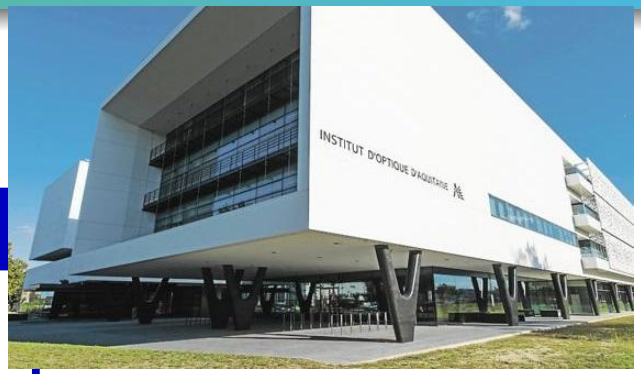
Mise en place de SAMBA-AD comme alternative à MS-AD

Philippe Hortolland - Séminaire RAISIN

3 octobre 2024

Présentation du laboratoire LP2N et contexte informatique



Fiche du laboratoire et missions du SI :

- Thématique de recherche : photonique et nanoscience
- Rattachement aux tutelles : Institut d'Optique - CNRS - Université de Bordeaux
- Ma mission : mettre en place l'architecture technique du système d'information
- Infrastructure mise à disposition :
  1 hyperviseur ProxMox + 1 Réseau géré par l'IOGS
- Objectif : Mettre en place une solution pour centraliser les comptes informatiques LP2N

Quelles solutions pour la centralisation des comptes

L'importance de la centralisation des comptes informatiques

- Sécurité renforcée de postes : La centralisation permet une gestion unifiée des accès, réduisant ainsi le risque de failles de sécurité et facilitant l'application de politiques de sécurité.
- Gestion simplifiée des comptes : Les administrateurs peuvent gérer les utilisateurs, les droits d'accès et les autorisations de manière centralisée.
- Conformité réglementaire : Une gestion centralisée des comptes aide à maintenir la conformité avec les réglementations en matière de protection des données et de cybersécurité.
- Audit et traçabilité : Il est plus facile de suivre l'activité des utilisateurs et de générer des rapports pour détecter d'éventuelles anomalies ou activités suspectes.

Quelles solutions pour la centralisation des comptes

- OpenLDAP : Une solution open-source qui implémente le protocole LDAP, largement utilisée pour la gestion des annuaires dans les environnements Linux, compatible avec les autres systèmes.
- **Samba 4** : Fournit une alternative open-source à Active Directory, permettant une intégration transparente avec les environnements Windows.
- MS AD : L'AD est l'approche préconisée par Microsoft pour gérer la sécurité d'un parc Windows ; ceci peut également représenter un point de faiblesse en cas de mauvaise gestion.
- MS AD Server Core

Quelles solutions pour la centralisation des comptes

Pourquoi Samba 4 ?

- Meilleur compromis dans un contexte hétérogène - interopérabilité.
- Coût du produit (vs licences des serveurs MS, licences CAL).
- Recommandé pour la sécurité des SI, compatible avec les points d'exigences de l'ANSSI - cf. Josy Active Directory, discours du RSSI CNRS.
- Simplicité de la mise en œuvre : De nombreux sites proposent des tutos pour l'installation.
  - Ex : LCC Toulouse, Jérôme Colombet *https ://homepages.lcc-toulouse.fr/colombet/samba-deployer-une-infrastructure-active-directory/*
  - Ex : Site Tranqu'il IT mise à jour régulièrement ses docs *https ://samba.tranquil.it/doc/fr*
- Installation rapide.

Fiche technique du produit SAMBA

Samba (informatique)

35 langues

Article | Discussion | Lire | Modifier | Modifier le code | Voir l'historique | Outils

Pour les articles homonymes, voir Samba.

Sommaire masquer

- Début
- Historique
- Fonctionnalités
- Interopérabilité
- Samba en Workgroup
- Samba PDC NT4
- Samba Active Directory
  - Heimdal Kerberos vs MIT Kerberos
  - Samba et OpenLDAP
- Samba 4
  - Nouveautés
- Principales versions[22]
- Liens externes
- Notes et références

Samba est un logiciel d'interopérabilité qui implémente le protocole propriétaire SMB/CIFS de Microsoft Windows (plus souvent connu sous le sigle SMB) dans les ordinateurs tournant sous le système d'exploitation Unix et ses dérivés de manière à partager des imprimantes et des fichiers dans un réseau informatique[3]. Samba facilite l'interopérabilité entre systèmes hétérogènes Windows-Unix. Il offre la possibilité aux ordinateurs d'un réseau d'accéder aux imprimantes et aux fichiers des ordinateurs sous Unix[4] et permettent aux serveurs Unix de se substituer à des serveurs Windows[5].

Il s'agit d'une réimplémentation des protocoles SMB/CIFS sous GNU/Linux et d'autres variantes d'Unix par ingénierie inverse. Samba a été initialement développée par l'Australien Andrew Tridgell et distribuée sous licence libre GNU GPL 3[6]. Son nom provient du nom du protocole standard de Microsoft, SMB (Server Message Block), auquel ont été ajoutées les deux voyelles *a* : « SaMBa ».

À partir de la version 3, Samba fournit des fichiers et services d'impression pour divers clients Windows et peut s'intégrer à un domaine Active Directory en tant que membre du domaine. Samba3 peut aussi être configuré en tant que PDC (Primary Domain Controller (en)) en mode domaine NT4.

À partir de la version 4, Samba peut servir de contrôleur de domaine Active Directory et fournir les services d'authentification AD à des postes Windows, des postes Linux et des serveurs membres.

Samba

SAMBA

Informations

Développé par	The Samba Team
Première version	1992[1]
Dernière version	4.21.0 (2 septembre 2024)[2]
Dépôt	git.samba.org
Écrit en	C, C++ et Python
Système d'exploitation	Linux, OpenVMS, macOS et type Unix
Environnement	Multiplateforme
Type	Système de fichiers distribué
Licence	GNU GPL 3
Documentation	wiki.samba.org/index.php/User_Documentation et www.samba.gr.jp/project/translation/current/htmldocs/manpages/index.html
Site web	www.samba.org

modifier - modifier le code - voir Wikidata (aide)

WIKIPÉDIA L'encyclopédie libre

RAISIN

Installation de la solution Samba AD - 2 Etapes (1/2)

Préparation

- Préparation et dimensionnement :
  2 machines virtuelles Proxmox. Pour une mise en production, un minimum de 4 Go de RAM et un espace disque de 10 Go sont généralement suffisants pour des domaines contenant plusieurs centaines d'utilisateurs.
- Installation de 2 serveurs fonctionnant sous Linux Debian 12.
- Précautions à prendre : Chiffrer les VM (LUKS).
- Installation d'OpenSSH pour faciliter l'interaction avec le serveur.
- Lien vers le tuto d'installation de Tranqu'il IT :
  https ://samba.tranquil.it/doc/fr.

Memory	4.00 GiB
Processors	4 (2 sockets, 2 cores)
BIOS	Default (SeaBIOS)
Display	Default
Machine	Default (i440fx)
SCSI Controller	VirtIO SCSI
CD/DVD Drive (ide2)	local:iso/debian-12.4.0-amd64-DVD-1.iso,media=cdrom,size=3900480K
Hard Disk (scsi0)	local-lvm:vm-202-disk-0,size=20G
Network Device (net0)	virtio=BC:24:11:C0:D4:55,bridge=vmbr0

Installation de la solution Samba AD - 2 Etapes (1/2)

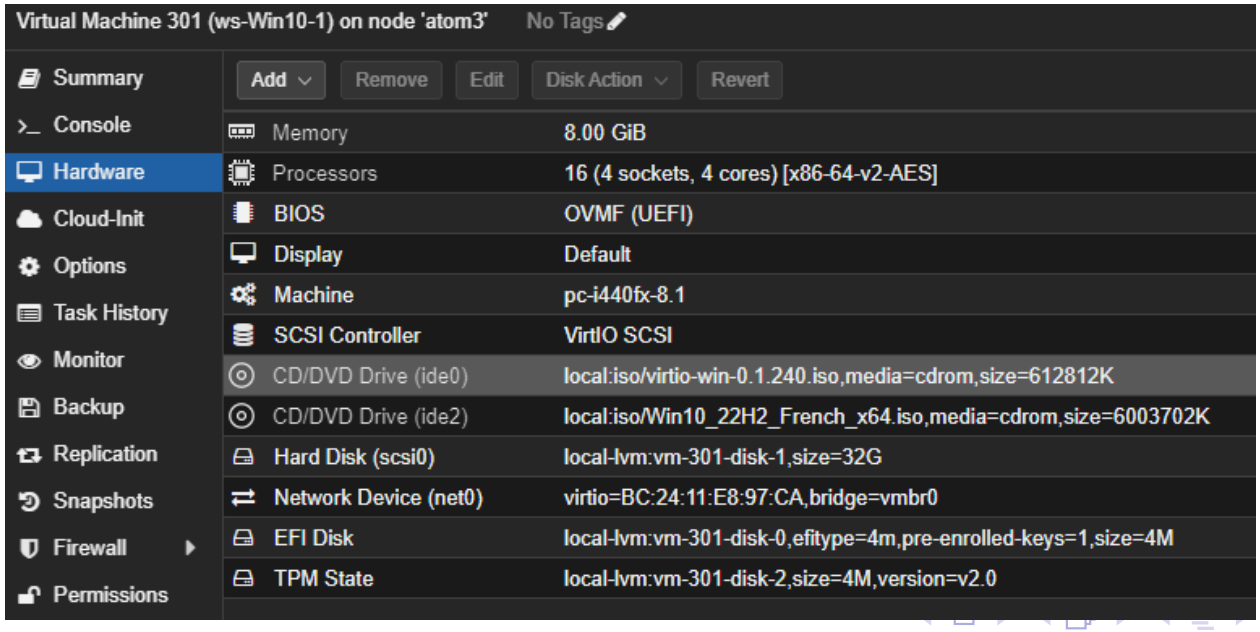
Phases d'installation côté serveur (source : Tranqu'il IT)

- Préparer votre machine Debian (nom, configuration réseau).
- Installer et configurer Samba-AD sur Debian (krb5.conf, smb.conf).
- Installer et configurer NTP pour Samba-AD sur Debian.
- Installer et configurer Bind-DLZ pour Samba-AD : Samba-AD vient par défaut avec son propre serveur DNS (winbind), mais il est recommandé d'utiliser Bind-DLZ.
- Installer et configurer un Samba-AD secondaire sur Debian.
- Installer et configurer Samba-AD RODC sur Debian.

Installation de la solution Samba AD - 2 Etapes (2/2)

Installation

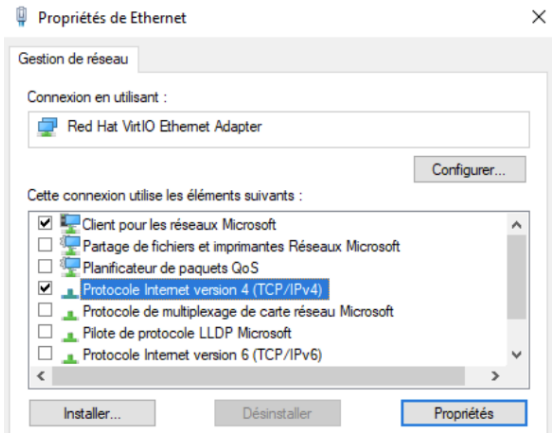
- Installation d'une VM Windows 10 : caractéristiques de la VM, dimensionnement et image.
- Attention à bien monter l'image ISO de la solution Windows VirtIO Drivers.
- Avantage : Poste exclusivement dédié à l'administration de l'AD.
- C'est une recommandation forte pour sécuriser son système d'information.

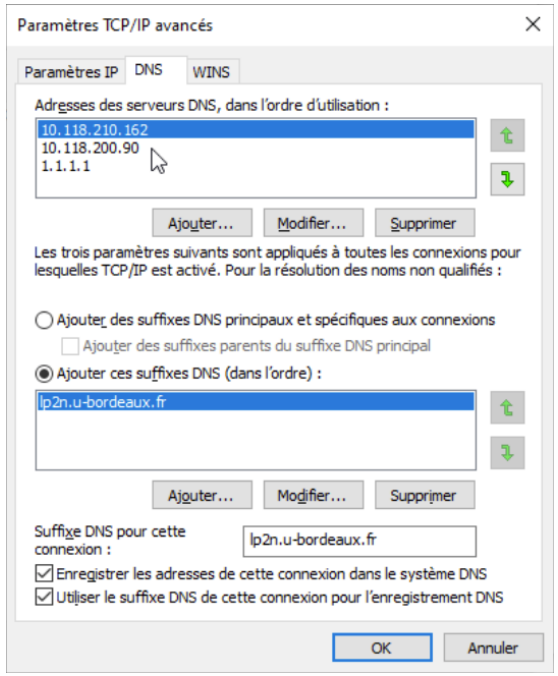


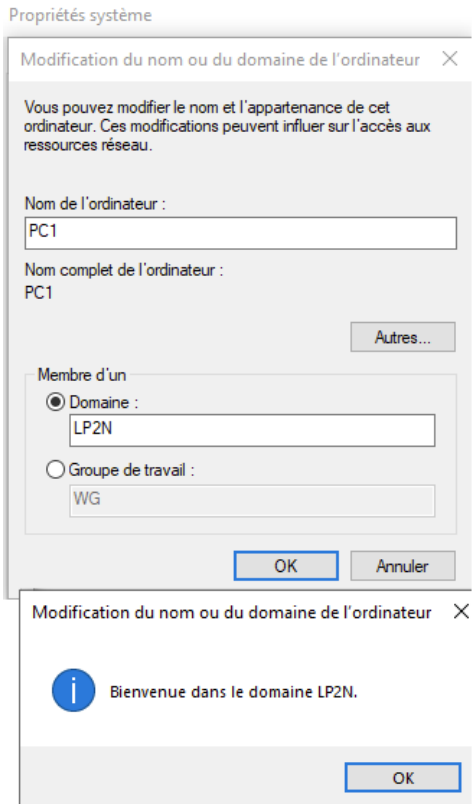
Installation de la solution Samba AD - 2 Etapes (2/2)

Phases d'installation côté console

- Configurer la VM Windows (nom, configuration réseau, DNS).
- Joindre le poste Windows au domaine nouvellement créé.
- Vérifier l'accès aux dossiers partagés SYSVOL du serveur.

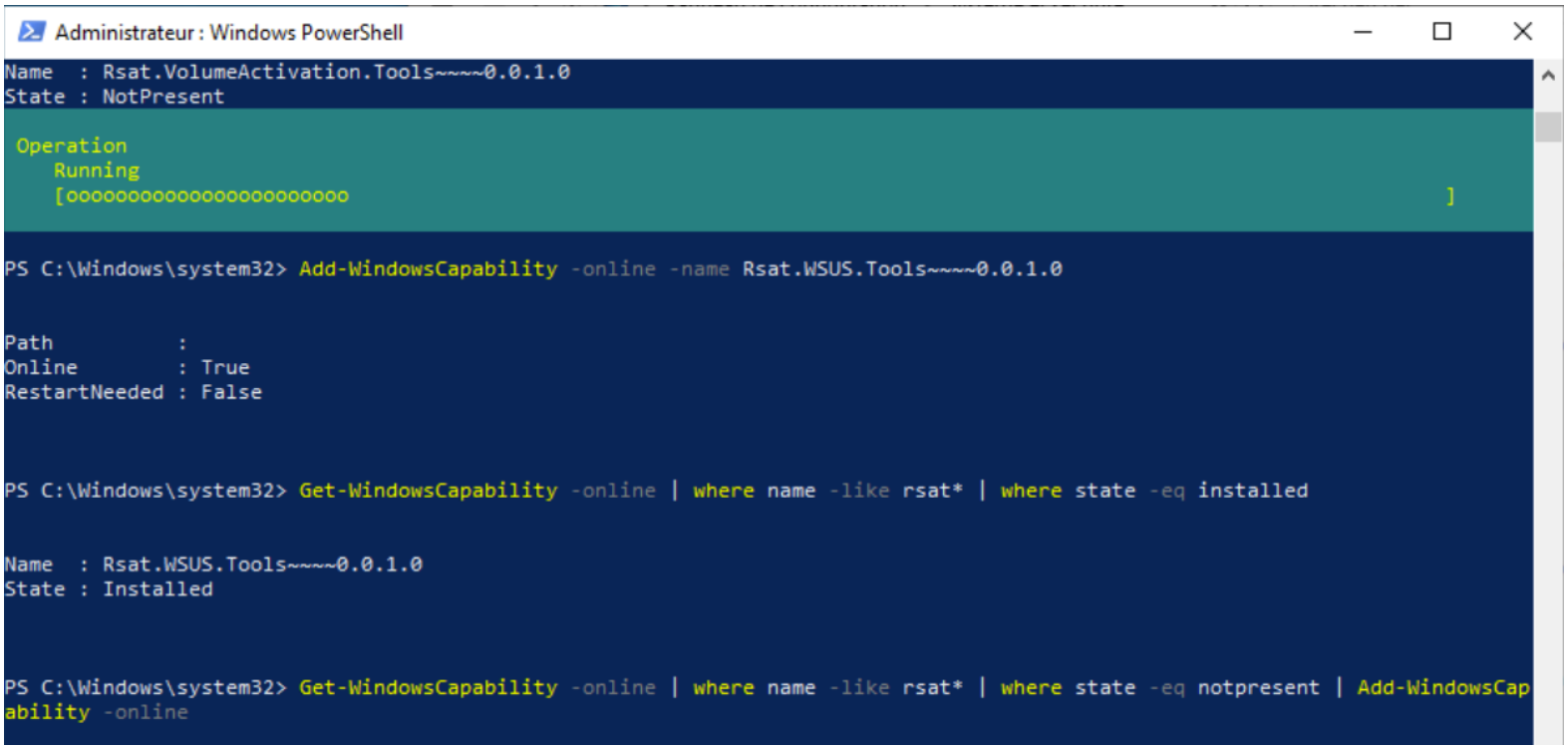






Installation des outils d'administration RSAT

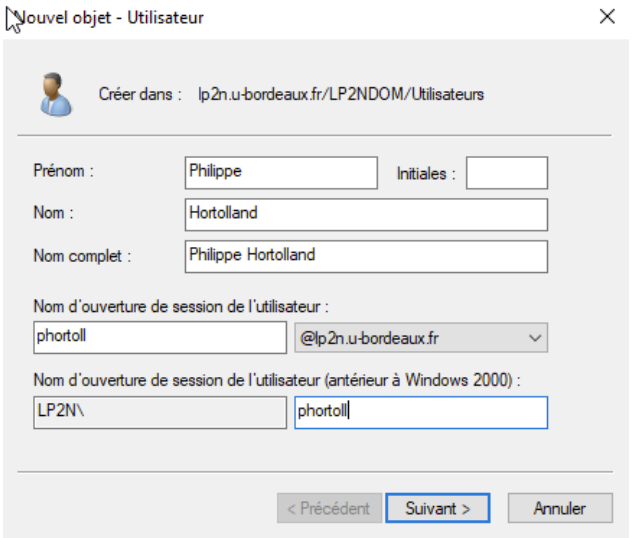
- Voici deux méthodes d'installation des outils RSAT :
- Vous pouvez télécharger directement le fichier WindowsTH-KB2693643-x64.msu à partir du lien suivant : `https://www.microsoft.com/en-us/download/details.aspx?id=45520`
- L'autre solution consiste à utiliser la ligne de commande PowerShell. Par exemple : Get-WindowsCapability -Online -Name RSAT*

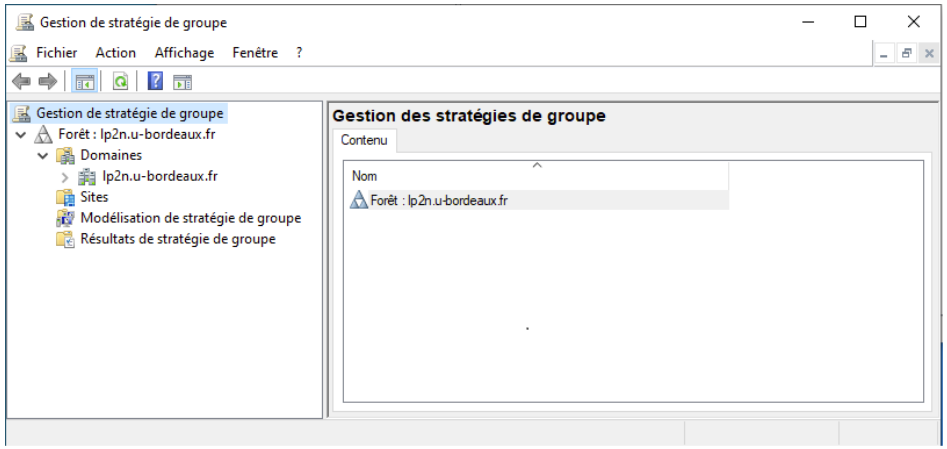


Présentation des outils d'administration RSAT

Les outils d'administration Service d'annuaire

- Avec les outils RSAT, c'est comme sur un serveur Microsoft AD
- Autre option, utiliser la ligne de commande samba en mode ssh
  Ex : `samba-tool user create <nom utilisateur> <mot de passe>`
- Possibilité d'utiliser des scripts pour l'ajout d'utilisateurs multiples



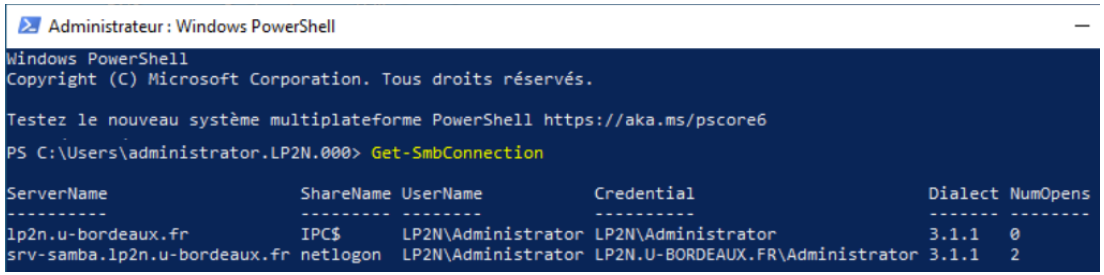


Gérer Samba à partir de la ligne de commande

Commandes	Usage
samba-tool -h	Affiche l'aide de la CMD samba-tool
samba-tool user -h	Affiche l'aide de la CMD samba-tool user
samba-tool user create xxx	Créer un utilisateur
samba-tool user list	Lister les utilisateurs du domaine
samba-tool user delete xxx	Supprimer un utilisateur
samba-tool user disable xxx	Désactiver un compte utilisateur
samba-tool user enable	Activer un compte utilisateur
samba-tool group add	Ajouter un groupe

Fiche technique de sécurité : Version de SMB

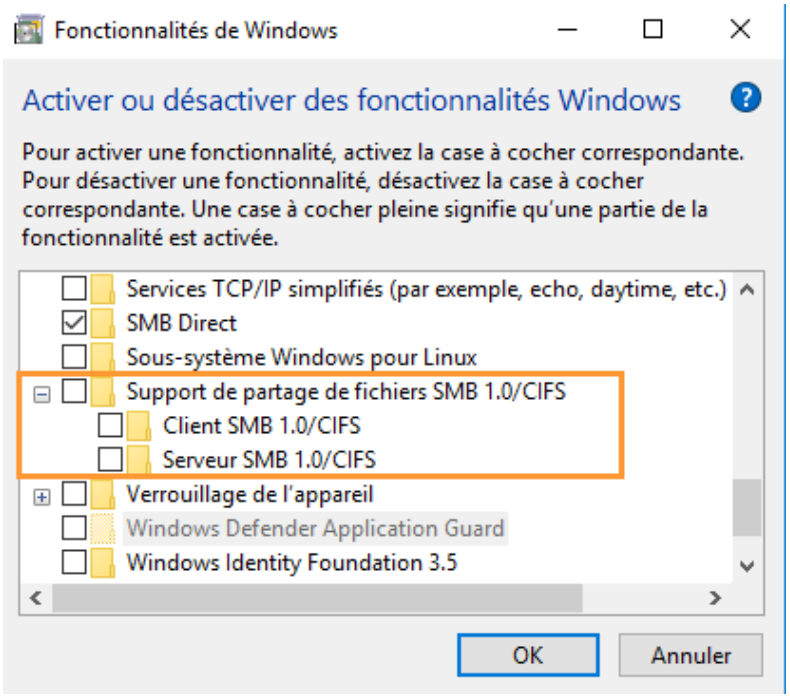
- Quel est le niveau du protocole SMB utilisé par Samba ?
- Un test simple permet d'afficher le résultat :
- Après vous être connecté au dossier `sysvol` du serveur AD, lancez la commande PowerShell suivante : Get-SmbConnection



OS	Windows 10/ 2016	Windows 8.1/ 2012 R2	Windows 8/ 2012	Windows 7 / 2008 R2	Windows Vista/ 2008	Windows XP/ 2003
Windows 10 / 2016	**SMB 3.1.1**	**SMB 3.0.2**	**SMB 3.0**	SMB 2.1	SMB 2.0.2	SMB 1
Windows 8.1/ 2012 R2	**SMB 3.0.2**	**SMB 3.0.2**	**SMB 3.0**	SMB 2.1	SMB 2.0.2	SMB 1
Windows 8/ 2012	**SMB 3.0**	**SMB 3.0**	**SMB 3.0**	SMB 2.1	SMB 2.0.2	SMB 1
Windows 7/ 2008 R2	SMB 2.1	SMB 2.1	SMB 2.1	SMB 2.1	SMB 2.0.2	SMB 1
Windows Vista 2008	SMB 2.0.2	SMB 2.0.2	SMB 2.0.2	SMB 2.0.2	SMB 2.0.2	SMB 1

Fiche technique de sécurité : Désactiver SMB V1.0

- Quel est le protocole SMB utilisé ?
  Démonstration V3.1.1, similaire à celui utilisé par MS AD.
- **Recommandation** : Désactiver SMB V1 (failles de sécurité à l'origine des cyber-attaques Wannacry et autres).

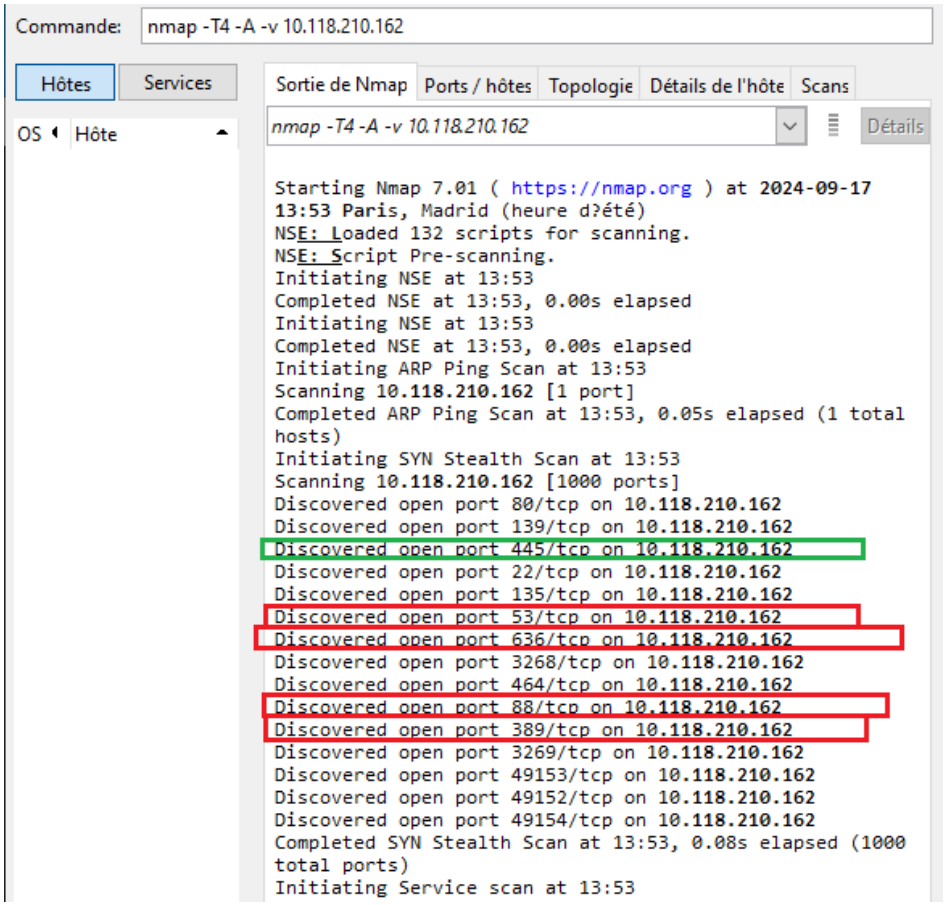


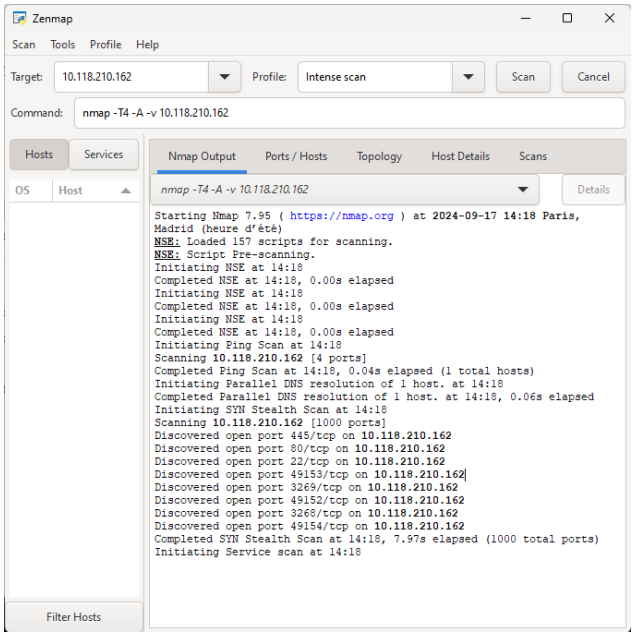
Les ports réseau utilisés par Samba

Protocoles utilisés et matrice des flux

- Un test `nmap` est réalisé à partir de la console vers le serveur.
  Détail de la commande : **nmap -T4 -A -v 10.118.210.162**
- Un autre test est réalisé à partir du poste de bureautique à joindre dans le domaine.
  On suppose que ce poste est dans un autre VLAN.
- Il reste à comparer les résultats et à ouvrir les ports en conséquence au niveau du pare-feu.

Les ports réseau utilisés par Samba





Bilan sur l'installation de Samba

Bilan

- **Avantages de la solution** :
  - Facilité de mise en œuvre d'une stratégie PCA/PRA - Dans un contexte de VM PVE et l'utilisation d'un PBS.
  - Amélioration de la sécurité - Solution minimaliste, plus facile à maîtriser.
  - Moins complet que MS AD mais suffisant dans la grande majorité des contextes.
- De nombreux établissements ont fait ce choix :
  Ministère de la Culture : 8000 postes, 170 sites, Ministère de l'Agriculture ...
  Source : https ://dev.tranquil.it/wiki/Samba4

Conclusions

Quelques questions ?

- La solution proposée par Tranqu'il IT est-elle la meilleure ?
  Pas forcément, oui dans le cas de l'utilisation de la solution WAPT.
- Quel est le niveau fonctionnel de SAMBA ?
  Schémas 2012 R2 et niveau fonctionnel 2008 R2 - suffisant pour gérer les postes Windows 10/11 avec des exigences de conformité strictes.
- Connaissiez-vous déjà SAMBA ?
- Qui utilise déjà SAMBA ?
- Autres questions ?

- Merci de votre attention ! -