

UNIVERSITÉ CHEIKH ANTA DIOP DE DAKAR

École Supérieure Polytechnique



ECOLE SUPERIEURE
POLYTECHNIQUE

Protocoles d'Accès et Services de Partage

Présenté par :

Salif BIAYE

Ndeye Astou DIAGOURAGA

Sous la direction de :

Dr Keba

Enseignant

Année universitaire 2024-2025

Table des Matières

Introduction

Kerberos et SSH

Introduction à Kerberos

Intégration avec SSH

Préparation du serveur et du client

Configuration du serveur SSH

Configuration du client SSH

Test de la connexion

Protocoles d'Accès Bureau à Distance

RD (Remote Desktop Protocol)

NoVNC

Samba avec LDAP et Kerberos

Introduction

Installation des paquets

Configuration de LDAP

Configuration de Kerberos pour Samba

Configuration de Samba

Ajout des utilisateurs Samba

Tests et validation

Services de Transfert de Fichiers

Conclusion

Introduction

Ce rapport présente l'implémentation de plusieurs protocoles d'accès et services de partage sécurisés dans un environnement d'entreprise. Dans un contexte de sécurité informatique en constante évolution, la mise en place de solutions d'authentification centralisées et de connexions distantes sécurisées est devenue indispensable.

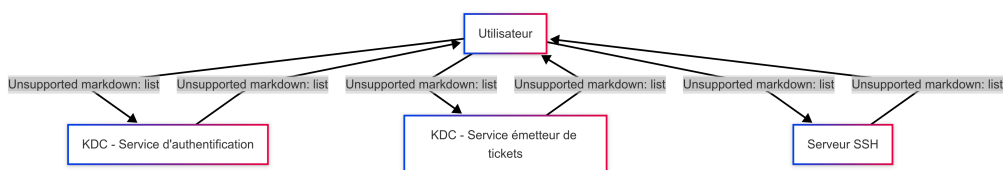
Nous aborderons l'intégration de Kerberos avec SSH pour l'authentification centralisée, les solutions d'accès bureau à distance avec RDP et NoVNC, la configuration de Samba avec LDAP et Kerberos, ainsi que les services de transfert de fichiers TFTP et SFTP.

L'objectif principal est de mettre en place une infrastructure sécurisée et efficace pour la gestion à distance des systèmes, en combinant des technologies complémentaires pour répondre aux besoins spécifiques de l'entreprise SmartTech.SN.

Kerberos et SSH

Introduction à Kerberos

L'intégration de Kerberos avec SSH permet d'optimiser la sécurité des connexions à distance sur des serveurs Linux/Unix en centralisant l'authentification des utilisateurs.



Intégration avec SSH

SSH (Secure Shell) est un protocole utilisé pour accéder à distance à des systèmes Unix/Linux de manière sécurisée. Lorsqu'il est couplé avec Kerberos, SSH bénéficie d'une authentification renforcée, permettant une gestion centralisée et simplifiée des identités et des accès.

Avantages du couplage Kerberos avec SSH

- **Authentification centralisée** : Les utilisateurs sont authentifiés via un serveur Kerberos, tel qu'un KDC (Key Distribution Center), permettant une gestion centralisée des identités.
- **Sécurité améliorée** : Kerberos utilise des tickets cryptographiques pour l'authentification, ce qui protège contre les attaques par interception de mot de passe.
- **Accès sans mot de passe** : Une fois l'utilisateur authentifié par Kerberos, il n'a pas à saisir son mot de passe à chaque connexion SSH, ce qui facilite l'accès sécurisé à plusieurs serveurs.

```
sudo apt-get install krb5-user libpam-krb5
```

Préparation du serveur et du client avec Kerberos

Pour configurer l'authentification Kerberos avec SSH, nous devons d'abord créer les principaux pour le serveur et le client, puis générer les clés Kerberos et ajouter les utilisateurs nécessaires dans la base de données Kerberos.

Création des principaux Kerberos

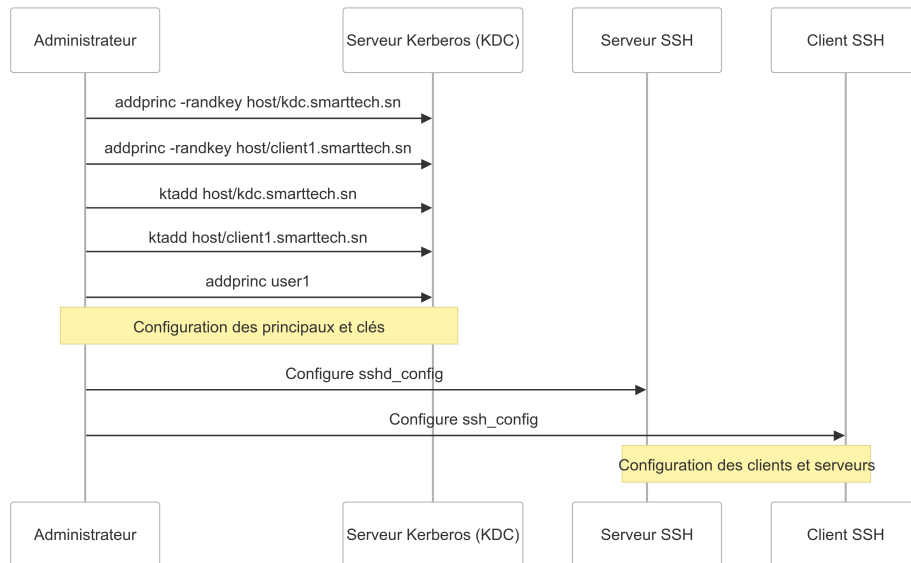
```
kadmin.local  
addprinc -randkey host/kdc.smarttech.sn  
addprinc -randkey host/client1.smarttech.sn
```

Génération des clés

```
ktadd host/kdc.smarttech.sn  
ktadd host/client1.smarttech.sn
```

Ajout d'un utilisateur

```
addprinc user1
```



Configuration du serveur SSH

Sur le serveur où SSH sera activé, nous devons configurer le fichier `sshd_config` pour activer l'authentification Kerberos.

```
# Éditer le fichier /etc/ssh/sshd_config
KerberosAuthentication yes
KerberosOrLocalPasswd yes
GSSAPIAuthentication yes
GSSAPICleanupCredentials yes
# Redémarrer le service SSH
systemctl restart sshd
```

Configuration du client SSH

Sur le client qui se connectera au serveur via SSH, nous devons configurer le fichier `ssh_config` pour activer l'authentification Kerberos.

```
# Éditer le fichier /etc/ssh/ssh_config
GSSAPIAuthentication yes
GSSAPIDelegateCredentials yes
```

Test de la connexion

Pour tester la connexion, nous devons d'abord obtenir un ticket Kerberos, puis utiliser ce ticket pour nous connecter au serveur SSH sans mot de passe.

```
# Obtenir un ticket Kerberos
kinit user1@SMARTTECH.SN
# Vérifier le ticket
klist
# Se connecter au serveur SSH
ssh kdc.smarttech.sn
```

Exemple de sortie réussie :

```
user1@client:~$ ssh kdc.smarttech.sn
The authenticity of host 'kdc.smarttech.sn (192.168.1.211)' can't be established.
ECDSA key fingerprint is SHA256:xCY1GIIrNHrF7DrDCg9gleHB/GenH3PqyGwtm5WiVxZg.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'kdc.smarttech.sn,192.168.1.211' (ECDSA) to the list of
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-130-generic x86_64)
[...Informations système...]
user1@kdc:~$ pwd
/home/user1
```

Protocoles d'Accès Bureau à Distance

RDP (Remote Desktop Protocol)

RDP est un protocole développé par Microsoft pour accéder à un bureau Windows à distance. Contrairement à SSH, qui est généralement utilisé pour une interface en ligne de commande, RDP permet une interaction graphique avec l'interface de l'ordinateur distant.

Caractéristiques principales de RDP

- **Accessibilité graphique** : Permet l'accès complet à l'interface graphique du système distant.
- **Contrôle à distance sécurisé** : RDP utilise des mécanismes de chiffrement pour sécuriser la communication entre le client et le serveur.

- **Utilisation dans des environnements Windows** : RDP est principalement utilisé dans des environnements Windows, mais des clients RDP existent pour d'autres systèmes d'exploitation.

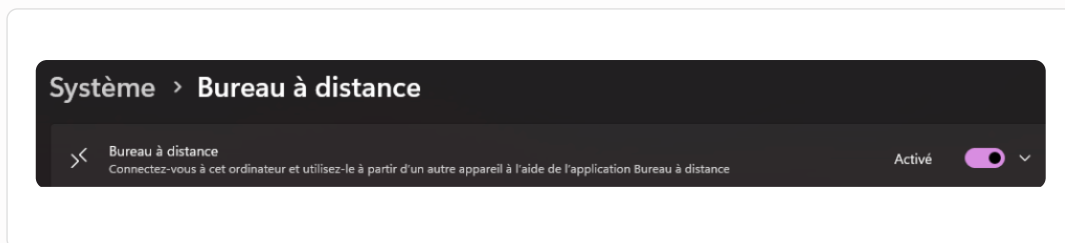
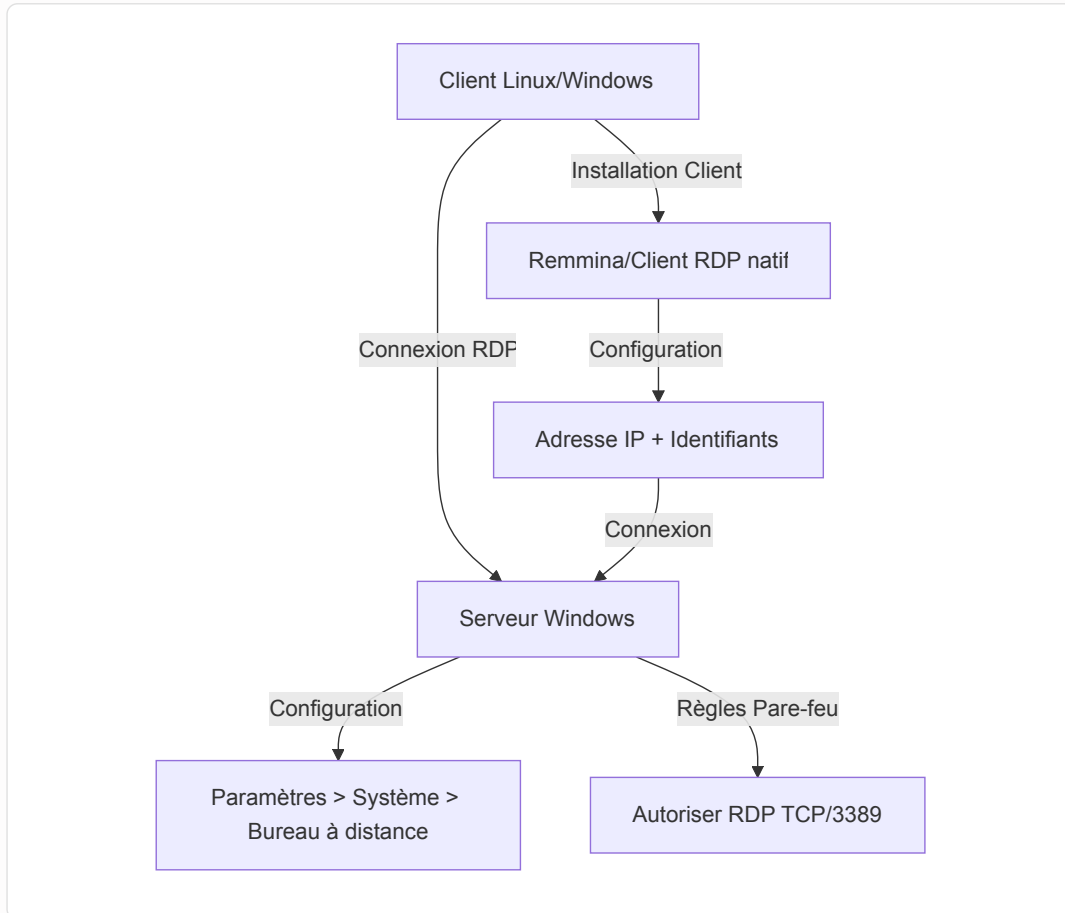
Configuration de RDP

Prérequis :

- Une machine Windows (version Pro, Enterprise, ou Education) pour servir de serveur RDP.
- Une machine Windows ou Linux pour agir comme client RDP.
- Accès administrateur sur la machine serveur.

Activer le Bureau à Distance sur le Serveur Windows


Paramètres > Système > Bureau à distance



on crée d'abord un utilisateur sur notre serveur Windows

Propriétés de : anta

Général Membre de Profil

 anta

Nom complet :

Description :

☐ L'utilisateur doit changer le mot de passe à la prochaine ouverture de session

☐ L'utilisateur ne peut pas changer de mot de passe

☒ Le mot de passe n'expire jamais

☐ Le compte est désactivé

☐ Le compte est verrouillé

OK Annuler Appliquer Aide

Sélectionnez des utilisateurs

Sélectionnez le type de cet objet :

Types d'objets...

À partir de cet emplacement :

Emplacements...

Entrez les noms des objets à sélectionner (exemples) :

Vérifier les noms

Avancé... OK Annuler

On va autoriser le bureau a distance au niveau des règles de parefeu.

Panneau de configuration > Système et sécurité > Pare-feu Windows Defender > Applications autorisées

Autoriser les applications à communiquer à travers le Pare-feu Windows Defender

Pour ajouter, modifier ou supprimer des applications et des ports autorisés, cliquez sur Modifier les paramètres.

Quels sont les risques si une application est autorisée à communiquer ?

 Modifier les paramètres

Applications et fonctionnalités autorisées :

Nom	Privé	Public
<input type="checkbox"/> BranchCache - Découverte d'homologue (utilise WSD)	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> BranchCache - Extraction du contenu (utilise HTTP)	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> BranchCache - Serveur de cache hébergé (utilise HTTPS)	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Bureau à distance	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Bureau à distance (WebSocket)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Calculatrice Windows	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Caméra Windows	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Cartes Windows	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Centre de configuration des graphiques Intel®	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> ceup.exe	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Compte professionnel ou scolaire	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Contacts Microsoft	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Détails...

Supprimer

Une fois ceci fait, les clients VNC sur Windows ou Linux peuvent se connecter. on va tester

avec un client linux

Configuration du client Linux

```
# Installation de Remmina
sudo apt update
sudo apt install remmina remmina-plugin-rdp
```

Lancer Remmina, créer une nouvelle connexion avec l'adresse du serveur et les identifiants d'un utilisateur autorisé.


Remote Connection Profile

Name

Quick Connect

Group

Protocol

 RDP - Remote Desktop Protocol

Basic

Advanced

Behavior

SSH Tunnel

Notes

Server

192.168.1.200

Username

anta

Password

Domain

Share folder

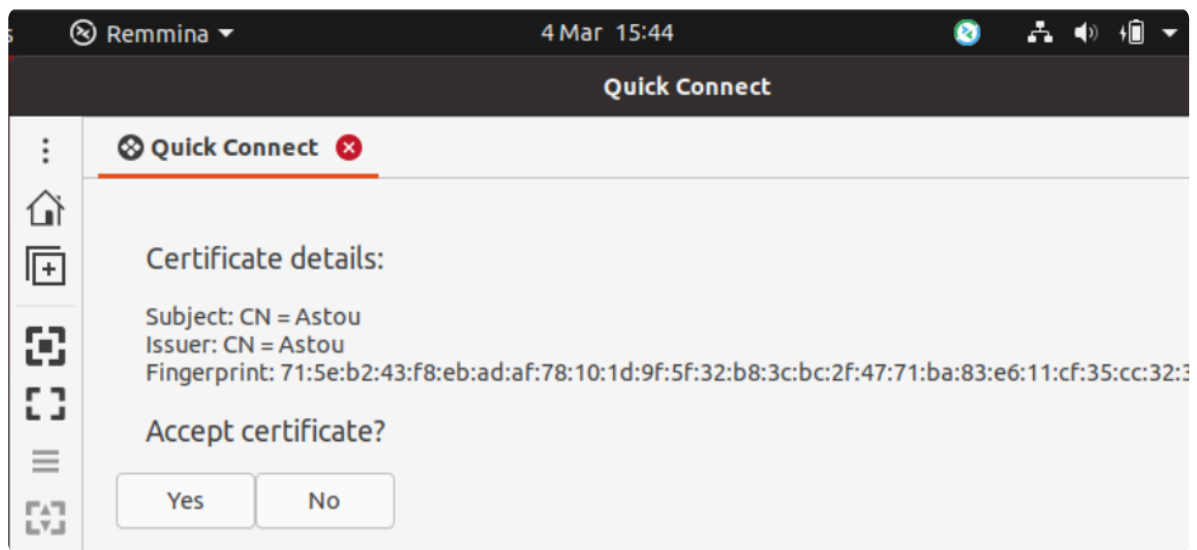
☐ (None)

☐ Restricted admin mode

Password hash

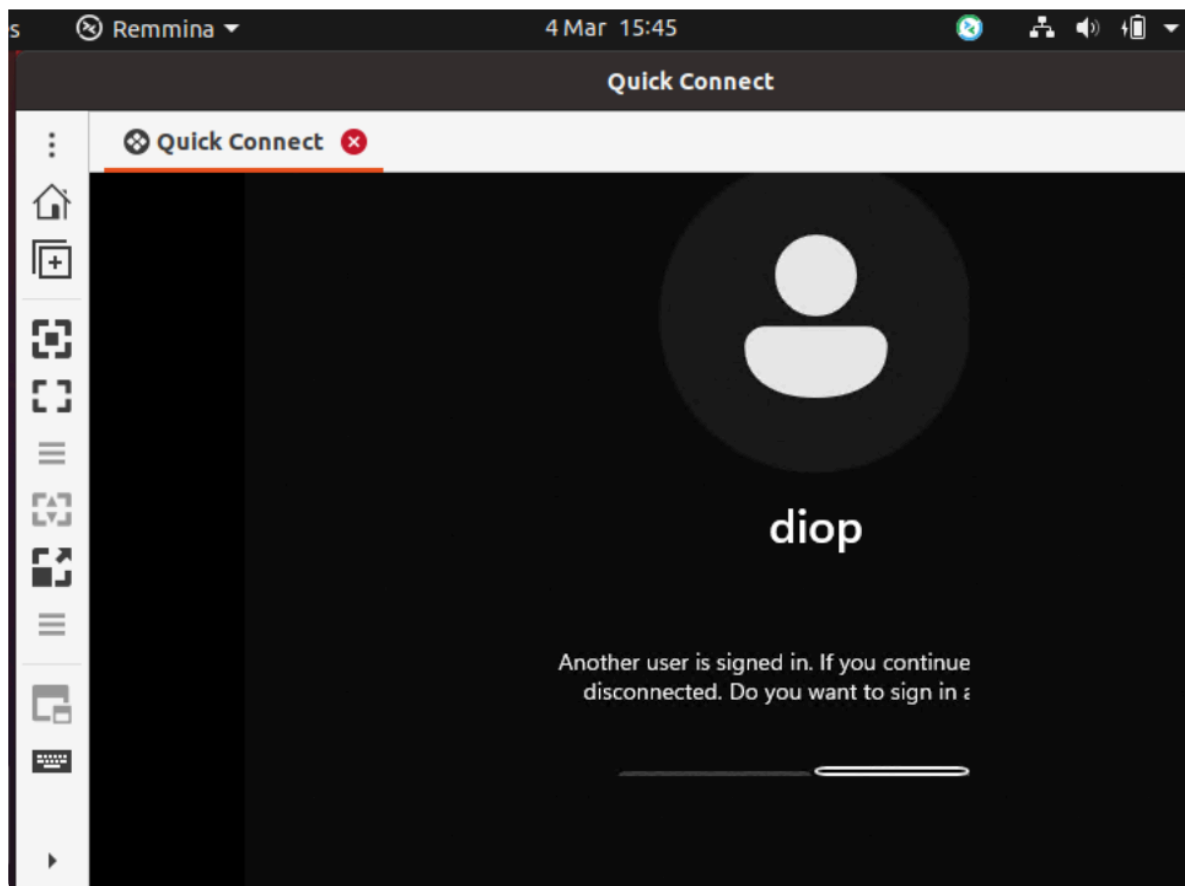
☐ Left-handed mouse support

☐ Disable smooth scrolling



On renseigne l'adresse du serveur distant ainsi que l'utilisateur qui est autorisé à accéder au bureau à distance et son mdp

 [Testons la connexion](#)



On peut ainsi accéder à distance à la machine serveuse via RDP.

D'un autre côté, [RDP](#) et [NoVNC](#) sont des solutions très utiles pour accéder à des bureaux distants dans des environnements Windows ou via un navigateur. RDP est adapté aux environnements Windows, tandis que NoVNC fournit une solution multiplateforme et accessible via un simple navigateur web.

NoVNC

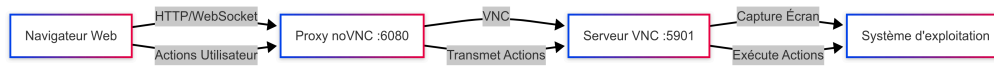
NoVNC est une implémentation du protocole VNC (Virtual Network Computing) qui permet d'accéder à un bureau distant via un navigateur web. Il fonctionne en utilisant le protocole WebSockets et permet de contrôler un ordinateur à distance en utilisant un client HTML5.

Caractéristiques principales de NoVNC

- [Accès via navigateur](#) : Permet d'accéder à un bureau distant sans installer de logiciel client, simplement via un navigateur web.
- [Compatibilité multiplateforme](#) : Étant basé sur HTML5, NoVNC fonctionne sur tous les systèmes d'exploitation modernes sans nécessiter de plugins.
- [Utilisation pour la gestion des serveurs virtuels](#) : NoVNC est souvent utilisé pour gérer des environnements de serveurs virtuels, notamment dans les infrastructures cloud.

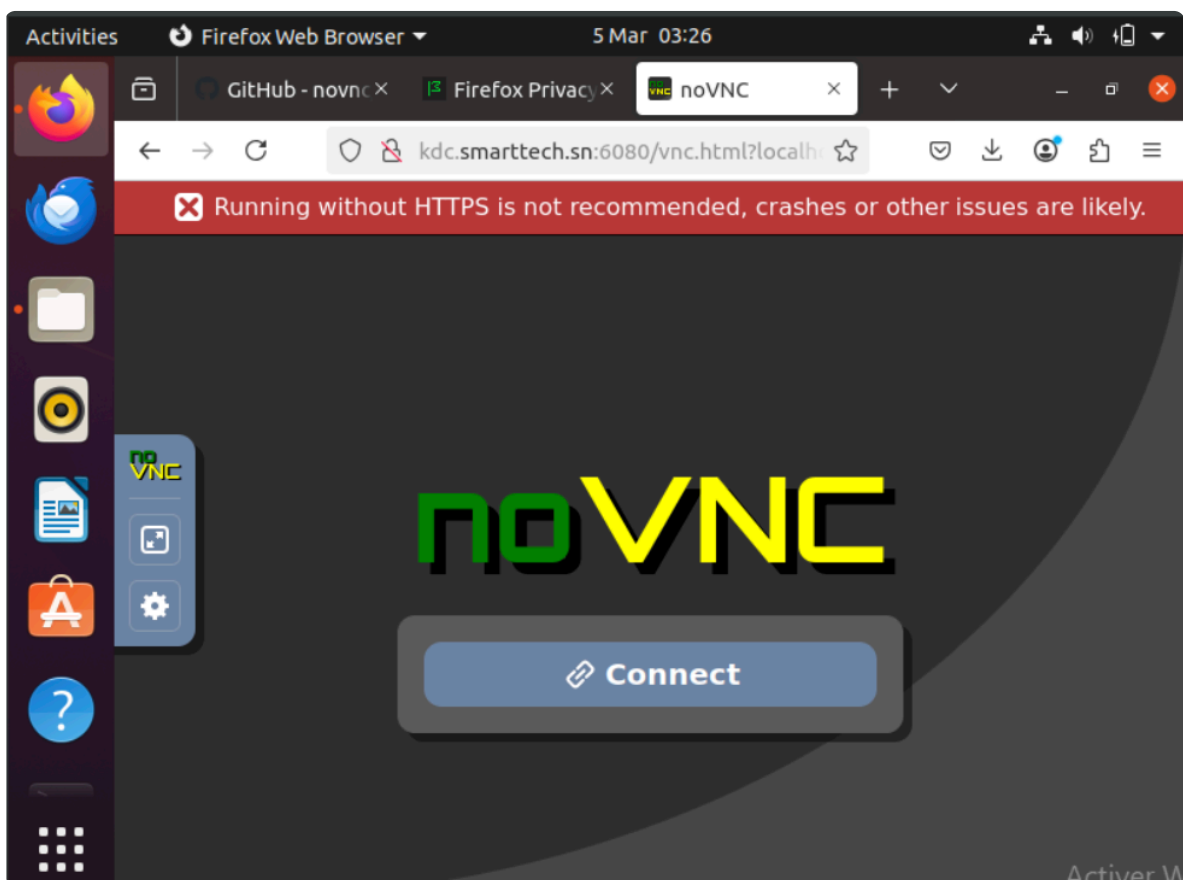
Installation et configuration

```
# Installation du serveur VNC
apt install tigervnc-server-standalone -y
# Clonage de noVNC
git clone https://github.com/novnc/novnc.git ~/novnc
# Création d'un lien symbolique
ln -s ~/novnc/utils/novnc_proxy /usr/local/bin/novnc_proxy
# Démarrage du proxy WebSocket
novnc_proxy --vnc localhost:5901 --listen 6080
```



Interface graphique

Lorsqu'on tape l'url au niveau de notre machine cliente on obtient:



noVNC va permettre à notre entreprise d'accéder aux interfaces graphiques des serveurs à distance via un simple navigateur, sans nécessiter de client VNC dédié. Cette solution a amélioré la flexibilité et la sécurité des connexions tout en simplifiant

la gestion des accès pour les utilisateurs. Son intégration a donc optimisé notre infrastructure en facilitant l'administration à distance et en réduisant les contraintes techniques.

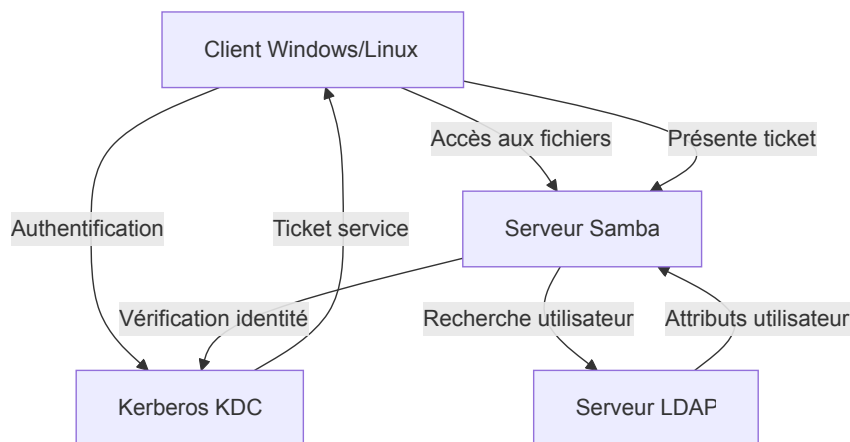
En combinant [Kerberos avec SSH](#) pour l'authentification centralisée et en utilisant [RDP](#) ou [NoVNC](#) pour l'accès graphique, on peut créer une infrastructure sécurisée et efficace pour la gestion à distance des systèmes.

Samba avec LDAP et Kerberos

Introduction

L'objectif de cette section est d'intégrer Samba avec LDAP et Kerberos sur SMART TECH.SN. Cette configuration permet :

- D'utiliser LDAP pour centraliser les comptes utilisateurs.
- D'utiliser Kerberos pour l'authentification sécurisée.
- D'autoriser l'accès aux partages Samba sans entrer de mot de passe grâce à Kerberos.



Installation des paquets

```
sudo apt install samba smbclient krb5-user winbind  
libnss-winbind libpam-winbind smbldap-tools schema2ldif -y
```

Configuration de LDAP

Ajout du schéma Samba à LDAP

```
# Localiser le schéma Samba
locate samba.schema
# Copier et convertir en LDIF
cp /usr/share/doc/samba/examples/LDAP/samba.schema /etc/ldap/schema/
schema2ldif /etc/ldap/schema/samba.schema > samba.ldif
# Ajout du fichier schema.ldif
sudo ldapadd -Y EXTERNAL -H ldapi:/// -f samba.ldif
# Vérification
ldapsearch -LLL -Y EXTERNAL -H ldapi:/// -b cn=schema,cn=config | grep samba
```

Configuration de Kerberos pour Samba

Fichier de configuration

```
# Éditer /etc/krb5.conf
[libdefaults]
default_realm = SMARTTECH.SN
[realms]
SMARTTECH.SN = {
    kdc = kdc.smarttech.sn
    admin_server = kdc.smarttech.sn
}
```

Création des utilisateurs

```
# Ajouter le principal salif
sudo kadmin.local addprinc salif@SMARTTECH.SN
# Ajouter le service Samba
addprinc -randkey cifs/server.smarttech.sn@SMARTTECH.SN
ktadd -k /etc/krb5.keytab cifs/server.smarttech.sn@SMARTTECH.SN
```

Configuration de Samba

Modification de /etc/samba/smb.conf

```
[global]
workgroup = SMARTTECH
security = user
realm = SMARTTECH.SN
encrypt passwords = yes
passdb backend = ldapsam:ldap://server.smarttech.sn
ldap admin dn = cn=admin,dc=smarttech,dc=sn
ldap suffix = dc=smarttech,dc=sn
ldap user suffix = ou=users
ldap group suffix = ou=groups
ldap machine suffix = ou=computers
ldap ssl = no
kerberos method = system keytab
dedicated keytab file = /etc/krb5.keytab
[partage]
path = /srv/samba/share
read only = no
browseable = yes
guest ok = no
```

Création du répertoire de partage

```
sudo mkdir -p /srv/samba/share
sudo addgroup smbusers
sudo chown -R root:smbusers /srv/samba/share
sudo chmod -R 2770 /srv/samba/share
```

Ajout des utilisateurs Samba

```
# Ajout d'un utilisateur Samba
sudo smbpasswd -a salif
# Vérification des utilisateurs Samba
pdbedit -Lv
```

Remarque : Avant ces commandes, l'utilisateur salif doit obligatoirement exister dans l'annuaire LDAP et dans le système (adduser). La commande smbpasswd ajoute seulement les attributs Samba dans l'annuaire.


```
root@kdc: /home/server

-----
Unix username:      salif
NT username:
Account Flags:      [U                ]
User SID:           S-1-5-21-1320290922-3887964779-207989209-1001
Primary Group SID:  S-1-5-21-1320290922-3887964779-207989209-513
Full Name:
Home Directory:     \\KDC\salif
HomeDir Drive:
Logon Script:
Profile Path:       \\KDC\salif\profile
Domain:             KDC
Account desc:
Workstations:
Munged dial:
Logon time:         0
Logoff time:        Wed, 06 Feb 2036 15:06:39 GMT
Kickoff time:       Wed, 06 Feb 2036 15:06:39 GMT
Password last set:  Wed, 05 Mar 2025 01:30:48 GMT
Password can change: Wed, 05 Mar 2025 01:30:48 GMT
Password must change: never
Last bad password   : 0
Bad password count  : 0
Logon hours        : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
root@kdc: /home/server#
```

Tests et validation

Redémarrage des services

```
sudo systemctl restart smbd nmbd krb5-kdc krb5-admin-server slapd winbind
```

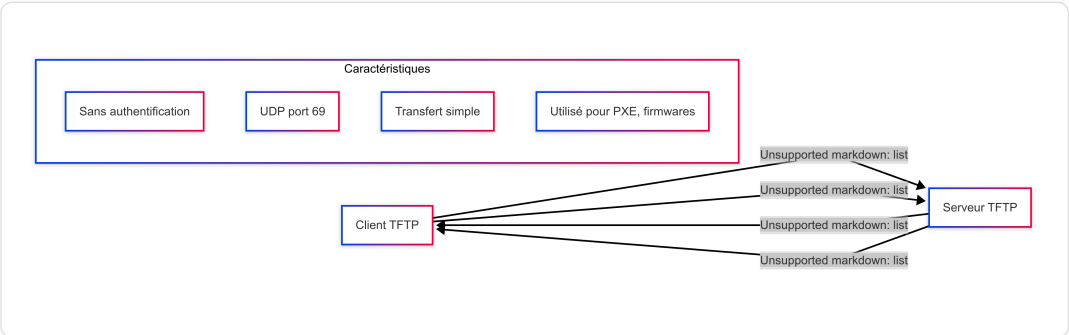
Connexion sans mot de passe via Kerberos

```
kinit salif@SMARTTECH.SN
smbclient -k -L //kdc.smarttech.sn
smbclient -k //kdc.smarttech.sn/partage
# Vérification du partage Samba
smb: > ls
```

Services de Transfert de Fichiers

TFTP (Trivial File Transfer Protocol)

Le Trivial File Transfer Protocol (**TFTP**) est un protocole de transfert de fichiers léger, principalement utilisé pour des opérations où l'authentification et les fonctionnalités avancées de gestion de fichiers ne sont pas nécessaires. Il est couramment utilisé pour le déploiement de systèmes d'exploitation via **PXE**, la mise à jour de firmwares, ainsi que le transfert de configurations d'équipements réseau (routeurs, switches, etc.). Ce rapport présente l'installation, la configuration et l'utilisation d'un serveur TFTP dans un environnement Linux et Windows.



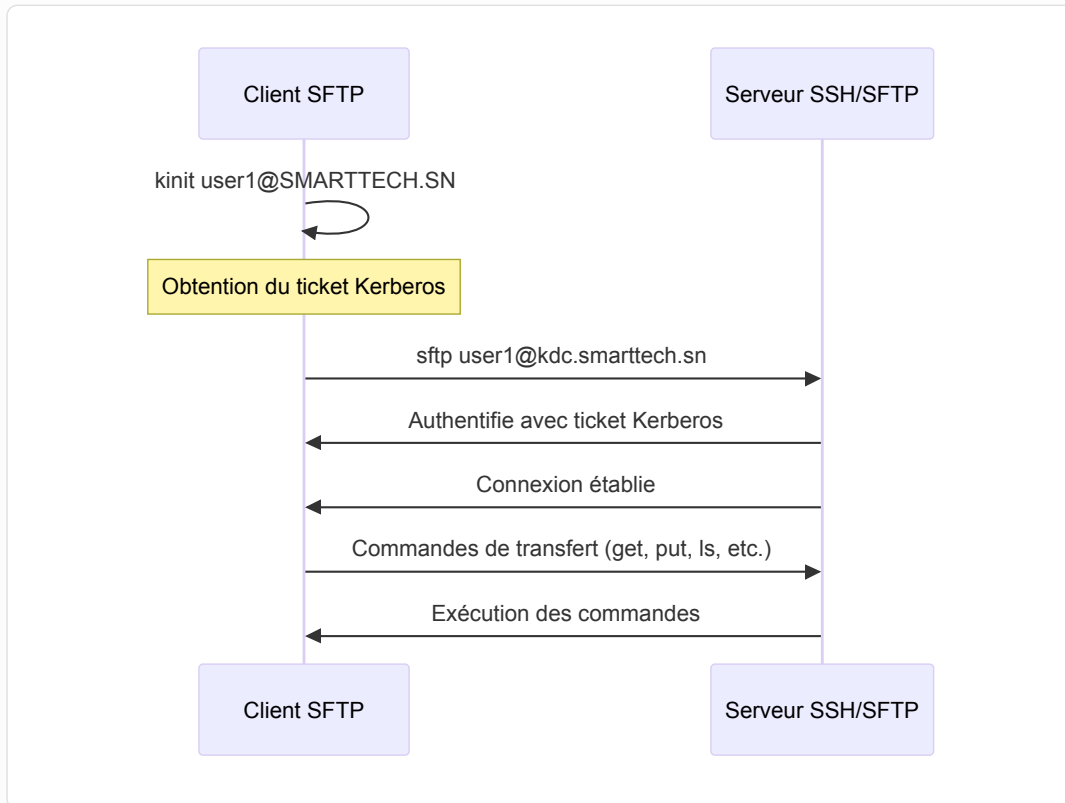
Installation d'un serveur TFTP sous Linux

```
# Installation du service TFTP
sudo apt update && sudo apt install tftpd-hpa -y
# Configuration du serveur TFTP
sudo nano /etc/default/tftpd-hpa
# Contenu:
TFTP_USERNAME="tftp"
TFTP_DIRECTORY="/srv/tftp"
TFTP_ADDRESS="0.0.0.0:69"
TFTP_OPTIONS="--secure"
# Création du répertoire de stockage
sudo mkdir -p /srv/tftp
sudo chmod -R 777 /srv/tftp
sudo chown -R tftp:tftp /srv/tftp
# Démarrage et activation du serveur
sudo systemctl restart tftpd-hpa
sudo systemctl enable tftpd-hpa
```

Pour des raisons de sécurité, nous préférons utiliser SFTP pour assurer un transfert de fichiers sécurisé.

SFTP (SSH File Transfer Protocol)

SFTP est un protocole de transfert de fichiers qui utilise SSH pour sécuriser les communications. Il est déjà configuré si SSH est configuré sur le système.



Test de connexion SFTP

```
# Obtenir un ticket Kerberos
kinit user1
# Se connecter via SFTP
sftp user1@kdc.smarttech.sn
# Exemple de sortie:
user1@kdc:/home/server$ sftp user1@kdc.smarttech.sn
Connected to kdc.smarttech.sn.
sftp> ls -l
drwx----- 3 user1 user1 4096 Mar 3 13:04 snap
sftp>
```

En activant SFTP, nous garantissons des transferts de fichiers sécurisés grâce à l'utilisation du chiffrement SSH, ainsi qu'un meilleur contrôle d'accès et une traçabilité des actions des utilisateurs. Cette solution est bien plus adaptée aux environnements nécessitant une protection renforcée des données.

Conclusion

Ce rapport a présenté l'implémentation de plusieurs technologies d'accès et de partage sécurisés au sein de l'environnement SmartTech.SN :

- **Kerberos avec SSH** : Cette intégration permet une authentification centralisée et une connexion sans mot de passe, améliorant à la fois la sécurité et l'expérience utilisateur.

- **RDP et NoVNC** : Ces protocoles offrent un accès graphique à distance adapté à différents scénarios, avec RDP pour les environnements Windows et NoVNC pour une solution multiplateforme accessible via navigateur.
- **Samba avec LDAP et Kerberos** : Cette configuration permet de centraliser la gestion des utilisateurs et de sécuriser les partages de fichiers, tout en offrant une intégration transparente avec les environnements Windows.
- **SFTP** : Ce protocole sécurisé remplace avantageusement TFTP pour les transferts de fichiers, grâce à l'utilisation du chiffrement SSH.

En combinant ces technologies, nous avons créé une infrastructure sécurisée et efficace pour la gestion à distance des systèmes. Cette architecture répond aux besoins de sécurité, de simplicité d'administration et d'expérience utilisateur, tout en assurant une traçabilité des actions et une protection des données.

