Documentation GSB

Sommaire

Contexte	2
Synoptique	3
Présentation du Proxmox	4
Partie SRV-AD	5
Création de l'utilisateur	8
Intégration au domaine	12
Partie VPN	17
Partie nexcloud :	20

Contexte

Je possède un hyperviseur nommé Proxmox pour faire tourner mon infrastructure.

Je possède une machine virtuelle sous Debian 12 qui possède un Nextcloud qui est une plateforme sécurisée pour stocker, partager et collaborer sur des fichiers en ligne. Une connexion vpn, ainsi qu'une seconde machine sous Windows serveur 2022 pour mon Active Directory.

Sujet 1 : Mettre en place l'authentification AD sur une plateforme NextCloud. Réaliser les tests et rédiger une documentation qui détaille l'installation et la configuration.

Sujet 2 : L'entreprise a acquis de nouveaux locaux. Mettre en place un VPN pour que les collaborateurs des nouveaux locaux puissent utiliser les ressources historiques (smb, intranet) (VPN open source).

Synoptique



Voici le schémas réseau de l'infrastructure.

Présentation du Proxmox



Voici l'interface du Proxmox, on peut retrouver mes VM à gauche et la console de la VM choisie à droite.

Partie SRV-AD



Je commence tout d'abord par modifier le nom de mon serveur SRV-AD.

🛓 Gestionnaire de serveur				- 0
Gestio	onnaire de serveur 🔸	Tableau de bord Pour quitter le mode plein écran, appuye	₂z sur Échap	Gérer Outils Afficher
Tableau de bord	BIENVENUE DANS GE	STIONNAIRE DE SERVEUR		
Serveur local				
Tous les serveurs		Configurar co convour local		
Services de fichiers et d	. 📩 Assistant Ajout de rôles et de fo	nctionnalités	- 🗆 X	
	Sélectionner des	rôles de serveurs	SERVEUR DE DESTINATION SRV-AD	
	Avant de commencer	Sélectionnez un ou plusieurs rôles à installer sur le serveur séle	ectionné.	
	Type d'installation	Rôles	Description	
	Sélection du serveur	Attestation d'intégrité de l'appareil	Les services AD RMS (Active Directory Rights Management	
	Fonctionnalités	Serveur de télécopie	Services) vous aident à protéger les informations de toute utilisation non	Masquer
	AD DS	Serveur DNCP	autorisée. Ils établissent l'identité	
	Services Bureau à distance	Service Guardian hôte	informations protégées aux	
	Services de rôle	 Services AD DS Services AD LDS (Active Directory Lightweight Dire 	licences.	
	Résultats	 Services AD RMS (Active Directory Rights Manage Services Bureau à distance 	I	
		 Services d'activation en volume Services d'impression et de numérisation de docur 		
		Services de certificats Active Directory		
		 Services de fichiers et de stockage (1 sur 12 installe Services de tratérie et d'accèr récenu 		
		Services WSUS (Windows Server Update Services)		
		< V Vindows Deployment Services V		
		< Précédent Suivar	nt > Installer Annuler	

Voici les fonctionnalités que je vais installer pour mon AD.

Je poursuis la configuration de l'AD.

Configuration de o	déploiement		SE	RVEUR CIBLE SRV-AD
Configuration de déploie Options du contrôleur de Options DNS Options supplémentaires Chemins d'accès Examiner les options Vérification de la configur Installation Résultats	Sélectionner l'opération de déplo Ajouter un contrôleur de dom Ajouter un nouveau domaine Ajouter une nouvelle forêt Spécifiez les informations de dom Nom de domaine racine :	iement aaine à un domaine existant à une forêt existante naine pour cette opération valentin.eu	2	
	En savoir plus sur les configuratio	ons de déploiement		
		< Précédent Suivant >	Installer	Annuler

Je crée une novelle forêt.

La Assistant Configuration des serv	vices de domaine Active Directory	- 🗆 X
Options suppléme	entaires	SERVEUR CIBLE SRV-AD
Configuration de déploie Options du contrôleur de Options DNS Options supplémentaires Chemins d'accès Examiner les options Vérification de la configur Installation Résultats	Vérifiez le nom NetBIOS attribué au Le nom de domaine NetBIOS :	u domaine et modifiez-le si nécessaire. VALENTIN
	5	
	En savoir plus sur d'autres options	
	[< Précédent Suivant > Installer Annuler
📥 Assistant Configuration des serv	ices de domaine Active Directory	- 🗆 ×
Chemins d'accès		SERVEUR CIBLE SRV-AD
Configuration de déploie Options du contrôleur de Options DNS Options supplémentaires Chemins d'accès Examiner les options Vérification de la configur Installation Résultats	Spécifier l'emplacement de la base Dossier de la base de données : Dossier des fichiers journaux : Dossier SYSVOL :	de données AD DS, des fichiers journaux et de SYSVOL
	En savoir plus sur les chemins d'acc	ès Active Directory
		< Précédent Suivant > Installer Annuler

📥 Assistant Configuration des services de domaine Active Directory × SERVEUR CIBLE Vérification de la configuration requise SRV-AD 🔗 Toutes les vérifications de la configuration requise ont donné satisfaction. Cliquez sur Installer pour comme... Afficher plus × Configuration de déploie... La configuration requise doit être validée avant que les services de domaine Active Directory soient Options du contrôleur de... installés sur cet ordinateur Options DNS Réexécuter la vérification de la configuration requise Options supplémentaires Voir les résultats Chemins d'accès de l'établissement de sessions sur canal sécurisé. Examiner les options Vérification de la configur.. Pour plus d'informations sur ce paramètre, voir l'article 942564 de la Base de connaissances (http://go.microsoft.com/fwlink/?LinkId=104751). 1 Cet ordinateur contient au moins une carte réseau physique pour laquelle aucune adresse IP statique n'a été attribuée à ses propriétés IP. Si IPv4 et IPv6 sont tous deux activés pour une carte réseau, vous devez attribuer des adresses IP statiques IPv4 et IPv6 aux propriétés IPv4 et IPv6 de la carte réseau physique. Ces affectations d'adresses IP statiques doivent être effectuées sur toutes les cartes réseau physiques pour que l'opération DNS soit fiable. A Si vous cliquez sur Installer, le serveur redémarre automatiquement à l'issue de l'opération de promotion. En savoir plus sur les conditions préalables < Précédent Suivant > Installer Annuler

Point de vigilance :

Il faut désinstaller la fonctionnalité certificat pour éviter une erreur d'installation

Création de l'utilisateur

Pour tester cette authentification il faut que je crée un utilisateur sur l'AD qui va pouvoir se connecter au nextcloud.

Dans un premier temps j'ai créé une nouvelle unité d'organisation et j'ai créé mon utilisateur compte de service.

Utilisateurs et ordinateurs Active Directory	₩ all	192.168.0.11	_ 🗗 ×	-	٥	\times
Fichier Action Affichage ?						
← ⇒ 2 📷 ¼ 🗉 🗙 🖾 Q 🕞 🛛 🛪 🕱 🕷	7 🗾 🕱					
Utilisateurs et ordinateurs Active Directory [SRV-AD.valentin.eu] > ■ Requêtes enregistrées * ■ valentin.eu > ■ Builtin ■ Computers ■ Domain Controllers > ■ Computers ■ Nanaged Service Accounts ■ nextCoud-user ■ Users	Nom Type	Description r				

Voici donc mon utilisateur de crée, je vais ensuite récupérer le lien de l'utilisateur dans l'AD pour l'autoriser à accéder au Nextcloud.

Il ne faut pas oublier de cocher cette option d'affichage avancer.



Utilisateurs et ordinateurs Active Directory		- 0 ×
Fichier Action Affichage ?	and 17 Ma	
 Utilisateurs et ordinateurs Active Directory (SRV-ADvalentin.eu) Requêtes enregistrées Valentin.eu Computers Computers Compares de service Sourciant Controllers Exerciant Service Accounts Reys LostAndFound Managed Service Accounts Program Data System Users MTDS Quotas MTDS Quotas Admin Nextcloud 	Nom Type Description Image: Second Secon	

Je recherche ensuite éditeur d'attribut, et il faut que je copie cette ligne-là.

Serveur		Attributs de connexion	Groupes			
1. Serve	eur : 192.168.0.	11 - +				
192.168	.0.11			389	Détecter le port	
CN=nex	tcloud,OU=com	nptes de service,DC=valent	in,DC=eu			

Je la copie ici, au-dessus dans la configuration LDAP du Next cloud l'adresse IP de mon serveur

1. Serveur : 192.168.0.11 -				
192.168.0.11		389	Détecter le port	
CN=nextcloud,OU=comptes de se	ervice,DC=valentin,DC=eu			
	Sauvegarder les inform	ations d'identif	ication	
OU=nextcloud-	Détecter le DN de base	Tester le DN c	le base	
Saisir les filtres LDAP manuellem	ent (recommandé pour les ann	uaires de grande	ampleur)	
Configuration	DK Continuer	• Aide		

Ensuite je rentre le mot de passe de l'utilisateur du compte de service.

Et en dessous les utilisateurs du groupe nextcloud user que je veux affilier au nextcloud

Utilisateurs et ordinateurs Active Directory Fichier Action Affichage ?		- 8 ×
🗢 🌩 🙍 📷 🤾 🖬 🗙 🗑 🍳 🗟 📷 🗏 🐮	a 🔻 🔟 🐱	
Utilisateurs et ordinateurs Active Directory [SRV-ADvalentin.eu] > ■ Requêtes enregistrées > ■ Builtin ≥ □ comptes de service > ■ Computers > ■ Computers	Nom Type Description g user1 Utilisateur Utilisateur g user2 Utilisateur	
 ForeignSecurityPrincipals Keys LostAndFound Managed Service Accounts nextdoud-user Pogram Data System Users NDS Quotas TMD Sevices Admin Nextcloud 	Propriétés de : nextdoud-user ? *	
	OK Annuler Appliquer Aide	

Je rentre ce lien-là qui est directement l'unité d'organisation des utilisateurs, quand un utilisateur serra crée dans cette unité il sera automatiquement sur nexcloud.

Intégration au domaine

Il faut maintenant que j'intègre au domaine mon client pour qu'il ait accès aussi au dossier partagé.



Voici des dossiers que j'ai créé sur le serveur AD.

📜 Propriétés de : partage_public		X		
Général Partage Sécurité Versions Partage de fichiers et de dossiers en re	a Accès réseau			
partage_public Partagé	Choisir les utilisateurs pouvant accéder à votre	e dossier partagé		
Chemin réseau : \\SRV-AD\partage_public	Tapez un nom et cliquez sur Ajouter, ou cliquez sur la flèche pour rechercher un utilisateur.			
Partager		~ Ajouter		
Partage avancé	Nom	Niveau d'autorisation		
d'autres options de partage.	🚴 Administrateur	Propriétaire		
Partage avancé	Studisateurs du domaine	Lecture 🔻		
	Je rencontre des difficultés pour partager.			
		Partager Annuler		

J'ai cliqué sur **Partager** et ajouté le groupe utilisateur du domaine pour que tous les utilisateurs.

 Propriétés de : partage_public Général Partage Sécurité Versions précédentes Personnaliser (×
Partage de fichiers et de dossiers en réseau partage_public Partagé Chemin réseau : \\SRV-AD\partage_public Partager Partage avancé Définir des autorisations personnalisées, créer des ressources parta d'autres options de partage. Partage avancé	Partage avancé × Partager ce dossier Paramètres Nom du partage : partage_public Ajouter Supprimer Limiter le nombre d'utilisateurs simultanés à : 16777 •
Fermer Ann	Autorisations Mise en cache OK Annuler Appliquer Uler Appliquer

Puis j'ai coché la case Partager ce dossier

Propriétés de : partage tech		
age Général Partage Sécurité Versions précédentes Per	🔶 🛛 🏭 Accès réseau	×
Partage de fichiers et de dossiers en réseau partage_tech Partagé Chemin réseau : \\SRV-AD\partage_tech	Choisir les utilisateurs pouvant ac Tapez un nom et cliquez sur Ajouter, ou clique	céder à votre dossier partagé ez sur la flèche pour rechercher un utilisateur.
Partager	[✓ Ajouter
Définir des autorisations personnalisées, créer des resso d'autres options de partage.	Nom 🚴 Administrateur	Niveau d'autorisation Propriétaire
Partage avancé	Stechnicien	Lecture 🔻
	Je rencontre des difficultés pour partager.	
ОК		Partager Annuler

Le même procédé pour les autres dossiers où cette fois j'ai autorisé uniquement le groupe **technicien** donc seuls les utilisateurs appartenant au groupe **technicien** pourront accéder à ce dossier.

Paramètres			- 0 ×				
命 Accueil	À propos de						
Rechercher un paramètre	Votre ordinateur est si protégé.	Paramètres associés Paramètres de Bitlocker					
Système	Voir les détails dans la sécurité Windows		Gestionnaire de périphériques				
🖵 Écran	Spécifications de l'appareil		Bureau à distance				
			Protection du système				
다까 Son	Nom de l'appareil	DESKTOP-LNDG0CK	Paramètres avancés du système				
□ Actions et notifications	Nom complet de l'appareil Processeur	DESKTOP-LNDG0CK.valentin.eu QEMU Virtual CPU version 2.5+	Renommer ce PC (avancé)				
Assistant de concentration	Mémoiro PAM installée	3.25 GHz					
() Alimentation et mise en veille	ID de périphérique	4,00 80 A08BFD6C-4EEC-48EF-976B- AA315C7545B1	Aide du web				
-	ID de produit	00330-80000-00000-AA212	Recherche du nombre de cœurs dont dispose mon processeur				
□ Stockage	Type du système	Système d'exploitation 64 bits, processeur x64	Vérification de la prise en charge de				
년 Tablette	Stylet et fonction tactile	La fonctionnalité d'entrée tactile ou avec un stylet p'est pas disponible	prusieurs langues				
⊟† Multitâche		sur cet écran	Obtenir de l'aide				
Projection sur ce PC	Copier		Donner des commentaires				
X Expériences partagées	Renommer ce PC						

Je me rends ensuite sur mon client Windows pour l'intégrer au domaine.

Je vais alors dans Renommer ce PC (anvancé)

ł	Propriétés système				>	×		
	Paramètres système avan	cés Protection du	és Protection du système			•		
L	Nom de l'ordir	nateur	1	Matéri	el			
	Windows utilise les informations suivantes pour identifier votre ordinateur sur le réseau.							
l	Description de l'ordinateur :							
l		Par exemple : "L'ordinateur du salon" ou "L'ordinateur d'Antoine".						
	Nom complet de l'ordinateur :	DESKTOP-LNDG0CK.valentin.eu						
t	Domaine :	valentin.eu						
•	Pour utiliser un Assistant et vous joindre à un domaine ou un groupe de travail, cliquez sur Identité sur le réseau.							
t	Pour renommer cet ordina domaine ou de groupe de	ateur ou changer de e travail, cliquez sur M	lodifier.	Mod	ifier			
E								
٦		ОК	Ann	uler	Appliquer			

Puis modifier

· · · · - · · · · · · · · · · · ·	×
Modification du nom ou du domaine de l'ordinateur $~ imes~$ on à dista	ance
Vous pouvez modifier le nom et l'appartenance de cet ordinateur. Ces modifications peuvent influer sur l'accès aux ressources réseau.	
Nom de l'ordinateur :	
DESKTOP-LNDG0CK	
Nom complet de l'ordinateur : DESKTOP-LNDG0CK.valentin.eu	
Autres	_
Membre d'un	u
Domaine :	
valentin.eu fier	
Groupe de travail :	
OK Annuler	
OK Annuler Appliq	uer

Ensuite on coche **Membre d'un domaine (**il est déjà coché chez moi car je l'avais fait au préalable mais avec c'était sur groupe de travail)

T

Grace à la connexion VPN, mon client Windows peut intégrer le domaine AD, et accéder au dossier partager de l'AD

Partie VPN

Voici les configuration vpn coté client ainsi que serveur.

Je possède 2 clients et je souhaite que les 2 accèdent au nexcloud donc j'ai créé 2 réseaux privé

Voir la config du ISP

Il faut donc installer le paquet wireguard sur notre serveur et crée le fichier de configuration ou le modifier dans **/etc/wireguard/wg0.conf**

Ensuite créer les clés publiques + privé pour le vpn :

wg genkey | tee privatekey |wg pubkey > publickey

Voici la confutilisée coté ISP :



Le bloc interface est la configuration du serveur avec sa clé privé.

Les blocs Peer sont les clients qui sont autorisé avec leur adresse réseau.

Pour la clé publique c'est la clé publique de mes clients.

Sur mes clients je télécharge le client wiregard et je crée un nouveau tunnel qui a va automatique crée une clé privée et je modifie ensuite le fichier de conf.

Pour redémarrer le service de wireguard : systemctl restart wg-quick@wg0.service

Voici la conf coté client windows :



Voici la conf du client Debian :



Partie nexcloud :

Une fois le serveur nexcloud installé, il faut que j'installe sur la VM nextcloud le paquet : phpldap

apt install php-ldap

Une fois cela fait je me rends ici et j'active le service LDAP, c'est ce qui vas me permettre de lier l'AD au nexcloud.

o⊖o					<u>,</u> Q	¢ 🖪	A,
Découvrir Vos applications		Packs d'applications					Â
 Applications actives 		Pack pour entreprise Tout télécharger et activer					
× Applications désactivées	٥	Auditing / Logging	1.21.0	🗸 En vedette		Activ	rer
Packs d'applications	÷	LDAP user and group backend	1.22.0	🖌 En vedette		Désactiv	/er
★ Applications en vedette Documentation développeurs		Pack pour éducation Tout désactiver					
		Dashboard	7.11.0	🗸 En vedette		Désactiv	/er
	<u>, 21</u>	Teams	31.0.0-dev.0	🖌 En vedette		Désactiv	/er
		Pack pour secteur public Tout télécharger et activer					
	*					_ 11:09	

J'active ensuite cette option.