Institut universitaire de technologie
Aix-Marseille université

Rapport de stage de fin de deuxième année
Bachelor Universitaire de Technologie Spécialité Réseaux et Télécommunications Parcours cybersécurité

Mise en place d'un serveur Radius avec authentification WPA2 entreprise et MAC

Yidhir MERAD

Arcanes - Conseil et intégrateur Sage X3

Responsable entreprise : Robin CHABAUD

Responsable académique : Ivan MADJAROV

2024

Remerciements

Je remercie l'équipe d'arcanes pour leur accueil et pour m'avoir accepté au sein de leur effectif.

Je remercie plus particulièrement :

Monsieur Nacer Khasri pour m'avoir offert cette opportunité très enrichissante au sein de son équipe.

Monsieur Robin Chabaud pour sa patience, écoute, conseils et surtout le suivi professionnel qu'il m'a accordé.

Je tiens aussi à remercier monsieur Ivan Madjarov, mon tuteur pédagogique pendant ce stage.

Table des matières

Introduction :

Je suis ravi de vous faire part de mon projet de stage au sein de l'entreprise Arcanes, une opportunité exceptionnelle pour approfondir mes compétences en gestion et sécurisation des réseaux informatiques. Durant cette période, mon travail s'est concentré sur un aspect essentiel de l'infrastructure réseau de l'entreprise : la sécurisation du réseau Wi-Fi via l'implémentation d'un système d'authentification RADIUS (Remote Authentication Dial-In User Service).

Dans un contexte où la sécurité des réseaux sans fil représente un enjeu critique pour la protection des données sensibles et la continuité des opérations, ce projet vise à renforcer significativement la sécurité des communications au sein de l'entreprise Arcanes. Les réseaux Wi-Fi, bien qu'indispensables pour la flexibilité et la mobilité qu'ils offrent, sont particulièrement vulnérables aux attaques et aux accès non autorisés. Une authentification robuste est donc impérative pour garantir que seuls les utilisateurs autorisés puissent accéder aux ressources réseau.

Le système RADIUS fut central dans cette démarche. Ce protocole permet une gestion centralisée de l'authentification, de l'autorisation et de la comptabilisation (AAA), offrant ainsi une solution fiable et évolutive pour sécuriser le réseau Wi-Fi. Mon objectif est d'implémenter et de configurer un serveur RADIUS capable de valider les identités des utilisateurs en se basant sur des informations stockées dans une base de données sécurisée, telle que Active Directory. Cette approche assurera non seulement une meilleure gestion des accès, mais aussi une traçabilité accrue des connexions.

En collaboration avec l'équipe réseau de l'entreprise, j'ai du analyser les besoins spécifiques de l'organisation, concevoir des politiques de sécurité adaptées, et déployer le système d'authentification RADIUS. Ce projet implique également la formation du personnel IT sur l'utilisation et la gestion du nouveau système, assurant ainsi une transition fluide et une adoption réussie de la solution.

Ce stage chez Arcanes a représenté une formidable opportunité pour moi de mettre en pratique mes connaissances théoriques, tout en apportant une contribution tangible à la sécurité de l'entreprise.

Contexte :

L'entreprise, son histoire :

Arcanes est une entreprise de services du numérique fondée en 1983 par monsieur Daniel PICOLET. Initialement éditrice de solutions d'aides à la gestion des entreprises, la société devient en 2000 intégratrice du logiciel Adonix X3 puis Sage X3.

L'entreprise est rachetée en 2013, par dix de ses dix-neuf salariés, lors du départ en retraite de son fondateur. Le groupe Arcanes a rach eté K-ZAM, une petite entreprise qui crée des sites web B2B et B2C. Le but étant de connecter ces sites web au logiciel SageX3.

Le groupe Arcanes emploie 51 salariés, et accueille en 2023-2024 septs alternants.

La direction est composée de six membres, parmi lesquels se trouvent deux anciens alternants, et un certain nombre d'autres salariés ont également réalisé leurs alternances au sein d'Arcanes, qui est donc familière avec ce concept.

Basée à Aubagne à sa création, l'entreprise cherchant à être propriétaire de ses locaux, un déménagement s'imposait. Arcanes a récemment déménagé à Marseille, Avenue du Prado.

L’activité, les services :

Arcanes est donc une société qui développe des logiciels en lien avec le logiciel X3 de Sage. Sage X3 est un Progiciel de Gestion Intégré (PGI / ERP) destiné aux PME. Il est la suite de l’ERP Adonix X3, édité par la société française Adonix, après le rachat de

Arcanes propose donc à leurs collaborateurs l’installation de ce logiciel dans les locaux des différentes entreprises, ou sur un serveur cloud.

Le logiciel proposé par l’entreprise et un logiciel gérant toute la partie logistique, gestion des entrepôts, gestion des stocks et la réception de colis. Dans le cas où certaines fonctionnalités ne sont pas présentes, chaque client peut demander le développement de ces dernières.

Les ressources humaines et techniques :

Arcanes compte une quarantaine d’employés, se répartissant de la manière suivante :

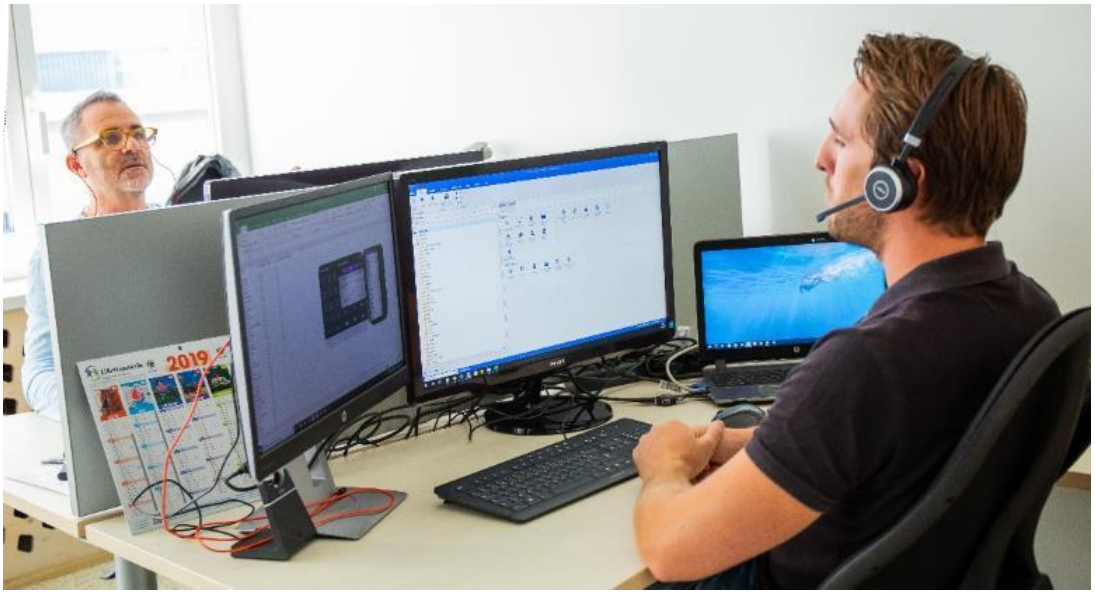
Mme Pascale AZEMA est à la tête de l’entreprise, aidée par 6 responsables de services.

Les différents services en question sont :

- Administration et comptabilité (3 employé(e)s)
- Commerce et marketing (4 employé(e)s)
- Consulting Sage X3 & BI (18 employé(e)s)
- Développeurs Sage X3 (12 employé(e)s)
- Support clients (2 employé(e)s)
- Service Informatique / support technique (3 employé(e)s)

Le service où j’effectue ma mission :

Pour reprendre l’organigramme précèdent, j’effectue mon stage dans l’équipe du service informatique / support technique pour les clients du groupe Arcanes. J’ai été Dirigé par mon tuteur de stage Mr Robin CHABAUD.



Qu’est-ce qu’un serveur radius ?

Dans un premier temps j’ai dû me renseigner sur le fonctionnement d’un serveur radius.

Fonctionnement théorique :

Un système RADIUS (Remote Authentication Dial-In User Service) est un protocole réseau qui assure l'authentification, l'autorisation et la comptabilisation (AAA) des utilisateurs se connectant à un réseau. Voici comment fonctionne un système RADIUS :

Authentification

1. **Demande d'Accès** : Lorsqu'un utilisateur tente de se connecter à un service réseau (comme un VPN, un point d'accès Wi-Fi, ou un serveur dial-up), le client RADIUS (généralement un NAS, Network Access Server) envoie une demande d'authentification au serveur RADIUS. Cette demande contient les informations d'identification de l'utilisateur, telles que le nom d'utilisateur et le mot de passe.
2. **Transmission de la Demande** : Le client RADIUS transmet ces informations via le protocole RADIUS au serveur RADIUS, généralement de manière chiffrée pour assurer la sécurité des informations.
3. **Validation des Informations** : Le serveur RADIUS vérifie les informations d'identification de l'utilisateur en les comparant à une base de données d'utilisateurs, souvent intégrée à un service d'annuaire comme Active Directory. Si les informations sont correctes, le serveur RADIUS envoie une réponse positive au client RADIUS. Sinon, il envoie une réponse de rejet.

Autorisation

1. **Vérification des Politiques** : Une fois l'utilisateur authentifié, le serveur RADIUS vérifie les politiques d'accès pour déterminer les permissions de l'utilisateur. Cela peut inclure des règles sur les heures d'accès, les types de services accessibles, et les restrictions de bande passante.
2. **Réponse d'Autorisation** : Le serveur RADIUS envoie au client RADIUS une réponse contenant les attributs d'autorisation, qui spécifient les permissions et les restrictions applicables à la session de l'utilisateur.

Comptabilisation

1. **Suivi des Sessions** : Le serveur RADIUS peut également suivre l'activité des utilisateurs pour des fins de comptabilisation. Chaque fois qu'un utilisateur commence et termine une session, le client RADIUS envoie des rapports au serveur RADIUS.
2. **Rapports de Comptabilisation** : Ces rapports incluent des informations comme l'identité de l'utilisateur, la durée de la session, la quantité de données transférées, et d'autres paramètres pertinents.
3. **Analyse et Facturation** : Les données de comptabilisation peuvent être utilisées pour générer des rapports d'utilisation, analyser les tendances du réseau, ou même facturer les utilisateurs en fonction de leur utilisation des services.

Exemple concret :

Voici un exemple de schéma RADIUS :

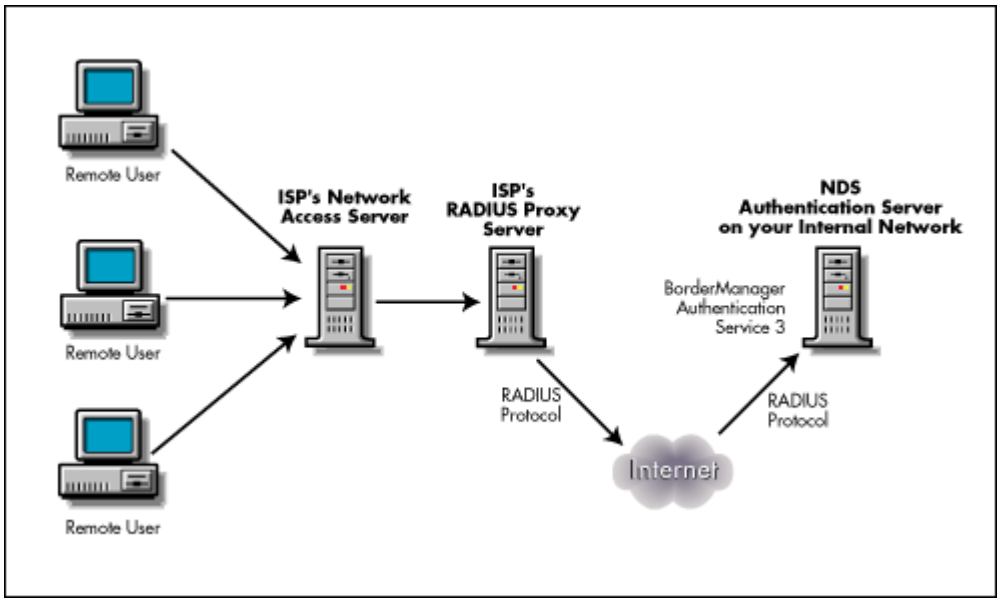


Figure 1 : Schéma d'un système radius

Dans cet exemple, on observe le fonctionnement d'un système RADIUS « classique ».

Composants Impliqués

1. **Remote Users** : Utilisateurs distants tentant de se connecter au réseau.

2. **ISP's Network Access Server (NAS)** : Serveur d'accès réseau de l'ISP (fournisseur de services Internet) qui reçoit les demandes de connexion des utilisateurs distants.
3. **ISP's RADIUS Proxy Server** : Serveur proxy RADIUS de l'ISP, qui relaie les demandes d'authentification RADIUS vers le serveur d'authentification interne.
4. **NDS Authentication Server on your Internal Network** : Serveur d'authentification interne de l'entreprise (utilisant NDS - Novell Directory Services), qui valide les informations d'identification des utilisateurs.
5. **Internet** : Le réseau utilisé pour transmettre les demandes et réponses RADIUS entre les différents serveurs.

Processus de Fonctionnement

1. **Connexion Initiale** :
    - Les utilisateurs distants tentent de se connecter au réseau via le NAS de l'ISP. Ils envoient leurs informations d'identification (nom d'utilisateur et mot de passe).
2. **Envoi de la Demande au Proxy RADIUS** :
    - Le NAS de l'ISP reçoit les informations d'identification et les encapsule dans une demande RADIUS.
    - Cette demande est envoyée au serveur proxy RADIUS de l'ISP.
3. **Relais de la Demande d'Authentification** :
    - Le serveur proxy RADIUS de l'ISP reçoit la demande et la relaie au serveur d'authentification interne de l'entreprise via le protocole RADIUS, passant par Internet.
4. **Validation des Informations d'Identification** :
    - Le serveur d'authentification interne (NDS Authentication Server) reçoit la demande et vérifie les informations d'identification contre sa base de données interne (NDS).
    - Si les informations sont correctes, le serveur d'authentification envoie une réponse positive (Access-Accept) au serveur proxy RADIUS de l'ISP.
    - Si les informations sont incorrectes, une réponse de rejet (Access-Reject) est envoyée.
5. **Transmission de la Réponse au NAS** :
    - Le serveur proxy RADIUS de l'ISP transmet la réponse (positive ou négative) au NAS de l'ISP.
6. **Autorisation d'Accès** :
    - Le NAS de l'ISP, sur réception d'une réponse positive, permet à l'utilisateur distant d'accéder au réseau.
    - Si la réponse est négative, l'accès est refusé.

Travaux effectués :

Installation de la VM :

Pour la machine virtuelle qui a servi de serveur RADIUS, j'ai utilisé VMware Workstation

(Outil de virtualisation de poste de travail crée par VMware).

VMware Workstation est une application de virtualisation de bureau qui permet aux utilisateurs d'exécuter plusieurs systèmes d'exploitation simultanément sur un même ordinateur physique. Développé par VMware, ce logiciel est principalement utilisé par les développeurs, les testeurs de logiciels, et les administrateurs système pour créer, tester et déployer des environnements multiples sans avoir besoin de matériel supplémentaire.

Les principales fonctionnalités de VMware Workstation incluent la capacité de créer et gérer des machines virtuelles (VM), le support de nombreux systèmes d'exploitation (Windows, Linux, etc.), la possibilité de cloner des VMs, ainsi que des outils de snapshots pour sauvegarder et restaurer des états de VM à différents points dans le temps. De plus, VMware Workstation offre des fonctionnalités avancées telles que le partage de VMs avec d'autres utilisateurs, le support de réseaux virtuels complexes, et l'intégration avec d'autres produits VMware pour faciliter le déploiement en production.

J'ai téléchargé une image Windows server 2022 et installé sur VMware Workstation. Par la suite j'ai installé l'image normalement

Installation de l'active directory :

Active Directory (AD) de Windows peut être intégré avec un serveur RADIUS (Remote Authentication Dial-In User Service) pour fournir une authentification centralisée et sécurisée des utilisateurs. Dans ce contexte, AD agit comme la base de données des utilisateurs et des groupes, stockant les informations d'identification et les autorisations associées. Le serveur RADIUS, quant à lui, sert de médiateur pour authentifier les utilisateurs qui tentent de se connecter à divers services réseau, tels que les VPN, les points d'accès Wi-Fi, ou autres dispositifs réseau. Lorsque qu'un utilisateur essaie d'accéder à un service, le serveur RADIUS transmet la demande d'authentification à AD, qui vérifie les informations d'identification fournies. Si elles sont valides, AD renvoie une réponse positive au serveur RADIUS, permettant ainsi l'accès au service demandé.

Pour configurer cette intégration, il est nécessaire de mettre en place un serveur RADIUS compatible avec AD, comme Network Policy Server (NPS) sous Windows Server. NPS peut être configuré pour utiliser AD comme source d'authentification, en créant des politiques de réseau qui spécifient les conditions et contraintes d'accès. Il est également possible de renforcer la sécurité avec des méthodes d'authentification à plusieurs facteurs (MFA), combinant des mots de passe avec des jetons matériels, des applications mobiles, ou des certificats numériques. Cette configuration permet non seulement de centraliser la gestion des identités et des accès, mais aussi de s'assurer que toutes les tentatives de connexion passent par un processus d'authentification robuste et conforme aux politiques de sécurité de l'organisation.

Pour la mise en place je suis passé par une virtualisation pour plusieurs raisons . La virtualisation offre plusieurs avantages significatifs pour la mise en place d'un serveur RADIUS. Voici quelques-uns des principaux intérêts :

1. **Flexibilité et Scalabilité** : La virtualisation permet de déployer rapidement des serveurs RADIUS dans des environnements de test, de développement, ou de production sans nécessiter de matériel physique supplémentaire. Les ressources (CPU, mémoire, stockage) peuvent être facilement ajustées en fonction des besoins, ce qui permet d'optimiser la performance et de répondre à des augmentations de charge. Si la demande pour le serveur RADIUS augmente, il est simple de cloner des machines virtuelles ou d'ajuster les ressources allouées pour répondre à ces besoins.

2. **Fiabilité et Continuité des Services** : En utilisant des machines virtuelles, il est possible de mettre en place des mécanismes de haute disponibilité et de récupération après sinistre. Par exemple, les snapshots permettent de sauvegarder l'état d'une VM à un moment précis, facilitant ainsi la restauration rapide en cas de problème. De plus, les hyperviseurs modernes permettent de migrer des VMs d'un hôte physique à un autre sans interruption des services (live migration), ce qui est crucial pour maintenir la continuité des services RADIUS critiques pour les au- thentifications réseau.

En résumé, la virtualisation rend la gestion des serveurs RADIUS plus agile, rentable et résiliente, en permettant des déploiements rapides, une utilisation optimisée des ressources, et des stratégies robustes de sauvegarde et de récupération.

Le schéma du réseau de Test ressemble donc à ceci :

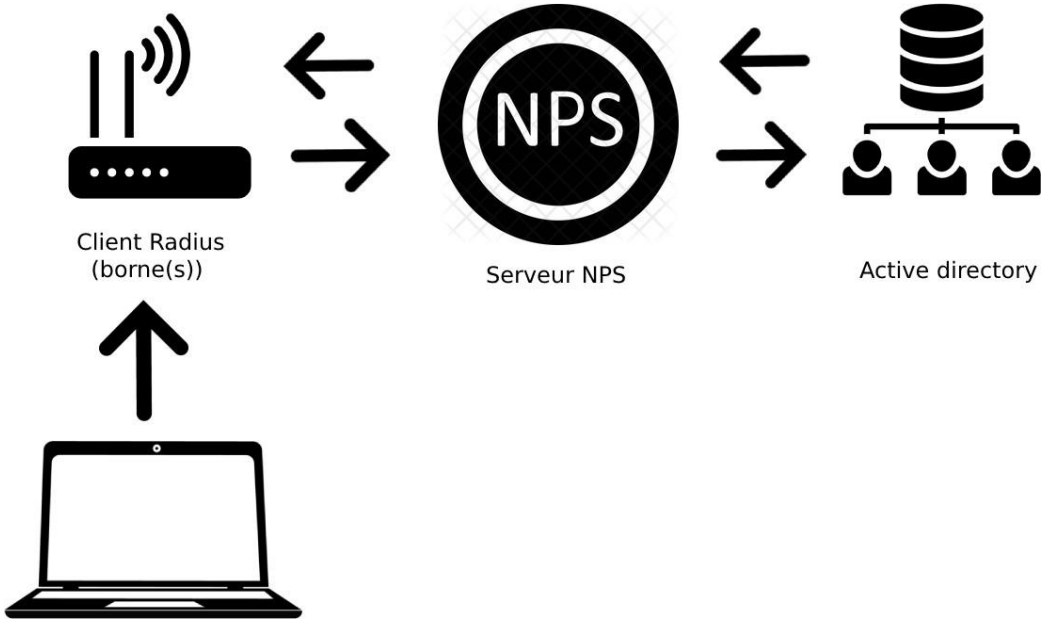


Figure 2 : Schéma du réseau dans lequel j'ai effectué mes test

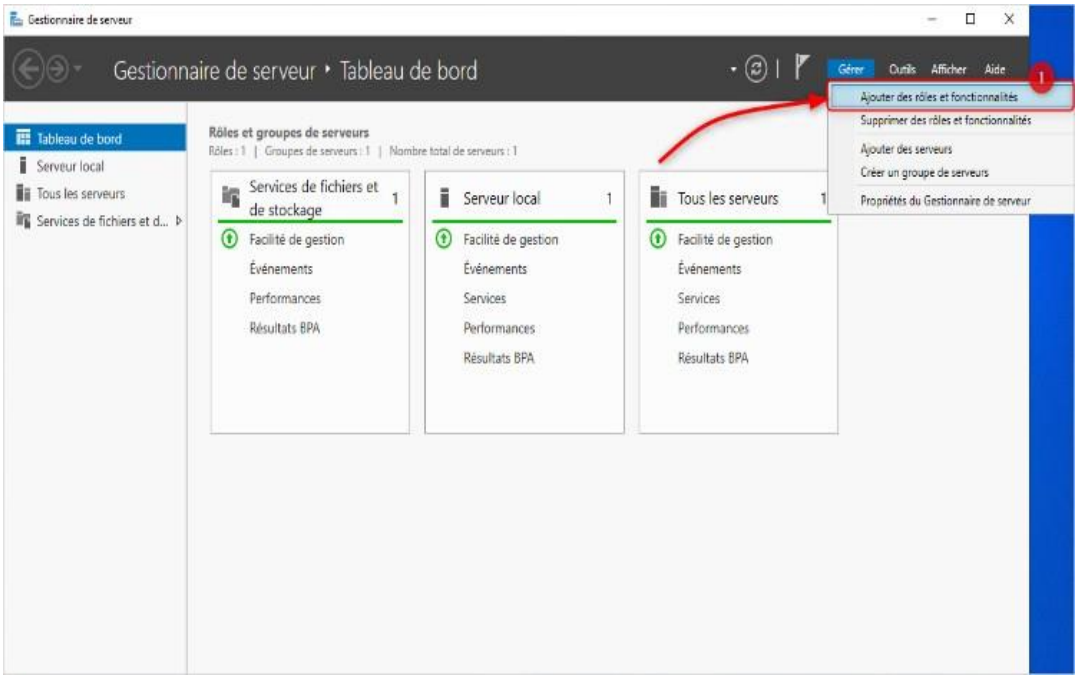
Active Directory :

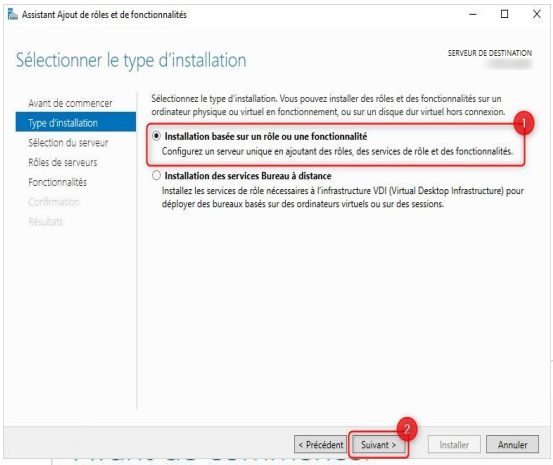
On commence donc par mettre en place l'Active directory :

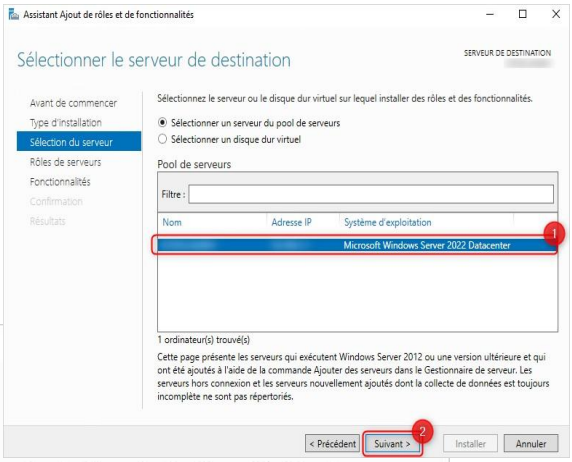
Sur le serveur Windows 2022, j'ai dû installer Windows Active Directory. J'ai fait cela par lebiais du gestionnaire de serveur.

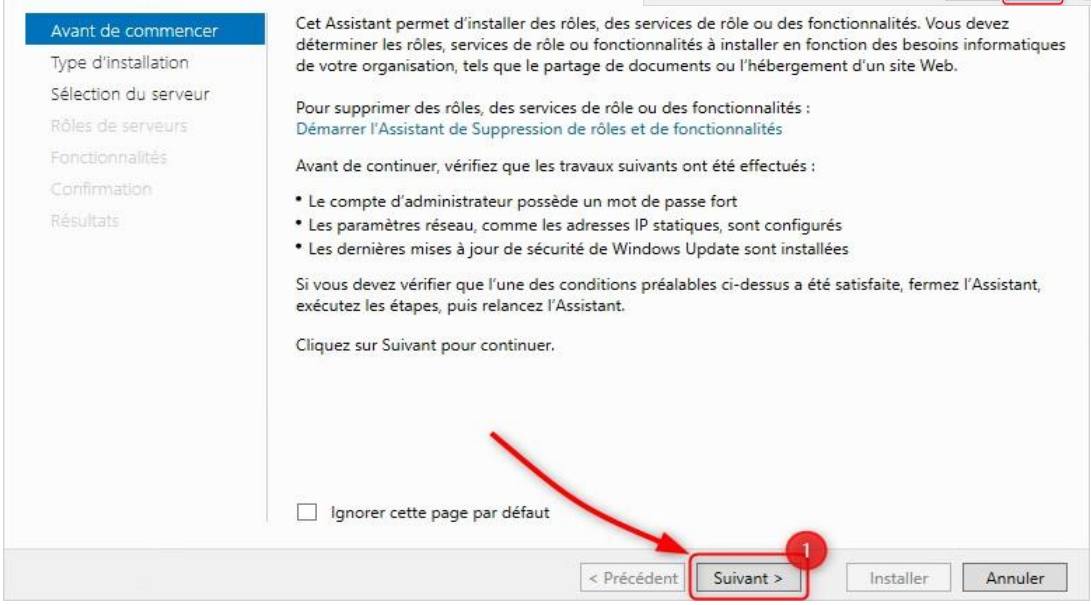
Le processus est simple : Gérer en haut à droite > Ajouter des rôles ou des fonctionnalités

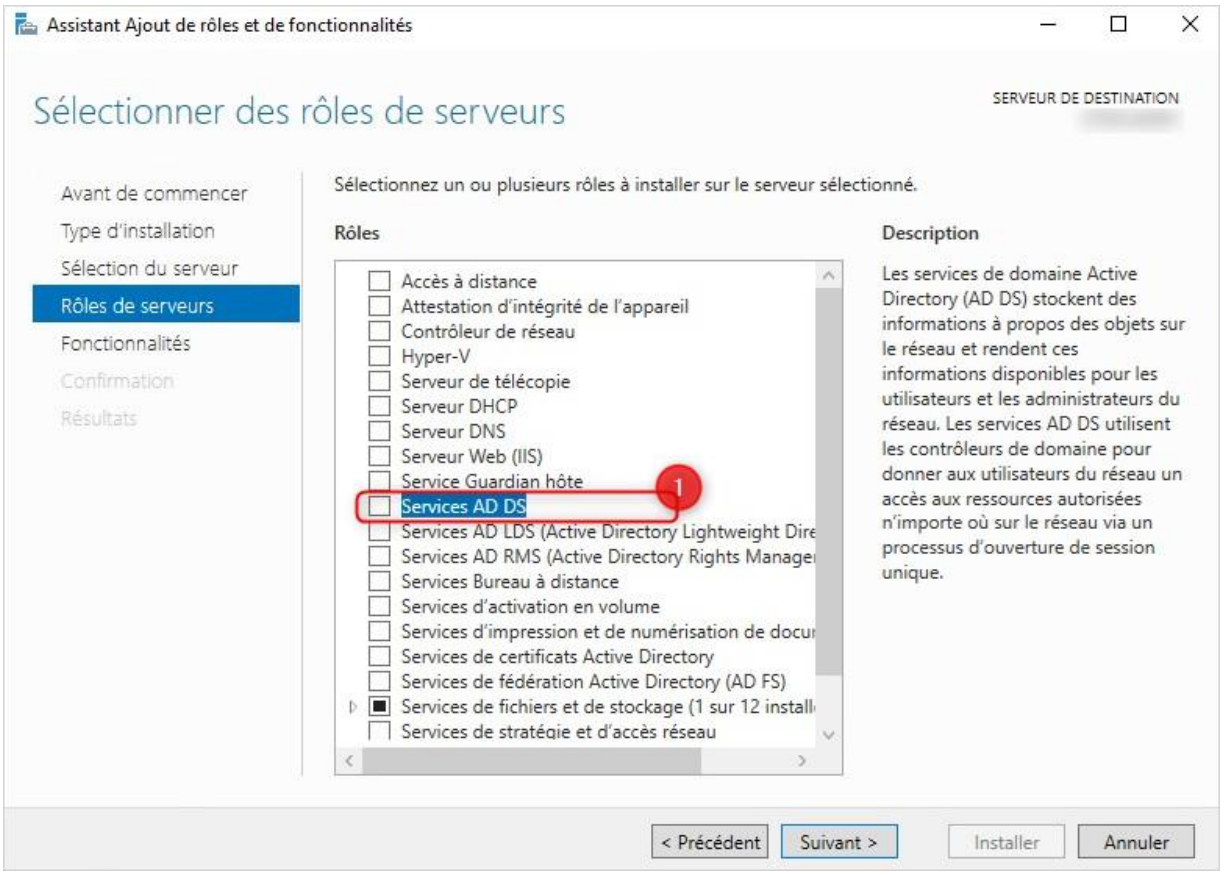
(totalité du processus détaillée dans les captures d'écran ci-dessous)

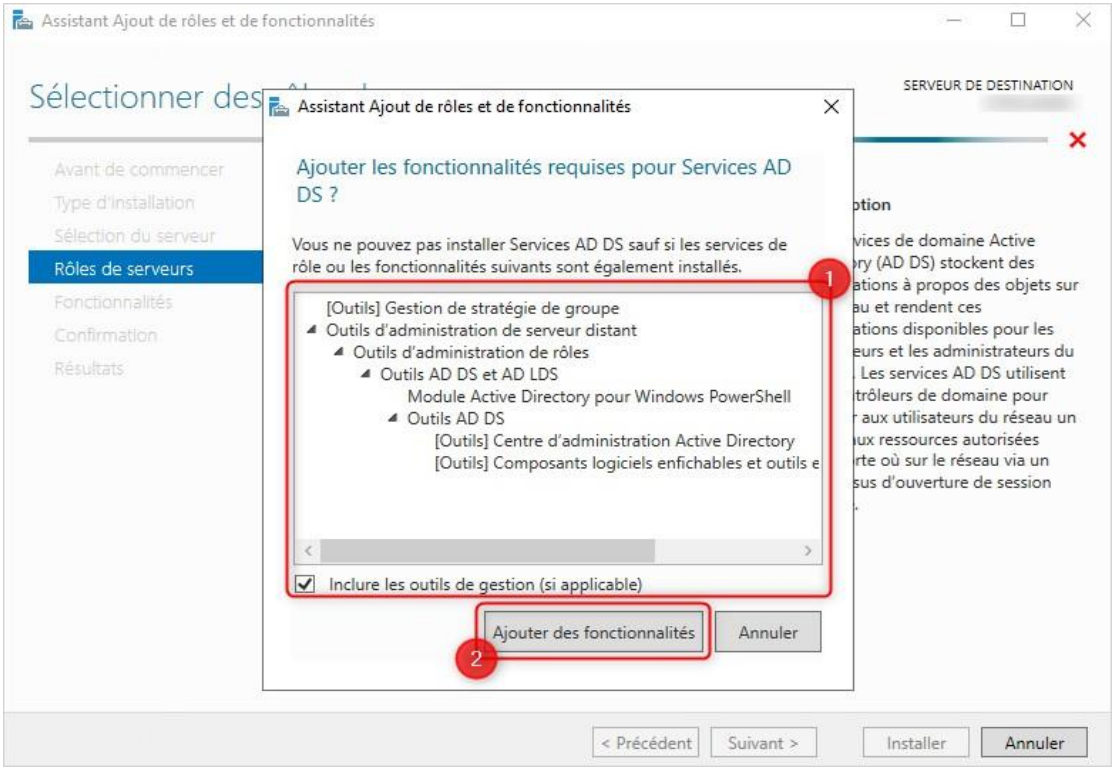

Gestionnaire de serveur
Gestionnaire de serveur • Tableau de bord
Gérer
Outils
Afficher
Aide
Ajouter des rôles et fonctionnalités
Supprimer des rôles et fonctionnalités
Ajouter des serveurs
Créer un groupe de serveurs
Propriétés du Gestionnaire de serveur
Tableau de bord
Serveur local
Tous les serveurs
Services de fichiers et d...
Rôles et groupes de serveurs
Rôles : 1 | Groupes de serveurs : 1 | Nombre total de serveurs : 1
Services de fichiers et de stockage 1
Serveur local 1
Tous les serveurs 1
Facilité de gestion
Événements
Performances
Résultats BPA
Services

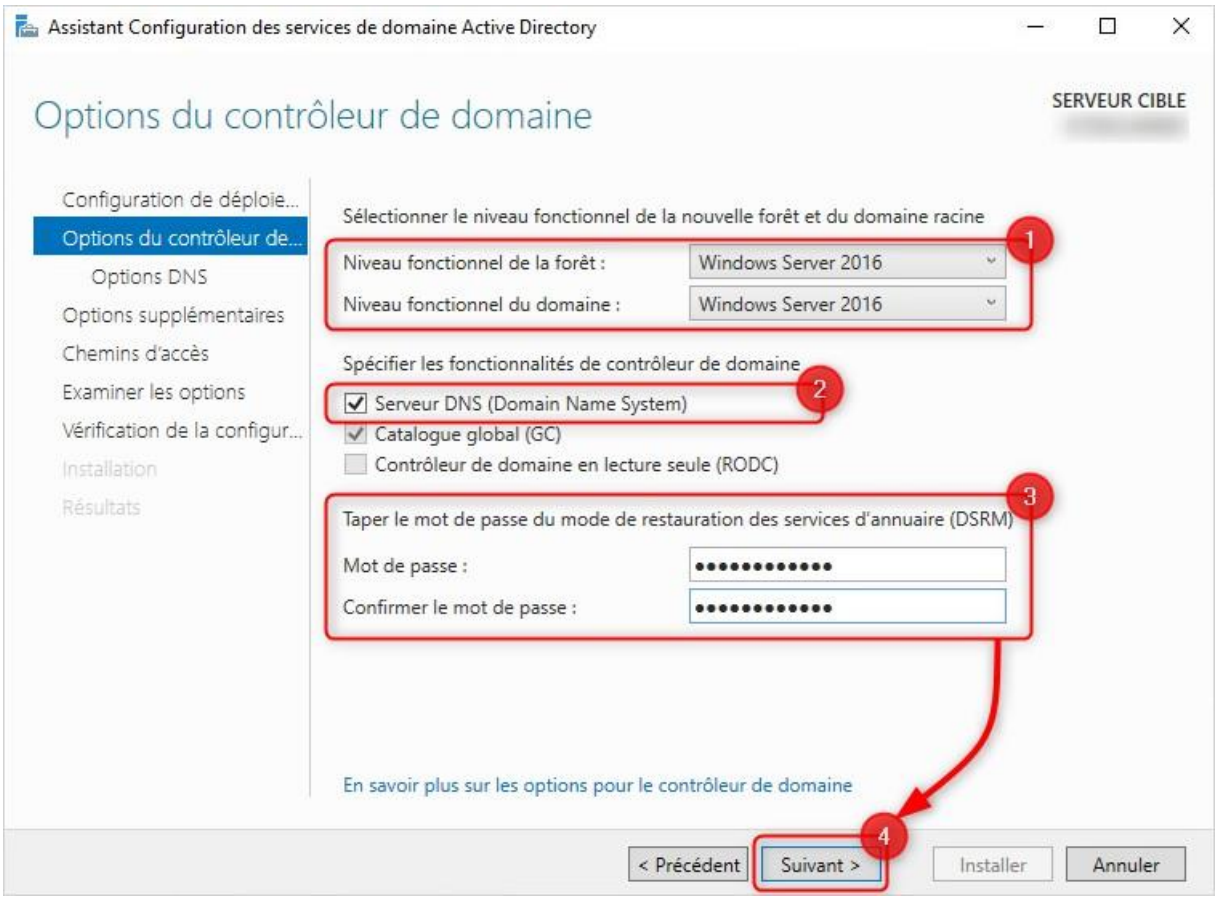

Assistant Ajout de rôles et de fonctionnalités
Sélectionner le type d'installation
SERVEUR DE DESTINATION
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats
Sélectionnez le type d'installation. Vous pouvez installer des rôles et des fonctionnalités sur un ordinateur physique ou virtuel en fonctionnement, ou sur un disque dur virtuel hors connexion.
Installation basée sur un rôle ou une fonctionnalité
Configurez un serveur unique en ajoutant des rôles, des services de rôle et des fonctionnalités.
Installation des services Bureau à distance
Installez les services de rôle nécessaires à l'infrastructure VDI (Virtual Desktop Infrastructure) pour déployer des bureaux basés sur des ordinateurs virtuels ou sur des sessions.
< Précédent
Suivant >
Installer
Annuler


Assistant Ajout de rôles et de fonctionnalités
Sélectionner le serveur de destination
SERVEUR DE DESTINATION
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats
Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.
Sélectionner un serveur du pool de serveurs
Sélectionner un disque dur virtuel
Pool de serveurs
Filtre :
Nom
Adresse IP
Système d'exploitation
Microsoft Windows Server 2022 Datacenter
1 ordinateur(s) trouvé(s)
Cette page présente les serveurs qui exécutent Windows Server 2012 ou une version ultérieure et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors connexion et les serveurs nouvellement ajoutés dont la collecte de données est toujours incomplète ne sont pas répertoriés.
< Précédent
Suivant >
Installer
Annuler

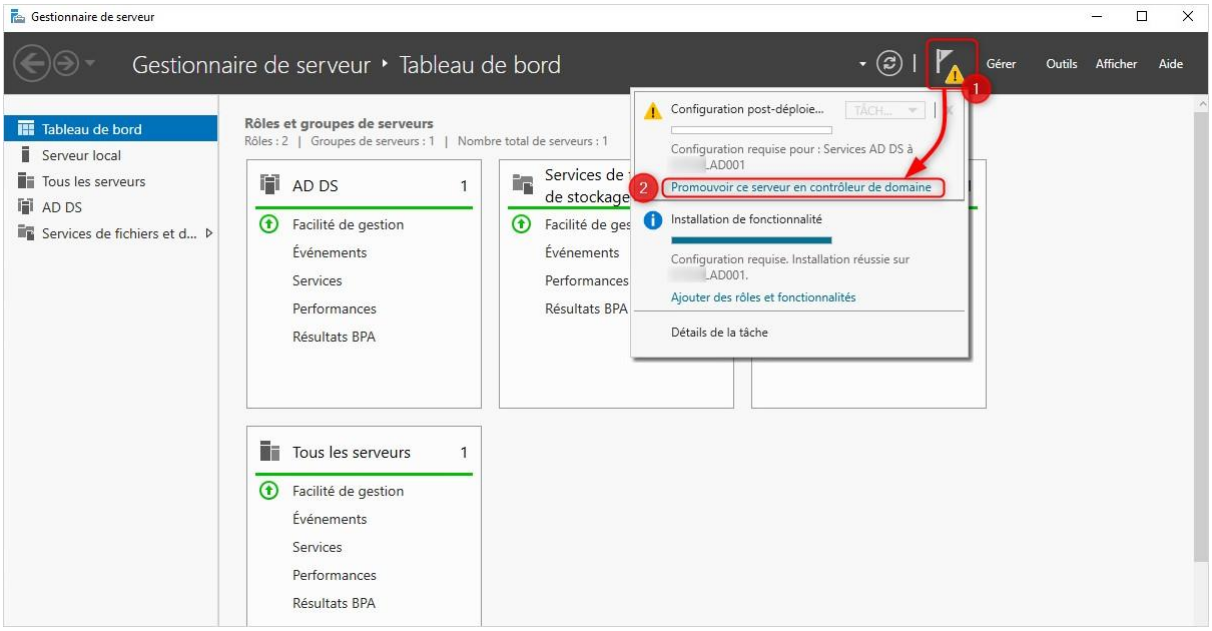

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats
Cet Assistant permet d'installer des rôles, des services de rôle ou des fonctionnalités. Vous devez déterminer les rôles, services de rôle ou fonctionnalités à installer en fonction des besoins informatiques de votre organisation, tels que le partage de documents ou l'hébergement d'un site Web.
Pour supprimer des rôles, des services de rôle ou des fonctionnalités :
Démarrer l'Assistant de Suppression de rôles et de fonctionnalités
Avant de continuer, vérifiez que les travaux suivants ont été effectués :
• Le compte d'administrateur possède un mot de passe fort
• Les paramètres réseau, comme les adresses IP statiques, sont configurés
• Les dernières mises à jour de sécurité de Windows Update sont installées
Si vous devez vérifier que l'une des conditions préalables ci-dessus a été satisfaite, fermez l'Assistant, exécutez les étapes, puis relancez l'Assistant.
Cliquez sur Suivant pour continuer.
Ignorer cette page par défaut
< Précédent
Suivant >
Installer
Annuler

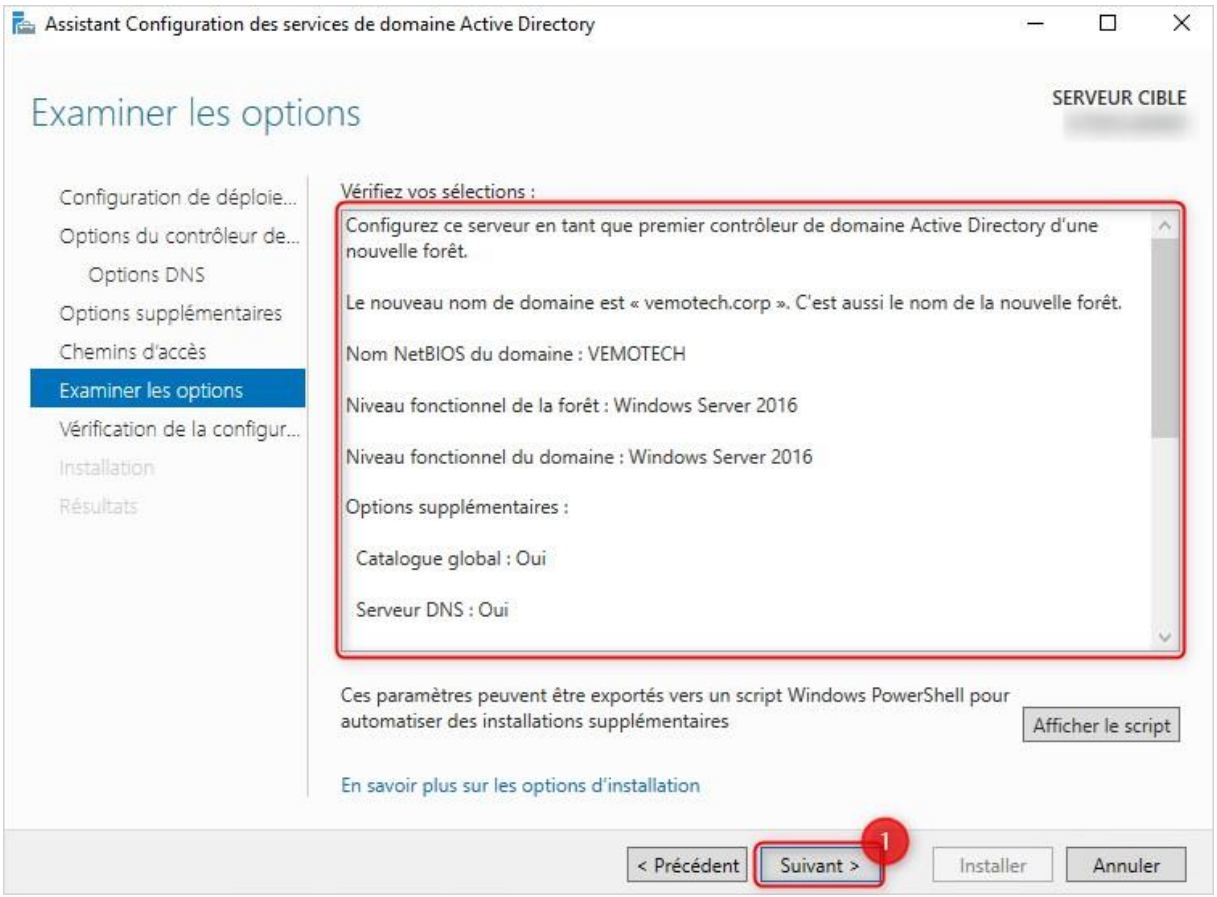

Assistant Ajout de rôles et de fonctionnalités
Sélectionner des rôles de serveurs
SERVEUR DE DESTINATION
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats
Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.
Rôles
Accès à distance
Attestation d'intégrité de l'appareil
Contrôleur de réseau
Hyper-V
Serveur de télécopie
Serveur DHCP
Serveur DNS
Serveur Web (IIS)
Service Guardian hôte
Services AD DS
Services AD LDS (Active Directory Lightweight Dire
Services AD RMS (Active Directory Rights Manage
Services Bureau à distance
Services d'activation en volume
Services d'impression et de numérisation de docu
Services de certificats Active Directory
Services de fédération Active Directory (AD FS)
Services de fichiers et de stockage (1 sur 12 install
Services de stratégie et d'accès réseau
1
Description
Les services de domaine Active Directory (AD DS) stockent des informations à propos des objets sur le réseau et rendent ces informations disponibles pour les utilisateurs et les administrateurs du réseau. Les services AD DS utilisent les contrôleurs de domaine pour donner aux utilisateurs du réseau un accès aux ressources autorisées n'importe où sur le réseau via un processus d'ouverture de session unique.
< Précédent
Suivant >
Installer
Annuler

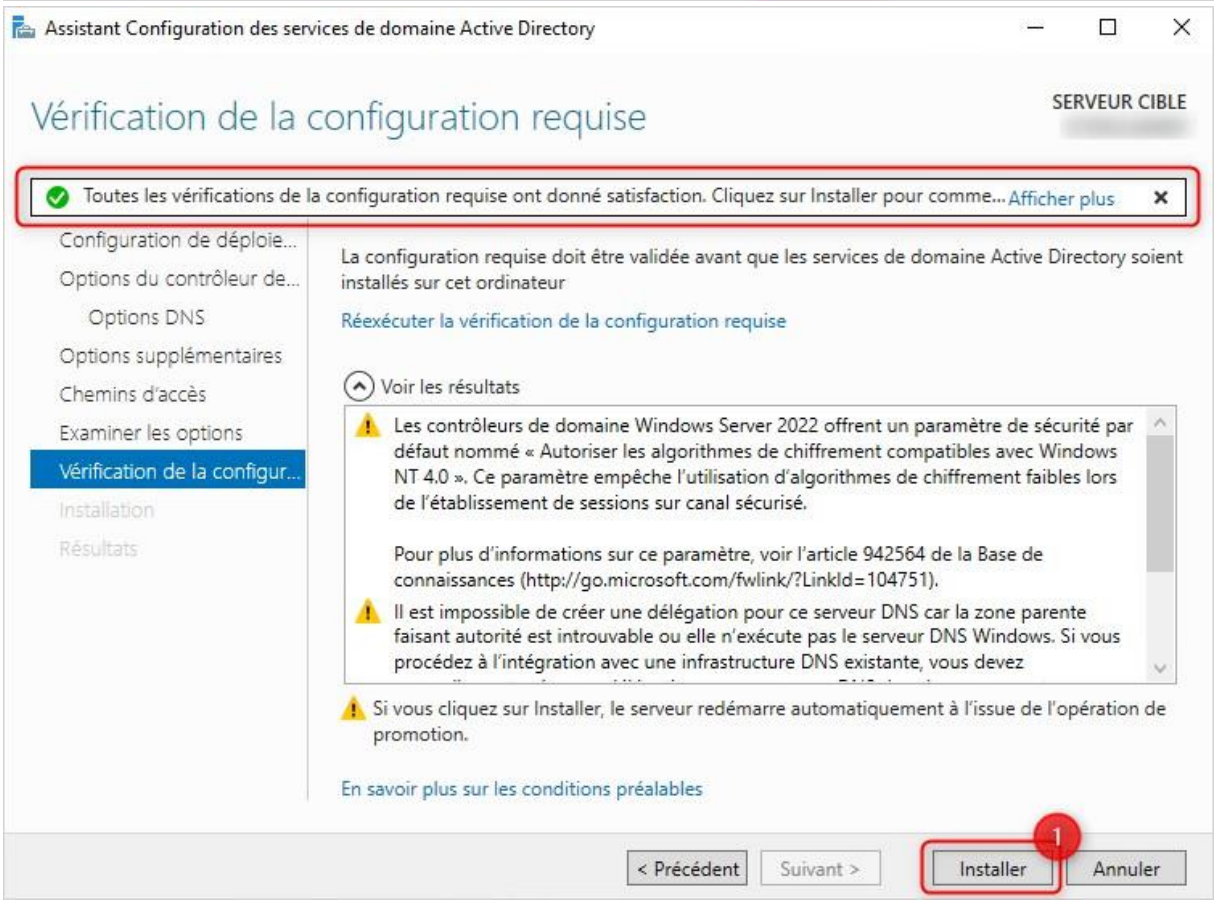

Assistant Ajout de rôles et de fonctionnalités
Sélectionner des
SERVEUR DE DESTINATION
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats
Assistant Ajout de rôles et de fonctionnalités
Ajouter les fonctionnalités requises pour Services AD DS ?
Vous ne pouvez pas installer Services AD DS sauf si les services de rôle ou les fonctionnalités suivants sont également installés.
[Outils] Gestion de stratégie de groupe
Outils d'administration de serveur distant
Outils d'administration de rôles
Outils AD DS et AD LDS
Module Active Directory pour Windows PowerShell
Outils AD DS
[Outils] Centre d'administration Active Directory
[Outils] Composants logiciels enfichables et outils e
1
Inclure les outils de gestion (si applicable)
Ajouter des fonctionnalités
Annuler
2
< Précédent
Suivant >
Installer
Annuler



Après avoir installé l'active directory, on promeut la VM en contrôleur de domaine, en l'occurrence dans mon cas il ne contrôlera que le VLAN Test qui m'a été attribué.




Assistant Configuration des services de domaine Active Directory
Examiner les options
SERVEUR CIBLE
Configuration de déploie...
Options du contrôleur de...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats
Vérifiez vos sélections :
Configurez ce serveur en tant que premier contrôleur de domaine Active Directory d'une nouvelle forêt.
Le nouveau nom de domaine est « vemotech.corp ». C'est aussi le nom de la nouvelle forêt.
Nom NetBIOS du domaine : VEMOTECH
Niveau fonctionnel de la forêt : Windows Server 2016
Niveau fonctionnel du domaine : Windows Server 2016
Options supplémentaires :
Catalogue global : Oui
Serveur DNS : Oui
Ces paramètres peuvent être exportés vers un script Windows PowerShell pour automatiser des installations supplémentaires
Afficher le script
En savoir plus sur les options d'installation
1
< Précédent
Suivant >
Installer
Annuler


Assistant Configuration des services de domaine Active Directory
Vérification de la configuration requise
SERVEUR CIBLE
Toutes les vérifications de la configuration requise ont donné satisfaction. Cliquez sur Installer pour comme... Afficher plus
Configuration de déploie...
Options du contrôleur de...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats
La configuration requise doit être validée avant que les services de domaine Active Directory soient installés sur cet ordinateur
Réexécuter la vérification de la configuration requise
Voir les résultats
Les contrôleurs de domaine Windows Server 2022 offrent un paramètre de sécurité par défaut nommé « Autoriser les algorithmes de chiffrement compatibles avec Windows NT 4.0 ». Ce paramètre empêche l'utilisation d'algorithmes de chiffrement faibles lors de l'établissement de sessions sur canal sécurisé.
Pour plus d'informations sur ce paramètre, voir l'article 942564 de la Base de connaissances (http://go.microsoft.com/fwlink/?LinkId=104751).
Il est impossible de créer une délégation pour ce serveur DNS car la zone parente faisant autorité est introuvable ou elle n'exécute pas le serveur DNS Windows. Si vous procédez à l'intégration avec une infrastructure DNS existante, vous devez
Si vous cliquez sur Installer, le serveur redémarre automatiquement à l'issue de l'opération de promotion.
En savoir plus sur les conditions préalables
1
< Précédent
Suivant >
Installer
Annuler

Installation de NPS :

J'installe NPS (Network policy server) pour qu'il joue le rôle de contrôleur d'accès : NPS permet d'appliquer des stratégies d'accès réseau, et lorsque configuré en tant que radius de gérer de manière centralisée l'authentification, autorisation et la comptabilité de l'accès réseau (AAA).

Le logiciel NPS (Network Policy Server) de Microsoft est un composant de Windows Server utilisé pour gérer et appliquer les politiques de réseau. Voici un petit résumé de ses principales fonctionnalités et utilisations :

Fonctionnalités principales :

1. **Serveur RADIUS** : NPS agit comme un serveur RADIUS (Remote Authentication Dial-In User Service), permettant l'authentification, l'autorisation et la comptabilisation (AAA) des connexions réseau.
2. **Contrôle d'accès réseau** : Il permet de définir et d'appliquer des politiques d'accès réseau basées sur des conditions spécifiques comme l'identité de l'utilisateur, le type de connexion, ou les propriétés du client.
3. **Authentification forte** : NPS peut intégrer des méthodes d'authentification forte, comme l'utilisation de certificats ou de cartes à puce.
4. **Intégration avec Active Directory** : Il s'intègre étroitement avec Active Directory, permettant l'utilisation des comptes d'utilisateur et des groupes pour la gestion des accès.
5. **Surveillance et rapports** : NPS fournit des fonctionnalités de journalisation et de génération de rapports pour surveiller les tentatives de connexion et les accès réseau.

Utilisations courantes :

- **Gestion des accès VPN** : NPS est souvent utilisé pour gérer les connexions VPN (Virtual Private Network), en assurant que seuls les utilisateurs autorisés puissent accéder au réseau.
- **Wi-Fi sécurisé** : Il est utilisé pour sécuriser l'accès aux réseaux Wi-Fi d'entreprise, en configurant des points d'accès sans fil pour utiliser le protocole RADIUS pour l'authentification.
- **Contrôle des accès basé sur les rôles** : Les administrateurs peuvent définir des politiques de réseau qui limitent l'accès à certaines ressources en fonction des rôles des utilisateurs dans l'organisation.

Avantages :

- **Sécurité renforcée** : En utilisant des politiques d'accès réseau et des méthodes d'authentification robustes, NPS aide à protéger les ressources réseau contre les accès non autorisés.
- **Centralisation de la gestion** : Il permet de centraliser la gestion des politiques d'accès, simplifiant ainsi l'administration réseau.
- **Flexibilité** : NPS offre une grande flexibilité dans la définition des politiques d'accès réseau, permettant de répondre à divers besoins et scénarios d'entreprise.

En résumé, le Network Policy Server de Microsoft est un outil puissant pour gérer l'accès et la sécurité des réseaux, particulièrement utile dans les environnements d'entreprise où l'intégration avec Active Directory et la gestion centralisée des politiques sont essentielles. (voir interface figure 3)

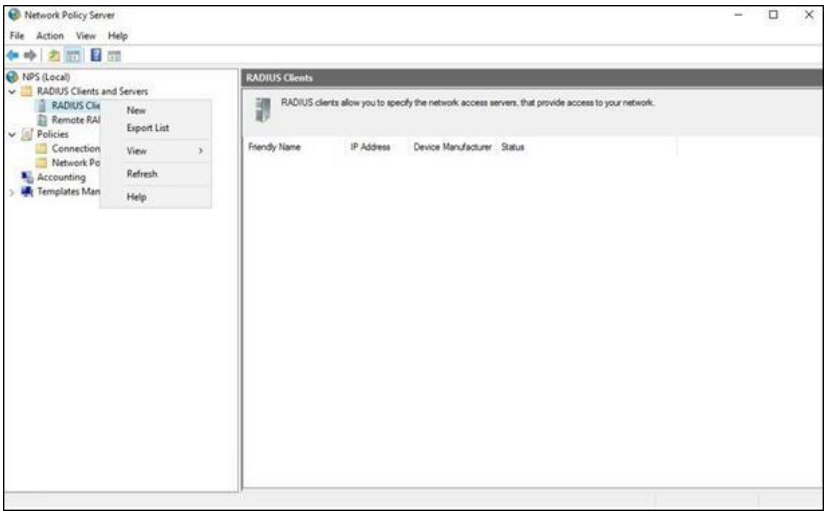


Figure 3 : Interface du logiciel NPS

On active le client RADIUS, on entre l'adresse IP du Client, et on précise l'adresse IP du point d'accès réseau. (Figure 4)

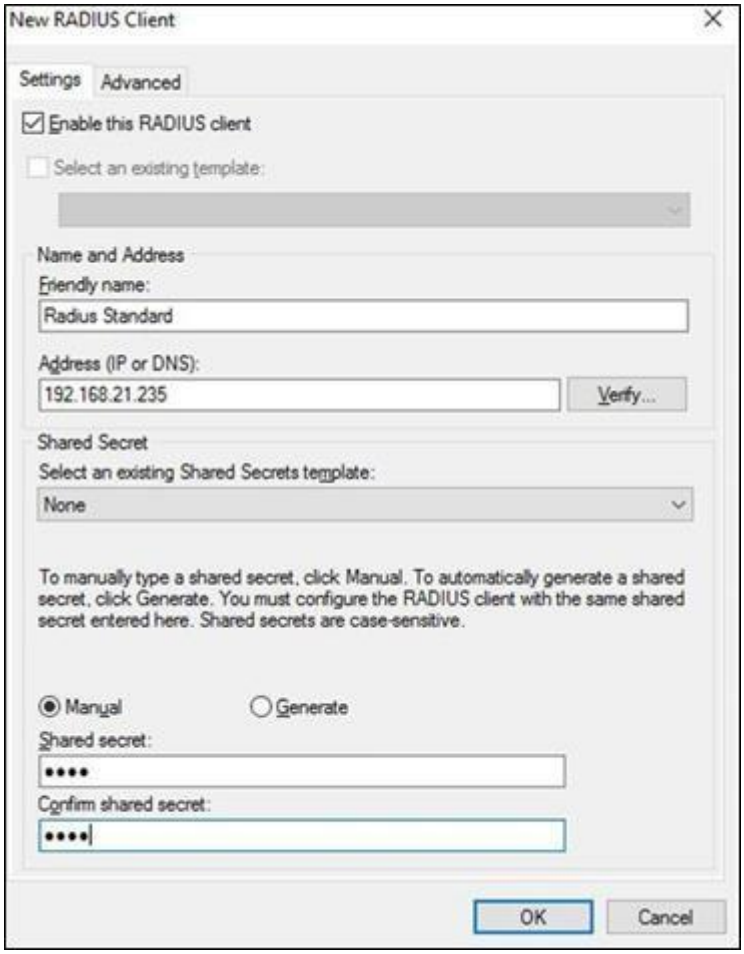


Figure 4 : Interface d'ajout de client NPS

Création de politiques de sécurité :

On crée d'abord un groupe test, et un utilisateur test dans le gestionnaire « utilisateurs et ordinateurs active directory ».

En créant la stratégie de réseau NPS, dans la section condition on mets comme condition l'appartenance au groupe crée plus tôt, ce qui fera que l'authentification par radius sera appliquée aux utilisateurs du groupe (en somme au groupe lui-même).

Le système AAA radius fonctionne avec un serveur radius, un client radius et un utilisateur final. L'utilisateur final communique avec le client radius, ce-dernier lui communique avec le serveur radius qui autorise ou refuse la connexion.

Borne Wifi :

J'ai utilisé une borne wifi Cisco WAP-371, qui était déjà configurée. J'ai donc dû faire un « factory reset », en pressant sur le bouton de reset pendant une dizaine de secondes. [voir figure 5] (Cela va donc réinitialiser la configuration de la borne)

Figure 5 : Cisco WAP371 (bouton de reboot entouré)

Par la suite je me suis connecté a l'adresse 192.168.1.245 (l'adresse par default), et j'ai modifié l'adresse IP du port management pour la mettre dans le VLAN en 172.17.199.15.Pour mettre en place la borne WiFi j'ai du déclarer le Vlan dans lequel j'ai travaillé (le vlan 199 ou vlan de test) sur les switchs du réseau, j'ai donc découvert les switchs ALCATELS sur lesquelles je n'ai jamais eu l'occasion de travailler auparavant.

Packetfence :

En utilisant NPS avec l'active directory, j'ai remarqué que je pouvais utiliser l'active directory comme source d'authentification, cependant je n'ai pas trouvé le moyen de mettre en place l'authentification mac à l'aide du même logiciel. De plus, même s'il existe des façons de contourner ce problème, je cherche une manière brève de mettre en place l'authentification par adresse MAC, alors que les solutions possibles étaient relativement longues, ne permettant pas de les appliquer à une plus grande échelle.

J'ai donc cherché des alternatives à Windows NPS, et je les ai comparées dans un tableau Excel sur plusieurs critères, notamment : la flexibilité, l'intégration avec d'autres systèmes, et le cout. [voir figure 6]

Logiciel \ critéres	Type	fléxibilié	Intégration avec d'autres systémes	Facilité de déploiement et d'utilisation	Coût
FREERADIUS	opensource	Très flexible et hautement personnalisable	integration possible avec des plugins et extensions	déploiement plus complexe (configuration et gestion manuelle)	Gratuit, mais peut nécessiter des ressources pour la configuration et la maintenance
Cisco ISE	propriétaire de cisco	Propose des fonctionnalités avancées mais moins flexible	s'intégre bien avec des produits cisco	interface "user friendly"	coût d'achat et coûts de licence associés
Aruba Clearpass	propriétaire d'Aruba networks	equilibré entre flexibilité et personalisation	Intégration native avec les équipements Aruba et peut être étendu pour prendre en charge d'autres équipements réseau	déploiement relativement faciel pour les environnements aruba	coût d'achat et coûts de licence associés
Packetfence	opensource	flexibe et personalisable	Offre une intégration avec de nombreux équipements réseau et systèmes d'authentification	deploiment relativement simple (interface et guides)	Gratuit, mais peut nécessiter des ressources pour la configuration et la maintenance
OpenNAC	opensource	très adaptable et peut être personnalisé selon les besoins spécifiques.	peut être intégré avec divers systèmes grâce à son architecture open-source	déploiement plus complexe (configuration et gestion manuelle)	Gratuit, mais peut nécessiter des ressources pour la configuration et la maintenance

Figure 6 : Tableau de comparaison des alternatives a NPS

Après une entrevue technique avec mon tuteur, nous avons choisi d'opter pour Packetfence, un logiciel open source qui ferait office de contrôleur d'accès.

J'ai donc eu à créer une autre VM pour cette fois une VM Debian. Pour ce faire, j'ai téléchargé depuis le site officiel de packetfence une image ISO du contrôleur d'accès.

Celle-ci installe plusieurs éléments :

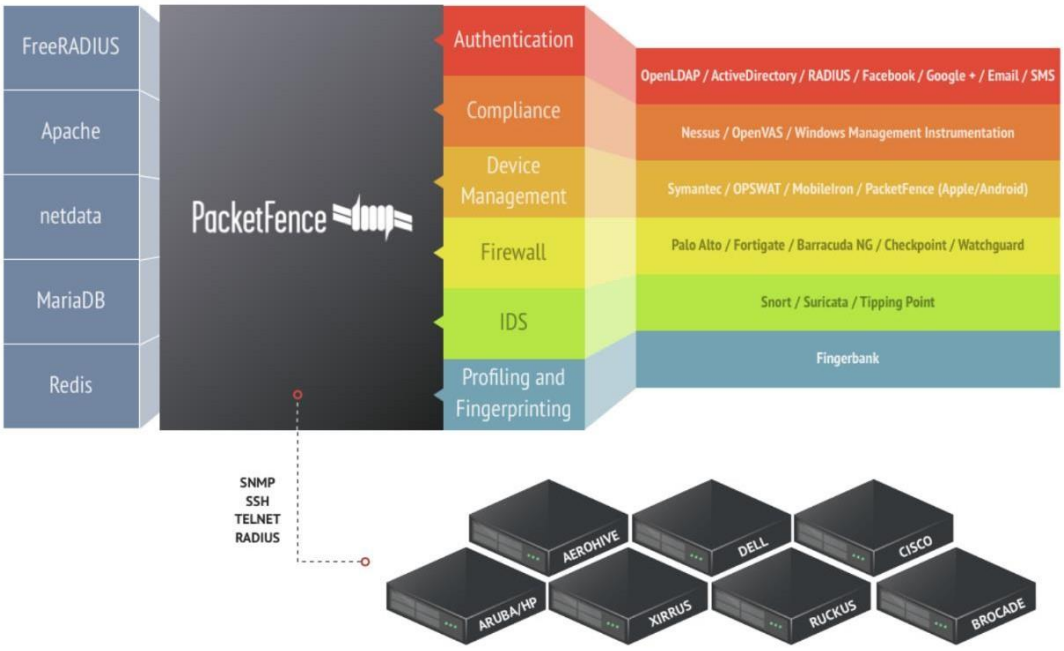


Figure 7 : Structure générale de NPS

Notamment Free radius pour l'authentification radius.

Par la suite, sur packetfence je me suis appuyé sur la documentation officielle pour établir un lien avec la borne et l'active directory.

Dans un premier temps, il s'agissait de lier packetfence a l'active directory. J'ai créé un compte Machine pour que packetfence puisse se connecter à l'active directory.

Il s'agissait donc de mettre une machine linux dans un active directory ce qui s'est avéré relativement compliqué.

En effet sur packetfence, je devais renseigner ce champ :

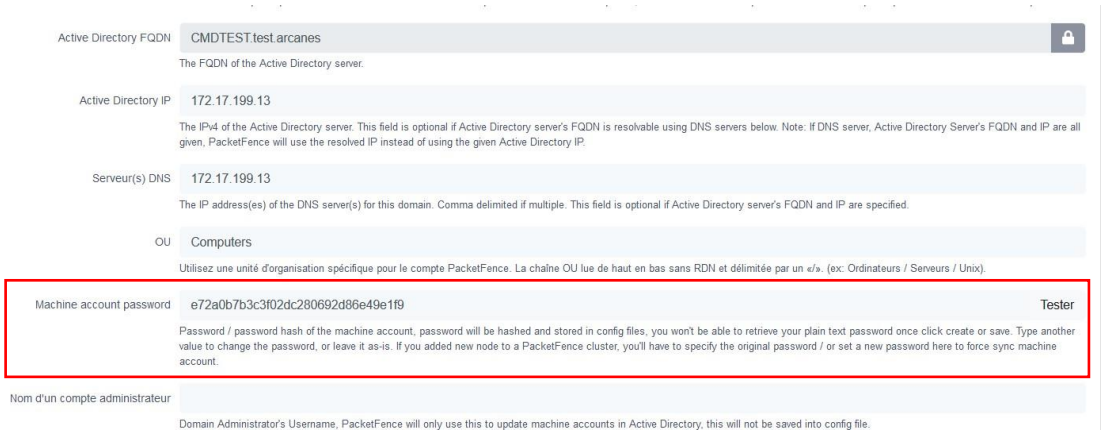


Figure 8 : Interface de création de l'active directory dans packetfence

Ce champ correspond donc au mot de passe du compte machine préalablement crée. Cependant, sur l'active directory Windows, lors de la création d'un compte machine, on ne peut pas modifier le mot de passe.

J'ai donc cherché un moyen externe de faire ainsi, ce qui m'a mené à utiliser un programme PowerShell.

Après l'utilisation du script, je suis donc arrivé à modifier le mot de passe du compte machine et à lier packetfence a l'active directory.

Figure 9 : Paramètres packetfence a configurer

Après avoir lié le domaine, j'ai dû créer une source d'authentification (Figure 10) prenant comme paramètre l'active directory.

Les sources d'authentification permettent de mettre en place des règles, des conditions et des actions. (figure 11),

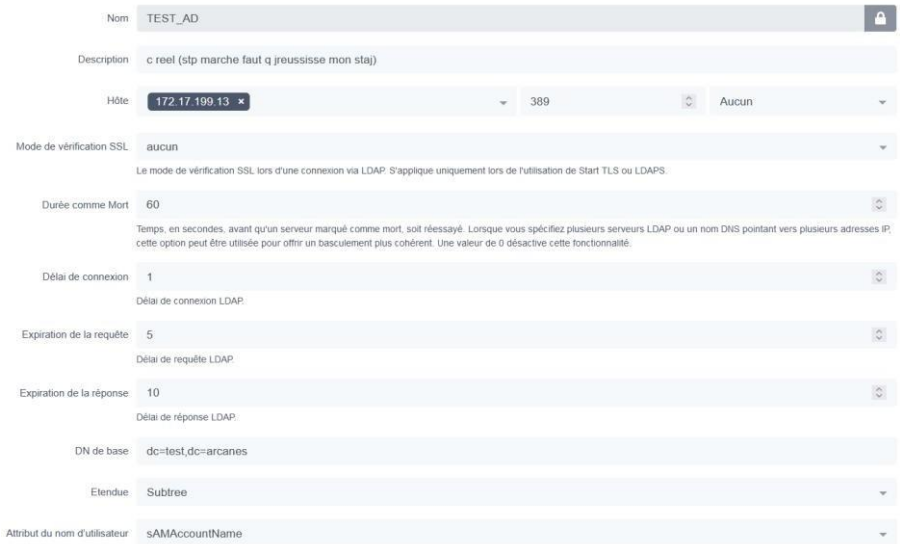


Figure 10 : Source d'authentification

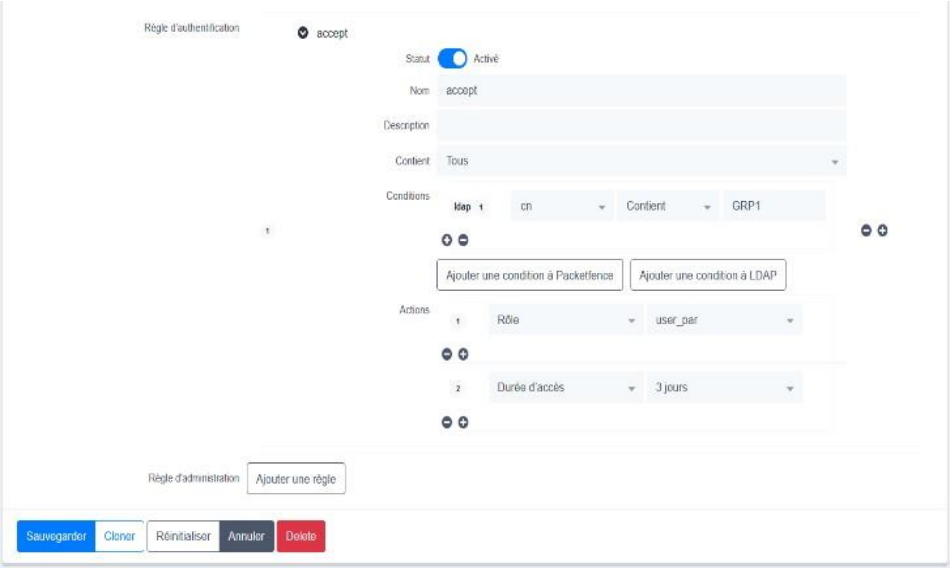


Figure 11 : Filtres de la source d'authentification

L'étape qui suit est la déclaration de la borne dans la section « commutateurs ». Pour cefaire, il a suffi de créer un nouvel appareil ensuite de lui associer l'adresse IP de la borne, soit172.17.199.15.

Après la déclaration de la borne, il a fallu créer un profil de connexion que j'ai nommé « test_AD2 ». Le profil de connexion est ce qui permet d'appliquer et de filtrer en utilisant la source d'authentification que j'ai créé plutôt.

Les paramètres de la configuration sont détaillés dans l'annexe avec des captures d'écran.

Pour assigner des VLANs selon les utilisateurs, packetfence utilise des « rôles ». Cependant, Il est expliqué dans la documentation packetfence que le logiciel n'est pas compatible avec tous les modèles de switchs. Après plusieurs tests, j'ai remarqué que les rôles ne s'assignaient pas.

J'en ai donc conclu que même si la connexion par active directory fonctionnait, Packetfence n'est pas totalement compatible avec mon modèle de switch.

Mon tuteur m'a relancé sur NPS.

Sur NPS, j'ai entrepris une approche légèrement différente de la précédente :

Désormais, je n'avais pas un, mais quatre clients NPS, qui correspondent aux quatre bornes de l'architecture réseau d'arcanes.

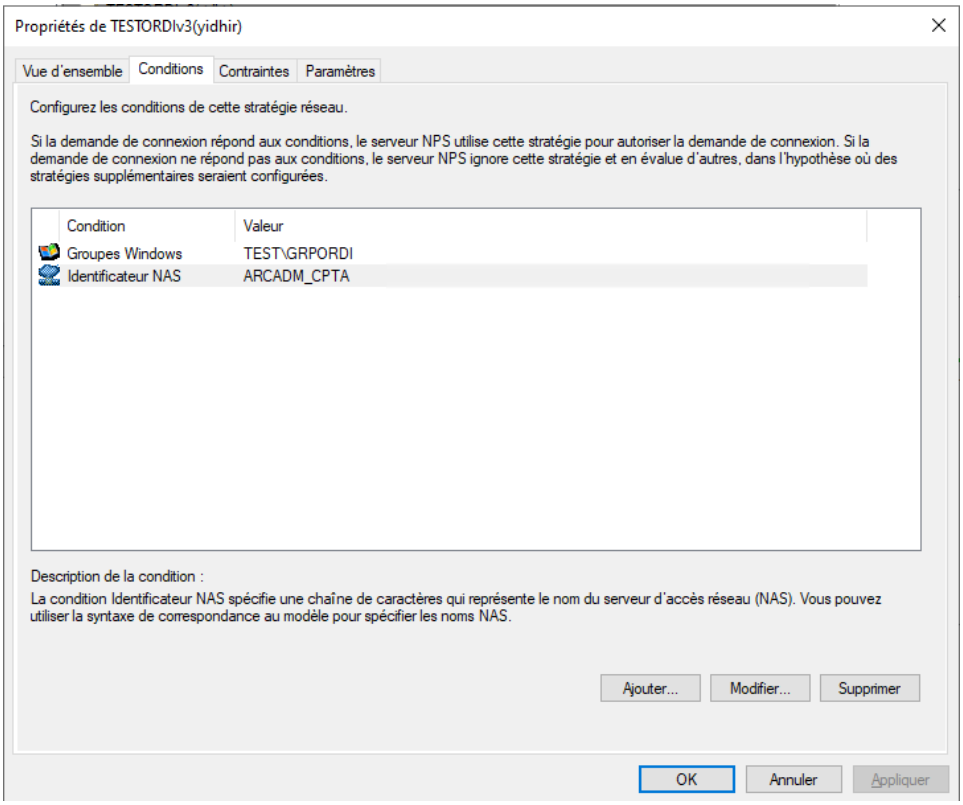


Figure 12 : Filtres NPS

L'identificateur NAS correspond à un identificateur qui est paramétré dans les bornes WIFI. Chaque identifiant NAS permettra ainsi de connecter les utilisateurs aux réseaux leur correspondant.

Pour assurer la connexion entre NPS et le borne, j'ai eu recourt à des certificats de connexion.

Certificats et autorités de certification :

Pour assurer la connexion, on dispose sur la machine de l'active directory d'une autorité de certification.

L'authentification par certificats utilise des certificats numériques émis par L'Autorité de Certification (CA) pour vérifier l'identité des utilisateurs ou des dispositifs. Le processus commence par l'émission d'un certificat contenant des informations sur le propriétaire et une clé publique, signé par la CA. Lors de l'authentification, l'utilisateur envoie son certificat au serveur, qui vérifie sa validité en confirmant la signature de la CA, l'expiration et l'absence de révocation du certificat. Si le certificat est validé, le serveur chiffre un message avec la clé publique du certificat, que l'utilisateur déchiffre avec sa clé privée, prouvant ainsi son identité. Ce mécanisme est couramment utilisé dans les communications sécurisées sur Internet, comme HTTPS et les VPN.

Dans les certificats ordinateurs, section Personnel > Certificats > on retrouve les certificats ordinateurs de la machine. (voir figure 13)

On retrouve dans la section suivante (Autorité de certification racine) les certificats de « confiance ».

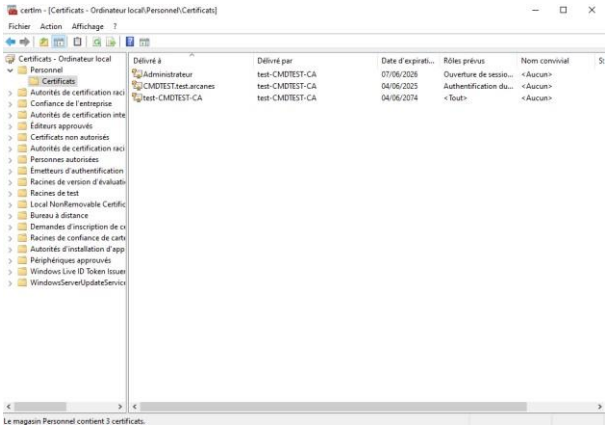


Figure 13 : Autorité de certification

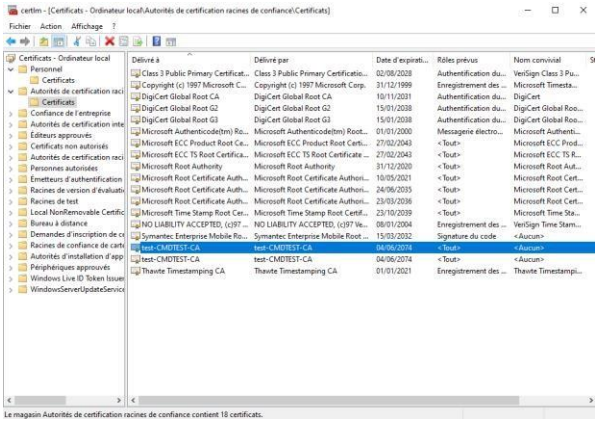


Figure 14 : Présence du Certificat

Il est impératif que le certificat de l'émetteur soit placé dans les autorités de certification racines (voir figure 14), sinon la connexion ne sera pas possible étant donné que le certificat ne sera pas validé.

Bilan

Durant mon stage de deux mois et demi, j'ai eu l'opportunité de travailler sur divers aspects des technologies de l'information, notamment la gestion de serveurs, la virtualisation, et l'intégration de systèmes. Ce stage a été une expérience enrichissante, me permettant de développer des compétences techniques précises et de mieux comprendre les environnements informatiques complexes.

1. Fonctionnement d'un Serveur RADIUS : J'ai commencé par me familiariser avec le fonctionnement des serveurs RADIUS (Remote Authentication Dial-In User Service). Ces serveurs jouent un rôle crucial dans l'authentification, l'autorisation et la gestion des comptes pour les utilisateurs se connectant à un réseau. J'ai appris à configurer un serveur RADIUS, à gérer les demandes d'authentification et à intégrer ce service dans un réseau existant pour assurer une sécurité renforcée et une gestion centralisée des accès.

2. Virtualisation avec VMware : Ensuite, j'ai pris connaissance et utilisé le logiciel de virtualisation VMware. La virtualisation est une compétence essentielle dans l'administration des systèmes modernes. J'ai consolidé mes connaissances en termes de création et gestion des machines virtuelles, optimisation des performances des serveurs virtuels et j'ai appris à utiliser les outils de gestion de VMware pour surveiller et maintenir un environnement virtualisé.

3. Microsoft NPS : J'ai approfondi mes connaissances sur Microsoft Network Policy Server (NPS). Ce rôle de serveur permet de créer et de faire appliquer des politiques de réseau pour les demandes d'authentification et d'autorisation. J'ai appris à configurer NPS pour travailler avec RADIUS, à créer des politiques de réseau et de connexion, et à gérer les accès réseau de manière sécurisée.

4. Installation et Utilisation de PacketFence : J'ai appris à installer et utiliser PacketFence, une solution de gestion d'accès au réseau (NAC - Network Access Control). PacketFence offre des fonctionnalités de sécurité avancées telles que l'isolement des périphériques non conformes et la gestion des points d'accès réseau. J'ai acquis des compétences dans la configuration de PacketFence pour surveiller et contrôler l'accès au réseau, améliorer la sécurité et assurer la conformité des périphériques connectés.

5. Comptes Ordinateurs Active Directory : Dans le cadre de la gestion des comptes ordinateurs dans Active Directory, j'ai appris que ces comptes utilisent des mots de passe cryptés, non révélés aux administrateurs. Cela garantit une sécurité accrue pour les ressources réseau. J'ai également appris à gérer et dépanner les comptes ordinateurs, en comprenant les mécanismes de mot de passe et de sécurité associés.

6. Intégration d'une Machine Linux dans un Active Directory Windows : Enfin, j'ai appris à intégrer une machine Linux dans un Active Directory Windows. Cette compétence est particulièrement utile pour les environnements hybrides utilisant à la fois des systèmes Windows et Linux.

Conclusion

Ce stage de deux mois et demi a été une expérience formatrice et enrichissante, me permettant de développer une compréhension approfondie des technologies de gestion des réseaux et des systèmes informatiques. J'ai eu l'opportunité de travailler sur des projets variés, allant de la configuration de serveurs RADIUS à l'intégration de machines Linux dans un environnement Active Directory Windows. Ces expériences m'ont permis d'acquérir des compétences techniques solides et de mieux comprendre les enjeux de sécurité et de gestion des réseaux.

Travailler avec des outils tels que VMware, Microsoft NPS, et PacketFence m'a également donné une perspective précieuse sur les différentes solutions disponibles pour la virtualisation, la gestion des politiques réseau et le contrôle d'accès. J'ai particulièrement apprécié l'approche pratique de ce stage, qui m'a permis de mettre en œuvre des solutions concrètes et de voir directement les résultats de mon travail.

Les connaissances et compétences acquises durant ce stage seront des atouts précieux pour ma carrière future. Je tiens à remercier mon équipe et mes superviseurs pour leur soutien et leurs conseils tout au long de cette période. Leur expertise et leur disponibilité ont grandement contribué à la réussite de ce stage.

En conclusion, ce stage m'a non seulement permis de renforcer mes compétences techniques, mais aussi de mieux comprendre le fonctionnement des environnements informatiques complexes et les meilleures pratiques en matière de sécurité et de gestion des réseaux. Je suis désormais mieux préparé pour relever les défis futurs et contribuer efficacement à des projets dans le domaine des technologies de l'information.

Bibliographie

Documentation PacketFence : https://www.packetfence.org/doc/PacketFence_Installation_Guide.html

Documentation officielle Microsoft : https://learn.microsoft.com/fr-fr/windows-server/networking/technologies/nps/nps-top

TechExpert tips : https://techexpert.tips/fr/powershell-fr/powershell-obtenez-des-informations-sur-les-ordinateurs-de-active-directory/

IT-connect : https://www.it-connect.fr/chapitres/recuperer-des-informations-sur-les-utilisateurs-avec-powershell/#III_Rechercher_des_utilisateurs_dans_une_OU_avec_-SearchBase

SourceForge : https://sourceforge.net/p/packetfence/mailman/message/34744600/

Narkive Archive : https://packetfence-users.narkive.com/nWxgtC2n/how-assign-reassign-vlan-based-on-ad-group-membership-or-lack-of-membership

Cisco guide : https://www.cisco.com/c/dam/en/us/td/docs/wireless/access_point/csbap/wap371/quick_guide/guide/QSG_ENGLISH.pdf

Spice Work security : https://community.spiceworks.com/t/nps-radius-works-with-win10-not-with-macintosh/774402/4

CloudRadius : https://www.cloudradius.com/how-to-setup-a-windows-radius-server/

Broadcom : https://techdocs.broadcom.com/us/en/fibre-channel-networking/fabric-os/fabric-os-administration/9-2-x/v26912536/v26753555/configuring-radius-server-support-with-windows-server-2022-nps-92x-admin.html

Arista Community Central : https://arista.my.site.com/AristaCommunity/s/article/setting-up-ad-nps-and-radius-authentication-using-windows-nps

Guide de configuration Alcatel : https://www.networklab.fr/guide-de-configuration-alcatel-switch/

PHP : https://www.php.net/manual/fr/radius.constants.attributes.php