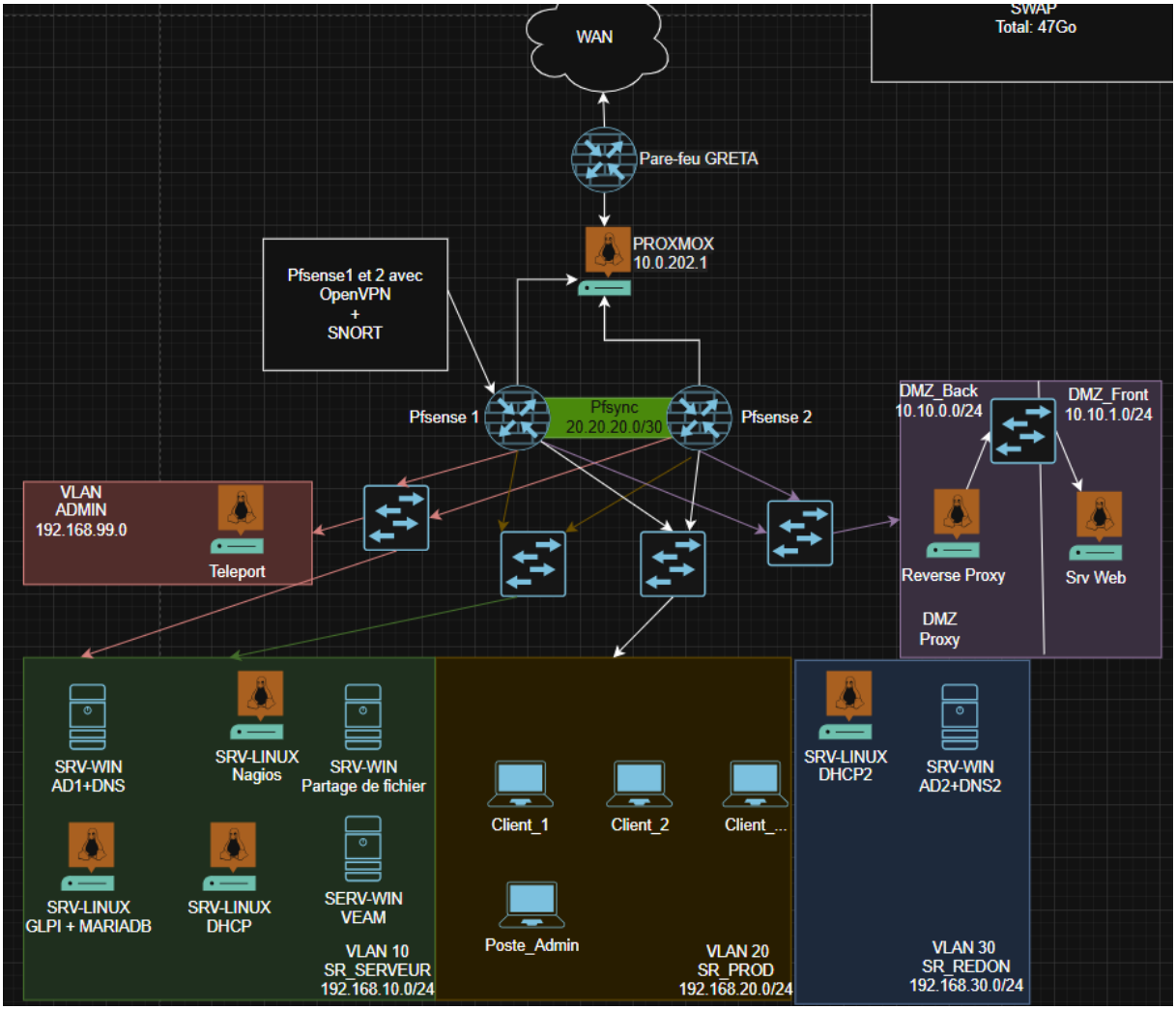
Teleport répond à l'ensemble des besoins identifiés : accès SSH et RDP centré, MFA natif, enregistrement complet des sessions, RBAC par label, intégration Active Directory via LDAPS, et PKI automatisée compatible AD CS. L'architecture en service unique (binaire + fichier YAML) simplifie le déploiement et la maintenance. Enfin le modèle Zero Trust (certificats à durée de vie courte, pas de mot de passe statique) renforce considérablement la posture de sécurité de l'infrastructure.

Étude de l'impact sur le SI existant :

L'ajout de Teleport aura les impacts suivants sur le système d'information :

- Organisationnels : centralisation des accès privilégiés sur un point unique, simplification de la gestion des droits et traitement facilité des demandes d'accès
- Sécurité : élimination des accès SSH par clé statique ou mot de passe, enregistrement systématique des sessions, possibilité de révoquer un accès instantanément
- Humains : réduction des risques d'erreur humaine grâce au RBAC et à l'audit ; les techniciens disposent d'un accès unifié sans gérer plusieurs jeux d'identifiants
- Technique : ajout d'un nœud supplémentaire sur le VLAN serveur (VLAN 10), GPO déployées sur l'AD, règles firewall à ouvrir sur pfSense

Plan d'adressage schéma réseau :



	Adresse réseau	Netmask	1ère adresse	Dernière adresse	Broadcast
PfSync	172.16.0.0	255.255.255.252	.1	.2	.3
Vlan_Prod	192.168.20.0	255.255.255.0	192.168.0.1	192.168.0.254	192.168.0.255
Vlan_Serveur	192.168.10.0	255.255.255.	192.168.10.1	192.168.10.254	192.168.10.255
Vlan_Serv_Redondance	192.168.30.0	255.255.255.0	192.168.30.1	192.168.30.254	192.168.30.255
SR_Admin	192.168.99.0	255.255.255.0	.1	.254	192.168.99.255

DMZ_Back	10.10.0.0	255.255.255.0	10.10.0.1	10.10.0.254	10.10.0.254
DMZ_Front	10.10.1.0	255.255.255.0	10.10.1.1	10.10.1.254	10.10.1.255

VM / Ressource	Adresse IP	VLAN	Gateway
Teleport (Debian 13)	192.168.99.10/24	VLAN 99 (gestion)	192.168.99.254
WAdDns01 (AD/DNS)	192.168.10.1/24	VLAN 10 (serveurs)	192.168.10.254
W11-ITAdmin (client Windows)	DHCP réservé 192.168.20.5	VLAN 20 (prod)	DHCP réservé
DHCP 1	192.168.10.7	VLAN 10	192.168.10.254
DHCP 2	192.168.30.8	VLAN 30 (redondance)	192.168.30.254

Phasage de l'intervention

1. Installation et configuration de la VM Debian 13
    - Test : vérifier la résolution DNS du FQDN (nslookup teleport.mysocvct.fr)
    - Test : vérifier la synchronisation NTP (chronyc tracking)
2. Installation du binaire Teleport et génération du fichier /etc/teleport.yaml
    - Test : teleport configure --test /etc/teleport.yaml
3. Génération de la CSR et signature par l'AD CS, rapatriement des certificats
    - Test : openssl verify -CAfile ca.crt teleport.crt
4. Démarrage du service Teleport et première connexion à l'interface web
    - Test : accès HTTPS à https://teleport.mysocvct.fr sans avertissement certificat
    - Test : tsh login depuis un poste client
5. Enrôlement d'un premier node Linux (agent SSH)
    - Test : tsh ls affiche le node enrôlé
    - Test : tsh ssh root@serveur fonctionne et la session est enregistrée
6. Configuration de l'agent Active Directory (Windows Desktop Service)
    - Test : exécution du script bootstrap PowerShell sans erreur

- Test : tsh desktop ls liste les desktops Windows
- Test : connexion RDP via l'interface web Teleport

7. Création des rôles RBAC et assignation aux utilisateurs
   - Test : tctl get users/admin confirme les rôles assignés

Mise en place

8. Prérequis :

Une VM debian 13 :

Composant	Minimum
vCPU	2 vCPU
RAM	4 Go
Disque OS	30 Go
Disque /var/lib/teleport	20 Go
OS	Debian 13 Trixie 64-bit

- DNS interne resolvant le FQDN Teleport (ex : teleport.domaine.local)
- NTP synchronise (important pour la validite des certificats Teleport)
- AD CS
- Ports a ouvrir sur le firewall LAN :
  - 443/tcp -- Interface Web Teleport (HTTPS)
  - 3023/tcp -- Proxy SSH pour les clients tsh
  - 3024/tcp -- Tunnel inverse Proxy vers Nodes
  - 3025/tcp -- Auth Server (restreindre au LAN uniquement)
  - 3022/tcp -- SSH sur les nodes enregistres

2. Préparation de Debian 13

2.1 Mise à jour et outils

```
apt install -y curl wget gnupg2 openssl chrony net-tools dnsutils apt-
transport-https ca-certificates



# Synchronisation NTP (important pour la validite des certs Teleport)

systemctl enable --now chrony

chronyc tracking
```

2.2 Hostname et DNS

Le FQDN défini ici sera inclus automatiquement dans le SAN du certificat auto-signé par Teleport.

```
sudo hostnamectl set-hostname teleport.domaine.local



# Verifier la resolution DNS

nslookup teleport.domaine.local



# Fallback /etc/hosts si DNS pas encore propage

echo '192.168.X.X  teleport.domaine.local  teleport' | sudo tee -a /etc/hosts
```

2.3 Utilisateur système Teleport

```
useradd --system --no-create-home --shell /usr/sbin/nologin teleport

mkdir -p /var/lib/teleport /var/log/teleport

chown -R teleport:teleport /var/lib/teleport /var/log/teleport

chmod 750 /var/lib/teleport
```

2.4 Installation du Binaire Teleport

Installation de curl et des binaires Teleport. Via scp (téléchargement Windows et transfert du .deb) et dpkg -i selon version, sinon :

```
apt install curl -y

curl https://cdn.teleport.dev/install.sh | bash -s 18.7.0
```

3. Préparation du Certificat sur Teleport

Créer le fichier de configuration pour la CSR, générer la clé privée, puis soumettre à AD CS depuis Windows.

```
# Créer le fichier de configuration pour la CSR
```

```
cat > /tmp/teleport-csr.conf <<EOF
[req]
default_bits       = 4096
prompt             = no
default_md         = sha256
distinguished_name = dn
req_extensions     = req_ext

[dn]
CN = teleport.mysocvct.fr

[req_ext]
subjectAltName = @alt_names

[alt_names]
DNS.1 = teleport.mysocvct.fr
DNS.2 = *.teleport.mysocvct.fr
EOF

# Générer la clé privée et la CSR
openssl req -new -newkey rsa:4096 -nodes \
  -keyout /var/lib/teleport/teleport.key \
  -out /tmp/teleport.csr \
  -config /tmp/teleport-csr.conf

# Vérifier la CSR
openssl req -text -noout -in /tmp/teleport.csr
```

Soumettre la CSR à AD CS depuis Windows (PowerShell) :

```
# Transfert de la CSR depuis le serveur Linux vers Windows
scp telloc@192.168.99.10:/tmp/teleport.csr "C:\temp\"

# Soumettre la CSR et récupérer le certificat signé
certreq -submit -attrib "CertificateTemplate:WebServer" `
```

```
  C:\temp\teleport.csr `
  C:\temp\teleport.crt


# Exporter le certificat CA
certutil -store Root "MySocVCt-CA" C:\Temp\CaMySocVCt.crt


# Convertir en PEM pour Debian
certutil -encode C:\Temp\CaMySocVCt.crt C:\Temp\CaMySocVCt.pem


# Copier vers le serveur Linux Teleport
scp "C:\Temp\CaMySocVCt.pem" "C:\Temp\teleport.crt"
telloc@192.168.99.10:/tmp/
```

Sur la VM Teleport :

```
# Placer les certificats
cp teleport.crt /var/lib/teleport/teleport.crt
chmod 600 /var/lib/teleport/teleport.key
chmod 644 /var/lib/teleport/teleport.crt


# Installer le certificat CA dans le store système Debian
cp ca.crt /usr/local/share/ca-certificates/mysocvct-ca.crt
update-ca-certificates
```

4. Configuration de Teleport

4.1 Générer /etc/teleport.yaml

La commande teleport configure sans option de certificat laisse Teleport gérer sa propre CA :

```
sudo teleport configure \
  --cluster-name=teleport.mysocvct.fr \
  --public-addr=teleport.mysocvct.fr:443 \
  -o file


sudo chmod 640 /etc/teleport.yaml
sudo chown root:teleport /etc/teleport.yaml
```

4.2 Configuration complète /etc/teleport.yaml

```
tee /etc/teleport.yaml << 'EOF'
teleport:
    nodename: teleport.domaine.local
    data_dir: /var/lib/teleport
    log:
        output: /var/log/teleport/teleport.log
        severity: INFO


auth_service:
    enabled: yes
    cluster_name: teleport.mysocvct.fr
    listen_addr: 0.0.0.0:3025
    public_addr: teleport.mysocvct.fr:3025
    authentication:
        type: local
        second_factor: otp


ssh_service:
    enabled: yes
    listen_addr: 0.0.0.0:3022
    public_addr: teleport.domaine.local:3022
    labels:
        env: production
        role: auth-proxy


proxy_service:
    enabled: yes
    listen_addr: 0.0.0.0:3023
    public_addr: teleport.domaine.local:443
    web_listen_addr: 0.0.0.0:443
    tunnel_listen_addr: 0.0.0.0:3024
    https_keypairs:
      - key_file: /var/lib/teleport/teleport.key
```

```
        cert_file: /var/lib/teleport/teleport.crt

EOF
```

4.3 Valider la configuration

```
teleport configure --test /etc/teleport.yaml

# Attendu : Configuration looks good.
```

Ajout agent (nœud Linux)

```
# Copier le certificat CA depuis la VM Teleport vers le nouvel agent

scp telloc@teleport.mysocvct.fr:/usr/local/share/ca-
certificates/CAMySocVCt.crt \

  /usr/local/share/ca-certificates/CAMySocVCt.crt



# Mettre à jour le store (doit afficher "1 added")

update-ca-certificates



# Enrôler le nœud

bash -c "$(curl -fsSL https://teleport.mysocvct.fr/scripts/XXXXX/install-
node.sh)"
```

Ajout agent Active Directory (Windows Desktop)

Récupérer le script de configuration depuis le serveur Teleport et le transférer sur le serveur AD :

```
tctl desktop bootstrap > configure-ad.ps1

# Transférer le script sur le serveur AD et exécuter en tant
qu'administrateur de domaine
```

Le script crée automatiquement :

- Un compte de service svc-teleport avec permissions minimales

- Une GPO "Block teleport-svc Interactive Login" (bloque les logins interactifs du compte)

- Une GPO "Teleport Access Policy" (importe le CA, configure le pare-feu, active RDP/RemoteFX)

Créer ensuite un compte utilisateur dédié à Teleport (tp-admin) via PowerShell :

```
New-ADUser `

    -Name "Teleport Admin" `

    -SamAccountName "tp-admin" `
```

```
    -AccountPassword (ConvertTo-SecureString "MotDePasseComplexe!" -
AsPlainText -Force) `
    -Enabled $true


Add-ADGroupMember -Identity "Remote Desktop Users" -Members "tp-admin"
Add-ADGroupMember -Identity "Domain Admins" -Members "tp-admin"
```

Générer un token windowsdesktop sur le serveur Teleport, puis compléter /etc/teleport.yaml :

```
tctl tokens add --type=windowsdesktop
echo "le_token" > /var/lib/teleport/token
chmod 600 /var/lib/teleport/token
# Ajouter dans /etc/teleport.yaml :
windows_desktop_service:
    enabled: true
    listen_addr: 0.0.0.0:3028
    ldap:
        addr: '192.168.10.1:636'
        domain: 'MySocVCt.fr'
        username: 'MYSOCVCT\svc-teleport'
        sid: 'S-1-5-21-XXXXXXXXX-XXXXXXXXX-XXXXXXXXX-XXXX'
        server_name: 'WAdDns01.MySocVCt.fr'
        insecure_skip_verify: false
    discovery_configs:
        - base_dn: "*"
```

Créer et appliquer le rôle d'accès aux desktops :

```
tctl create -f /tmp/windows-desktop-admins.yaml
tctl users update admin --set-roles "access,editor,windows-desktop-admins"
tctl get users/admin  # Vérification
```

Commandes de diagnostic

```
# Statut complet + info CA
sudo tctl status


# Valider la configuration
sudo teleport configure --test /etc/teleport.yaml
```

```
# Logs en direct
sudo journalctl -u teleport -f

# Nodes enregistrés
sudo tctl nodes ls

# Détails du certificat HTTPS
openssl s_client -connect teleport.domaine.local:443 2>/dev/null | openssl
x509 -noout -text

# Tester l'API avec la CA exportée
curl --cacert /tmp/teleport-ca.crt
https://teleport.domaine.local/v1/webapi/ping
```

Récapitulatif — Fichiers clés

Chemin	Rôle
/usr/local/bin/teleport	Binaire principal
/usr/local/bin/tctl	Outil d'administration CLI
/etc/teleport.yaml	Fichier de configuration principal
/etc/systemd/system/teleport.service	Unité systemd
/var/lib/teleport/	Données persistantes + clés
/var/lib/teleport/host_uuid	Identifiant unique du nœud
/var/log/teleport/	Logs applicatifs et audit
/etc/nftables.d/teleport.conf	Règles pare-feu

Récapitulatif — Commandes de gestion

Action	Commande

Démarrer Teleport	sudo systemctl start teleport
Recharger sans coupure	sudo systemctl reload teleport
Voir les logs	sudo journalctl -u teleport -f
Exporter la CA	sudo tctl auth export --type=tls > teleport-ca.crt
Ajouter un utilisateur	sudo tctl users add <nom> --roles=access --logins=<login>
Lister les nodes	sudo tctl nodes ls
Générer un token node	sudo tctl tokens add --type=node --ttl=2h
Statut + expiration CA	sudo tctl status
Rotation des CA	sudo tctl auth rotate --grace-period=48h

Rapport de tests

Les tests ont été réalisés au fil de la procédure, intégrés à chaque étape de l'installation.

Test	Commande / Méthode	Résultat attendu	Statut
Résolution DNS du FQDN	nslookup teleport.mysocvct.fr	IP du serveur Teleport retournée	OK
Synchronisation NTP	chronyc tracking	Synchro du temps correct	OK
Validation YAML	teleport configure --test /etc/teleport.yaml	Configuration looks good	OK
Accès HTTPS interface web	Navigateur sur https://teleport.mysocvct.fr	Page de login sans avertissement TLS	OK
Connexion client tsh	tsh login --proxy=teleport.mysocvct.fr	Session authentifiée avec OTP	OK
Enrôlement node Linux	tsh ls	Node visible dans la liste	OK
Session SSH enregistrée	tsh recordings ls après session SSH	Session apparaît dans les enregistrements	OK
Liste desktops Windows	tsh desktop ls	W11-ITAdmin visible	OK
Connexion RDP web	Interface web > Desktops > tp-admin@W11-ITAdmin	Session RDP ouverte dans le navigateur	OK
RBAC rôles utilisateur	tctl get users/admin	Rôles access,editor,windows-desktop-admins	OK

Rapport de déploiement

Le déploiement de Teleport s'est déroulé en deux étapes conformément au phasage prévu. La première phase a permis d'installer et de configurer le serveur Teleport sur la VM Debian 13, de signer le certificat HTTPS via l'AD CS interne et d'enrôler un premier node Linux avec enregistrement de sessions fonctionnel.

La seconde phase a couvert l'intégration Active Directory : exécution du script bootstrap PowerShell sur le serveur AD (création du compte svc-teleport, GPO Block Interactive Login, GPO Teleport Access Policy), configuration du Windows Desktop Service avec LDAPS, et création du compte tp-admin. La connexion RDP via l'interface web Teleport est opérationnelle sans installation de client sur les postes utilisateurs.

L'ensemble des tests du tableau précédent ont été validés avec succès.

Bilan

Conclusion :

Ce TP m'a permis de découvrir et de mettre en œuvre une solution PAM professionnelle, Teleport, dans un contexte d'infrastructure Active Directory. L'expérience a été enrichissante aussi bien sur le plan technique (PKI, LDAPS, RBAC, enregistrement de sessions) que conceptuel (approche Zero Trust, principe du moindre privilège). La comparaison avec Guacamole m'a permis de comprendre les différentes philosophies de solutions de bastion et de justifier le choix de Teleport pour ce contexte.

Auto-évaluation :

La partie la plus complexe a été la chaîne PKI : génération de la CSR, soumission à l'AD CS, conversion PEM et configuration dans teleport.yaml. Les erreurs TLS m'ont amené à approfondir ma compréhension des certificats X.509 et des SAN. L'intégration AD via LDAPS et le script bootstrap PowerShell se sont révélés plus intuitifs une fois la documentation Teleport bien assimilée. Je suis satisfait du résultat final : une infrastructure d'accès privilégié fonctionnelle, sécurisée et auditée.