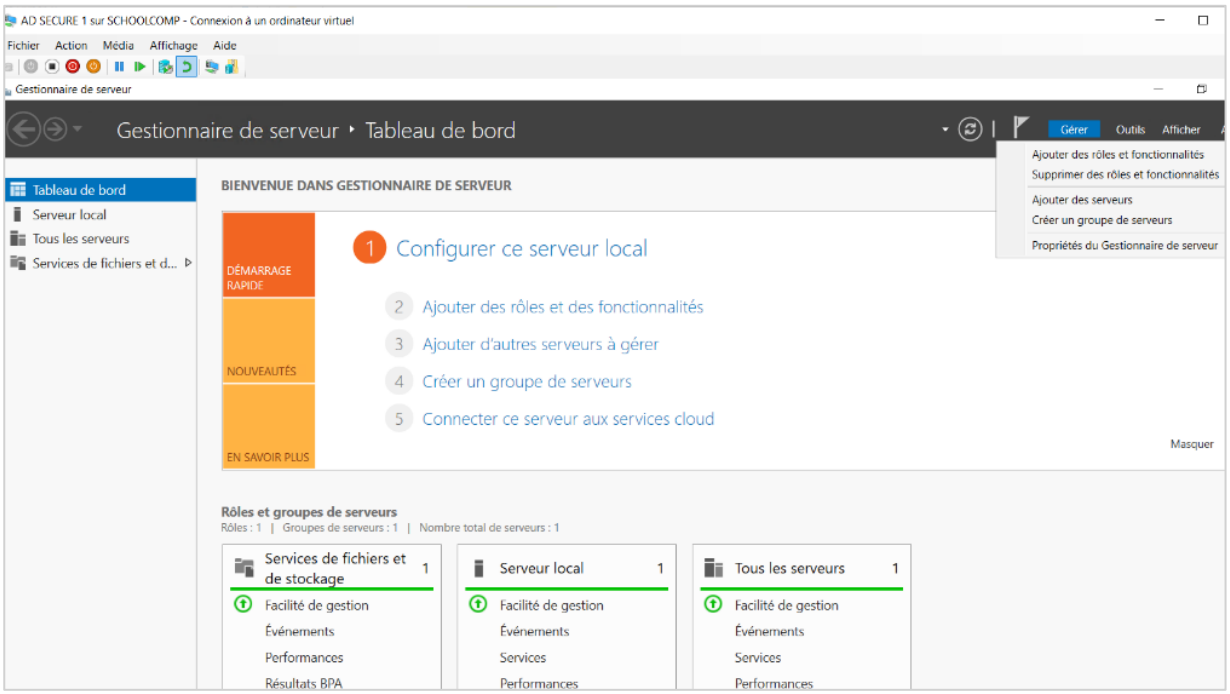
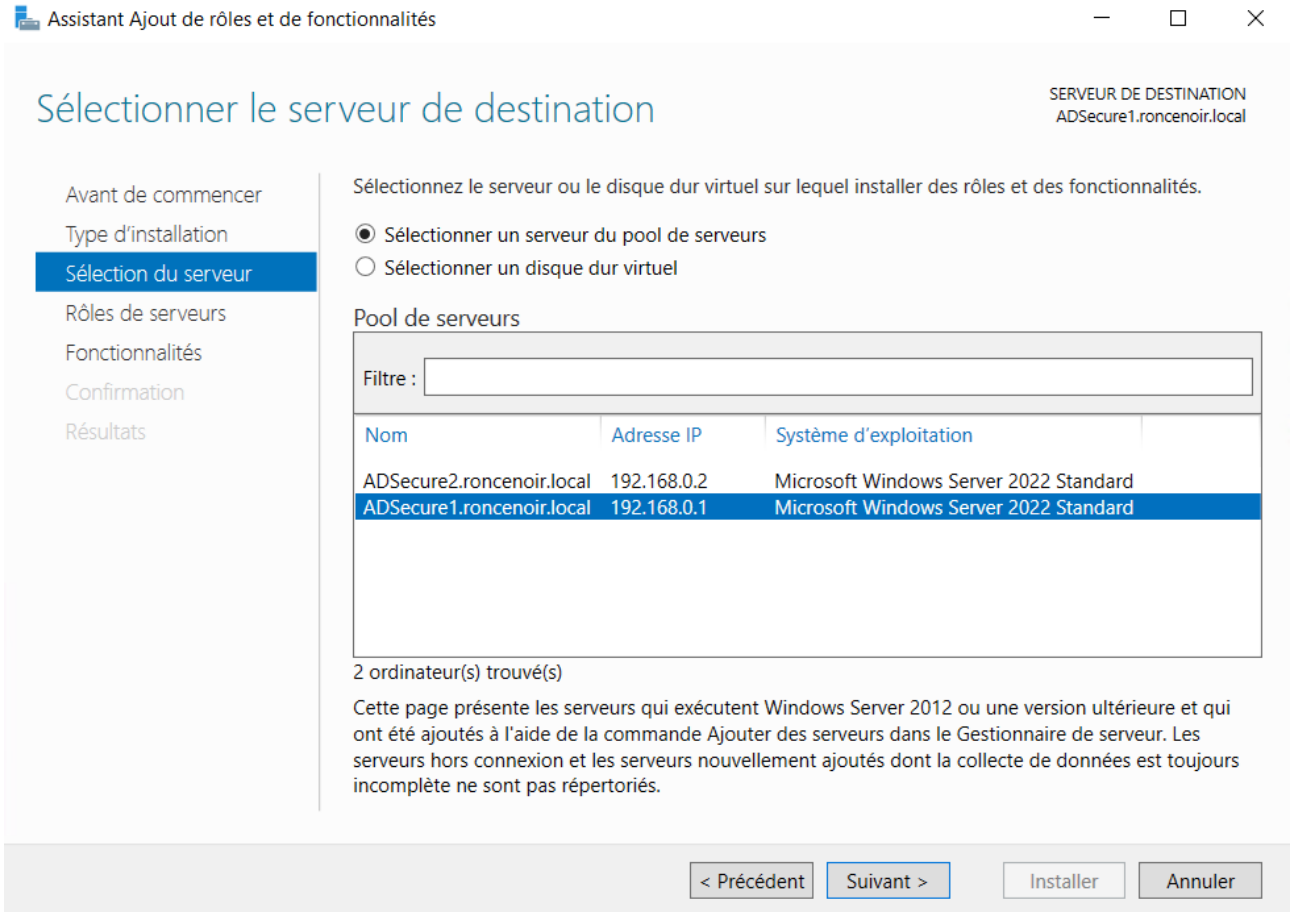
RADIUS

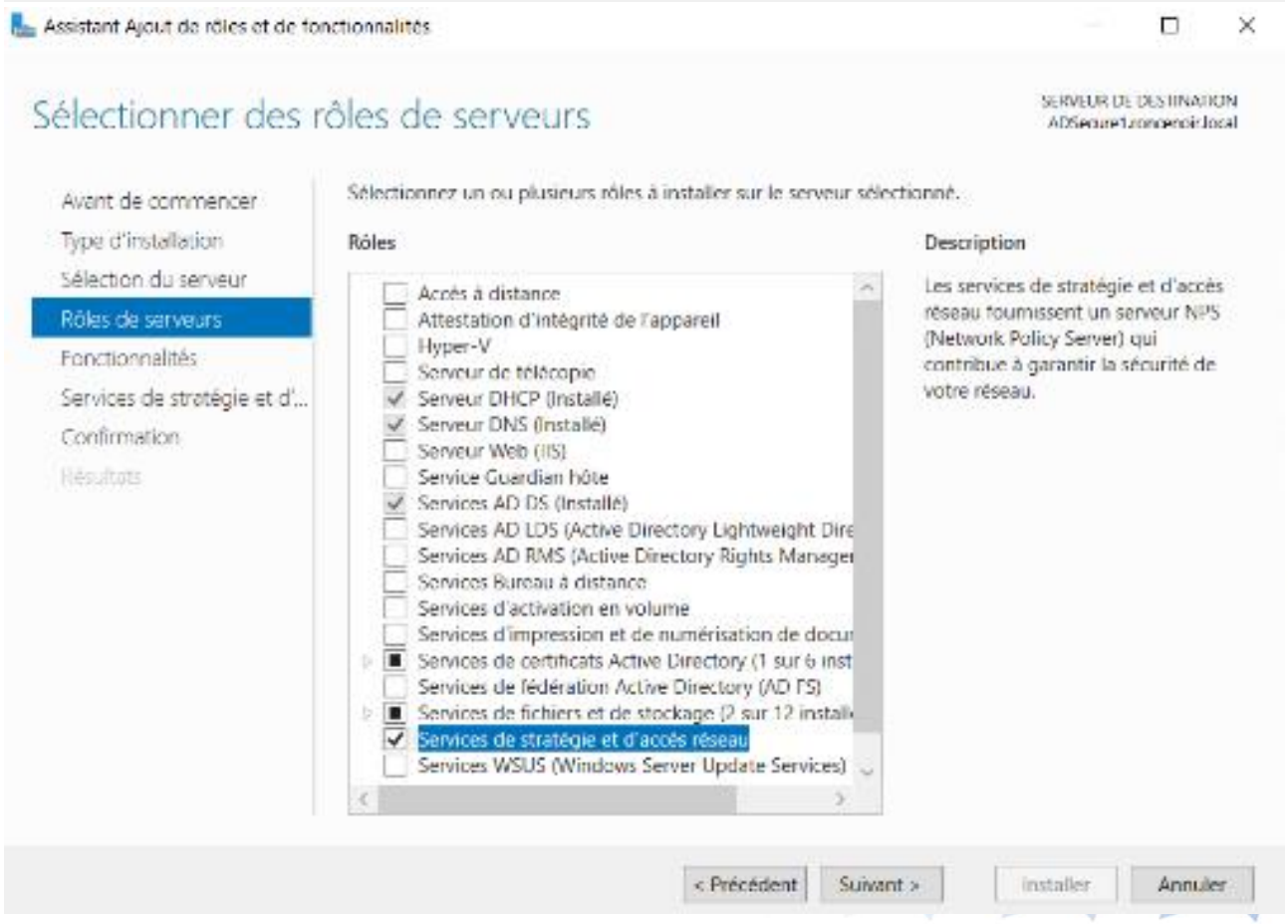
RADIUS (Remote Authentication Dial-In User Service) est un protocole d'authentification centralisé qui permet de contrôler l'accès au réseau. Dans le contexte d'une borne WiFi, comme celles de la marque Ubiquiti, RADIUS est utilisé pour authentifier les utilisateurs avant qu'ils puissent se connecter au réseau sans fil, en vérifiant leurs identifiants auprès d'un serveur central (comme FreeRADIUS ou NPS de Microsoft).

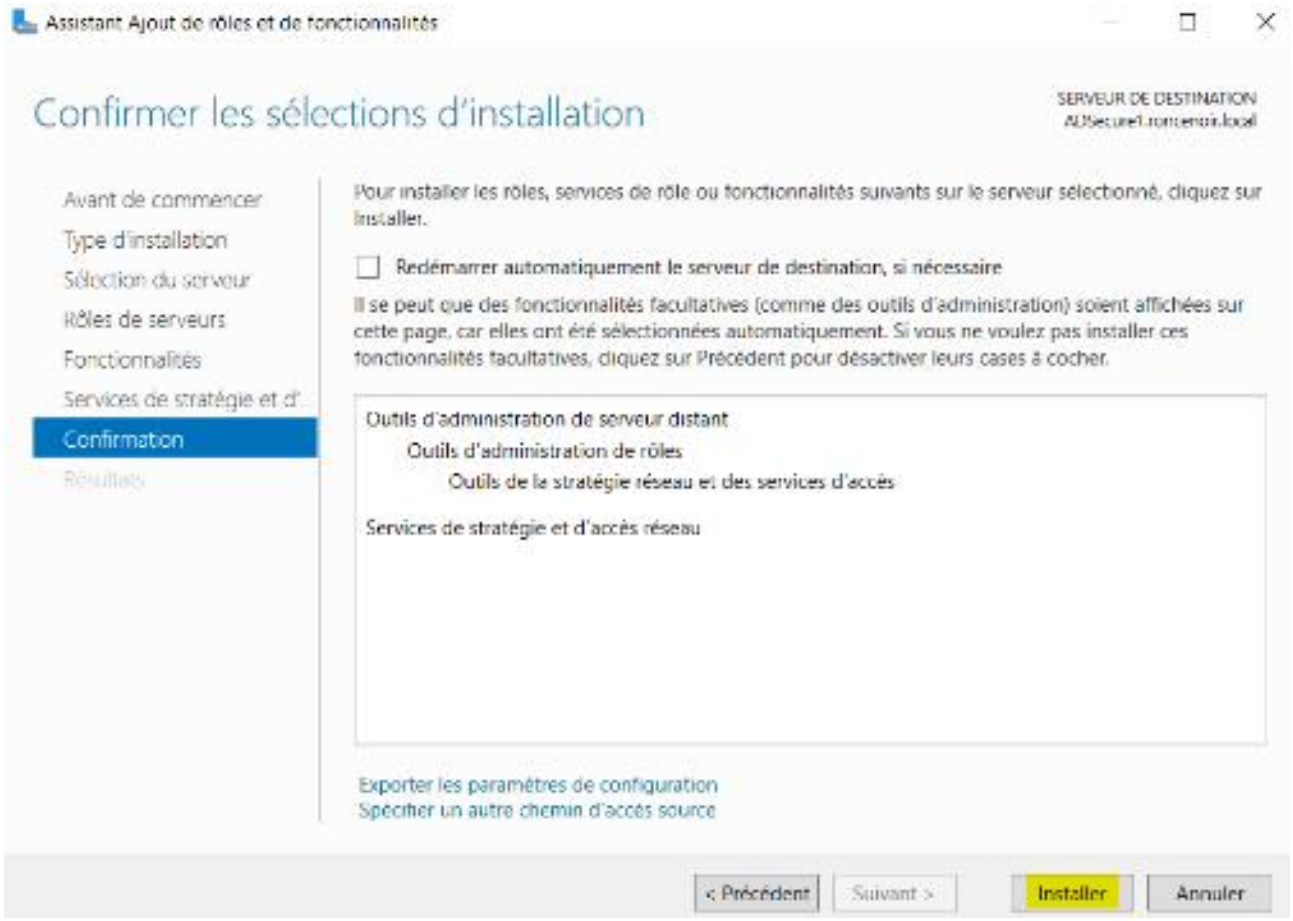
Ce mécanisme renforce la sécurité en remplaçant les mots de passe partagés (WPA2-Personal) par une authentification individuelle (WPA2-Enterprise), souvent liée à un annuaire tel qu'Active Directory.

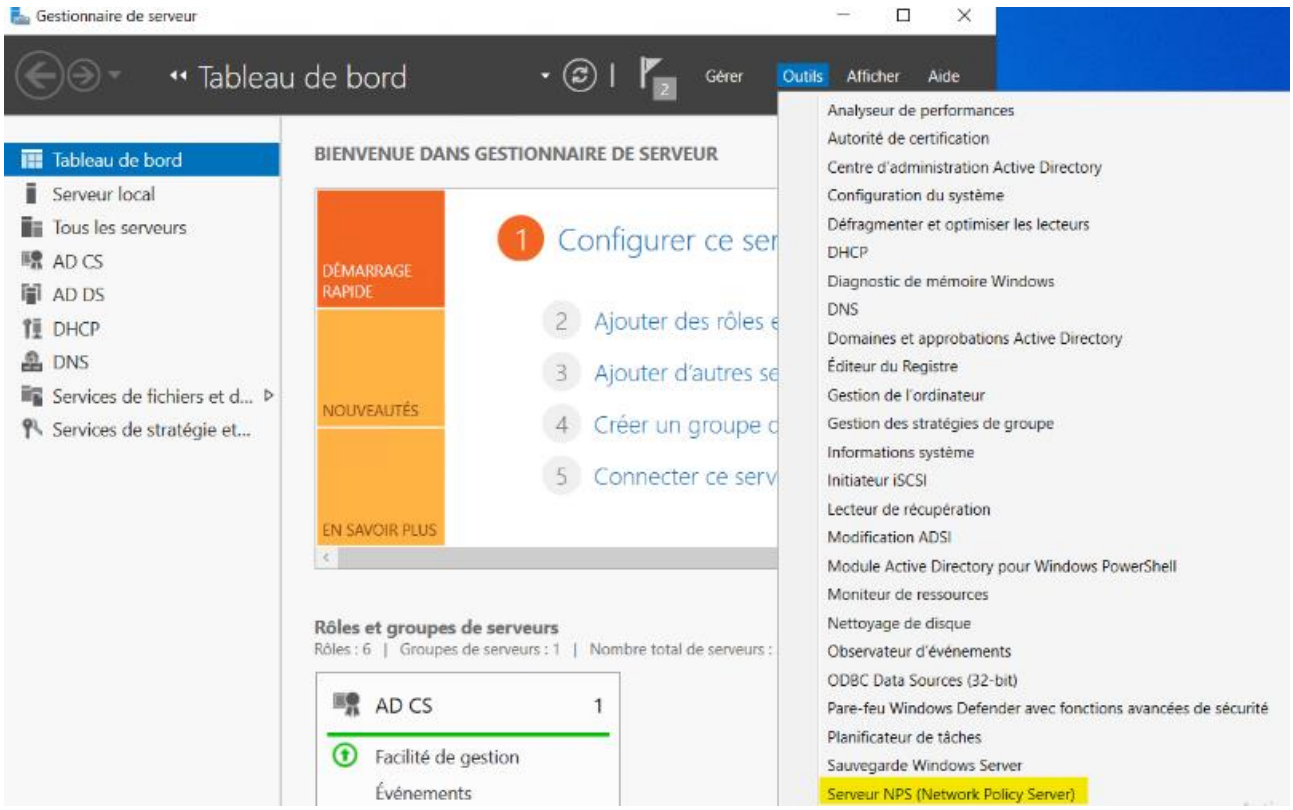
Tout d'abord, sur mon active directory ADSECURE1, j'installe le rôle NPS.

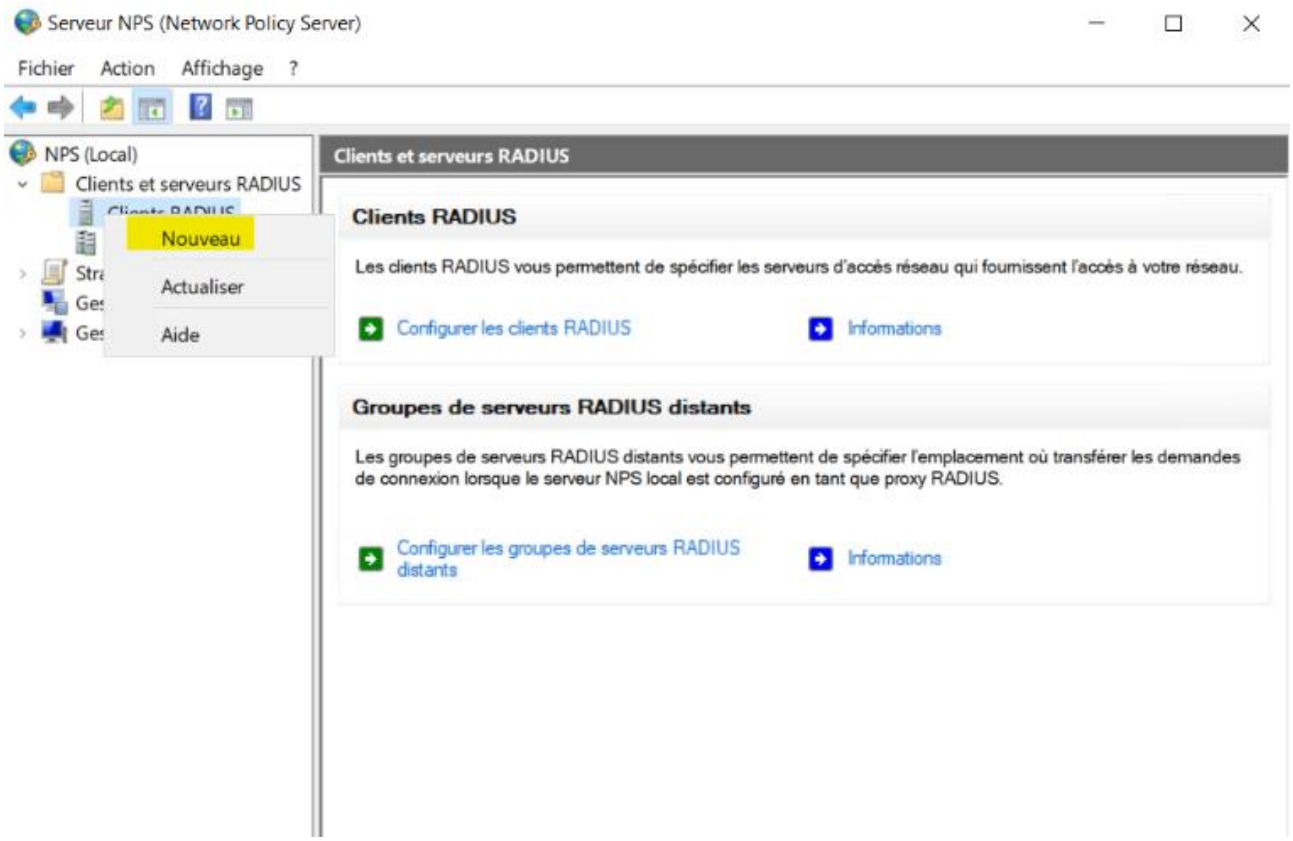


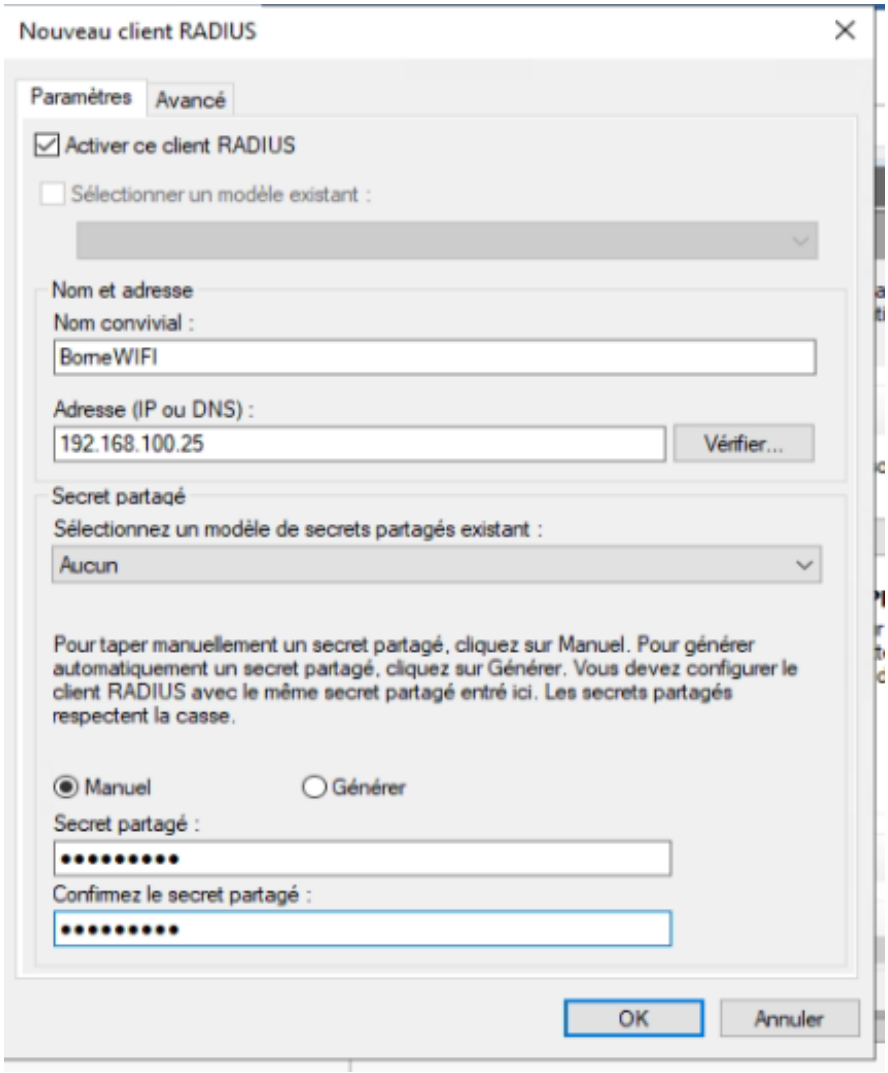

Assistant Ajout de rôles et de fonctionnalités
Sélectionner le serveur de destination
SERVEUR DE DESTINATION
ADSecure1.roncenoir.local
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats
Sélectionnez le serveur ou le disque dur virtuel 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
ADSecure2.roncenoir.local
192.168.0.2
Microsoft Windows Server 2022 Standard
ADSecure1.roncenoir.local
192.168.0.1
Microsoft Windows Server 2022 Standard
2 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


Assistant Ajout de rôles et de fonctionnalités
Sélectionner des rôles de serveurs
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Services de stratégie et d'...
Confirmation
Résultats
Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.
Rôles
Description
Accès à distance
Attestation d'intégrité de l'appareil
Hyper-V
Serveur de télécopie
Serveur DHCP (Installé)
Serveur DNS (Installé)
Serveur Web (IIS)
Service Guardian hôte
Services AD DS (Installé)
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 (1 sur 6 inst
Services de fédération Active Directory (AD FS)
Services de fichiers et de stockage (2 sur 12 install
Services de stratégie et d'accès réseau
Services WSUS (Windows Server Update Services)
Les services de stratégie et d'accès réseau fournissent un serveur NPS (Network Policy Server) qui contribue à garantir la sécurité de votre réseau.
< Précédent
Suivant >
Installer
Annuler


Assistant Ajout de rôles et de fonctionnalités
Confirmer les sélections d'installation
SERVEUR DE DESTINATION
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Services de stratégie et d'
Confirmation
Résultats
Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectionné, cliquez sur Installer.
Redémarrer automatiquement le serveur de destination, si nécessaire
Il se peut que des fonctionnalités facultatives (comme des outils d'administration) soient affichées sur cette page, car elles ont été sélectionnées automatiquement. Si vous ne voulez pas installer ces fonctionnalités facultatives, cliquez sur Précédent pour désactiver leurs cases à cocher.
Outils d'administration de serveur distant
Outils d'administration de rôles
Outils de la stratégie réseau et des services d'accès
Services de stratégie et d'accès réseau
Exporter les paramètres de configuration
Spécifier un autre chemin d'accès source
< Précédent
Suivant >
Installer
Annuler

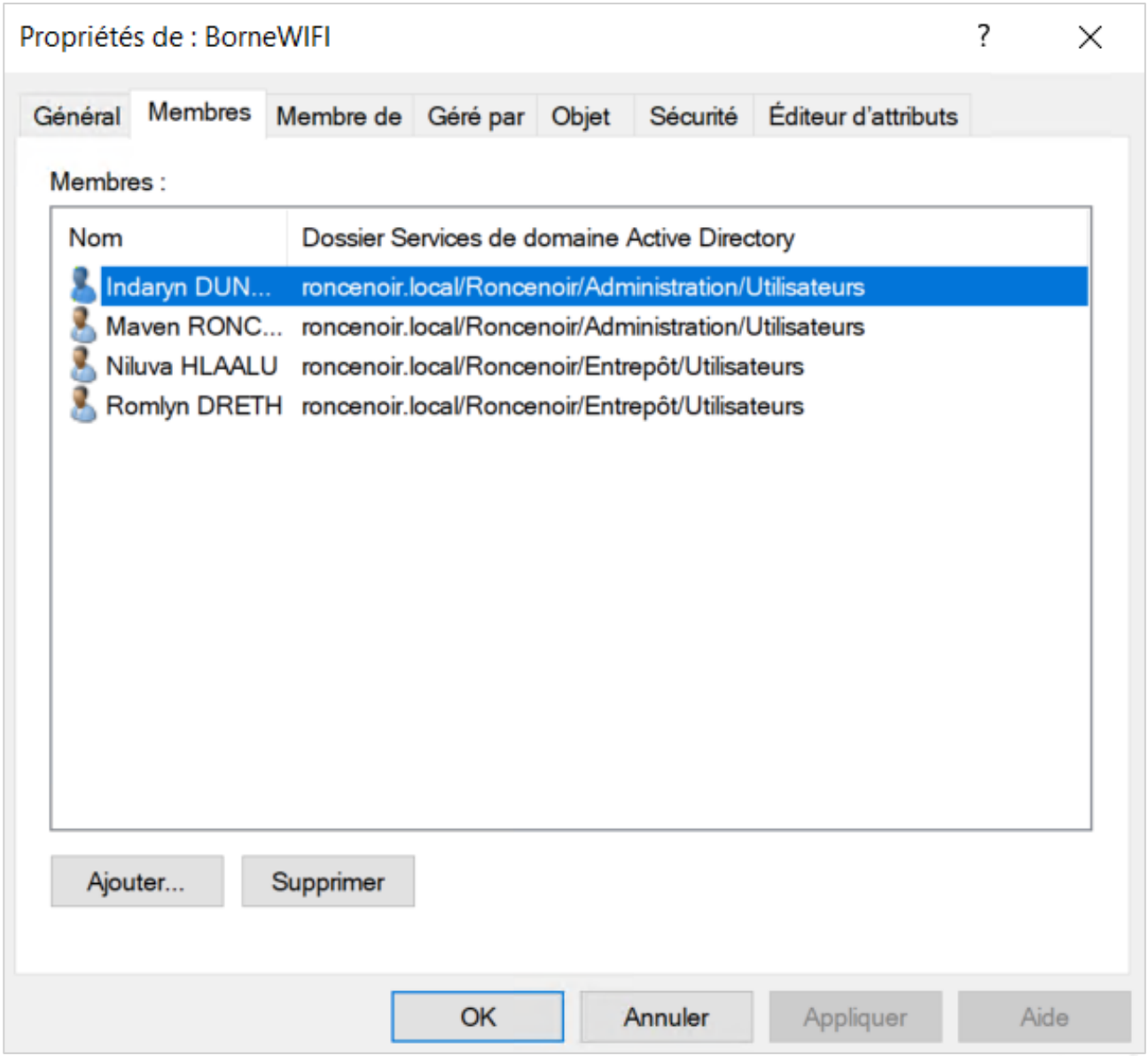

Gestionnaire de serveur
Tableau de bord
Gérer
Outils
Afficher
Aide
Tableau de bord
Serveur local
Tous les serveurs
AD CS
AD DS
DHCP
DNS
Services de fichiers et d...
Services de stratégie et...
BIENVENUE DANS GESTIONNAIRE DE SERVEUR
DÉMARRAGE RAPIDE
NOUVEAUTÉS
EN SAVOIR PLUS
1 Configurer ce ser
2 Ajouter des rôles e
3 Ajouter d'autres se
4 Créer un groupe d
5 Connecter ce serv
Rôles et groupes de serveurs
Rôles : 6 | Groupes de serveurs : 1 | Nombre total de serveurs :
AD CS 1
Facilité de gestion
Événements
Analyseur de performances
Autorité de certification
Centre d'administration Active Directory
Configuration du système
Défragmenter et optimiser les lecteurs
DHCP
Diagnostic de mémoire Windows
DNS
Domaines et approbations Active Directory
Éditeur du Registre
Gestion de l'ordinateur
Gestion des stratégies de groupe
Informations système
Initiateur iSCSI
Lecteur de récupération
Modification ADSI
Module Active Directory pour Windows PowerShell
Moniteur de ressources
Nettoyage de disque
Observateur d'événements
ODBC Data Sources (32-bit)
Pare-feu Windows Defender avec fonctions avancées de sécurité
Planificateur de tâches
Sauvegarde Windows Server
Serveur NPS (Network Policy Server)

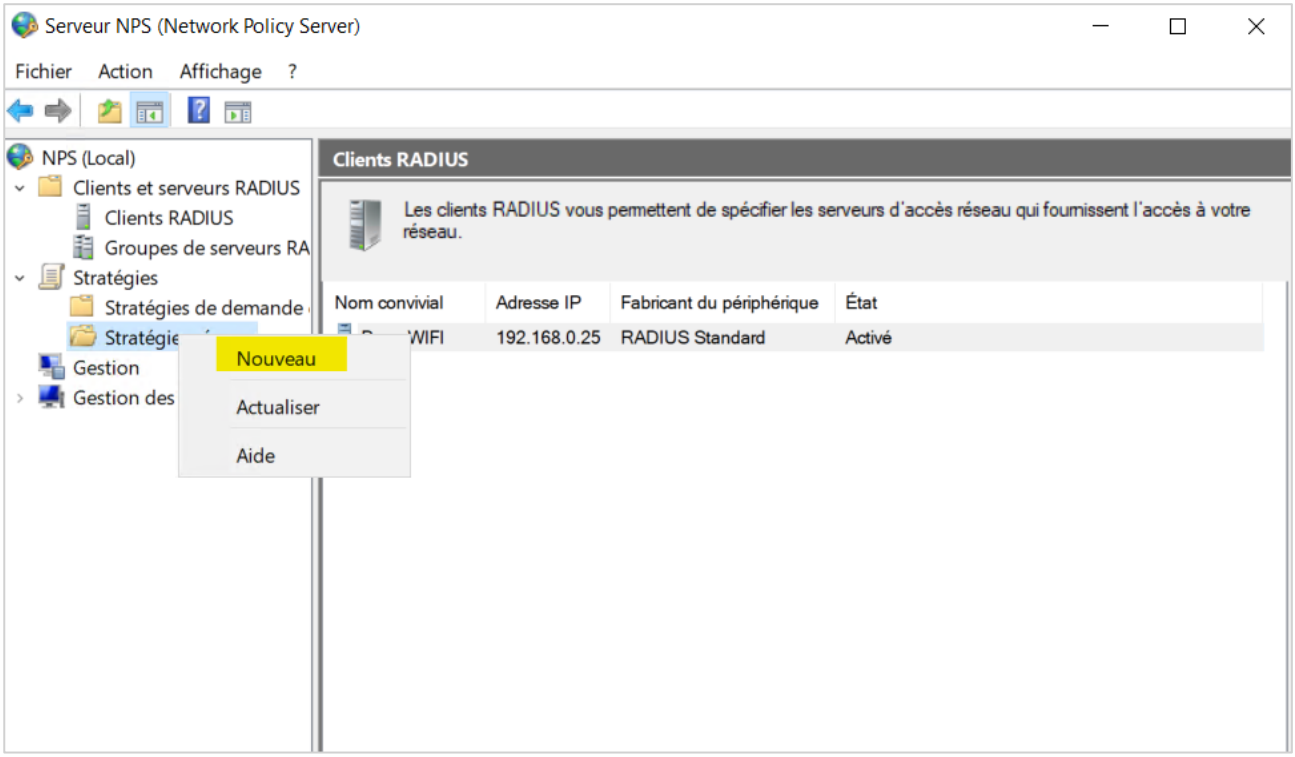


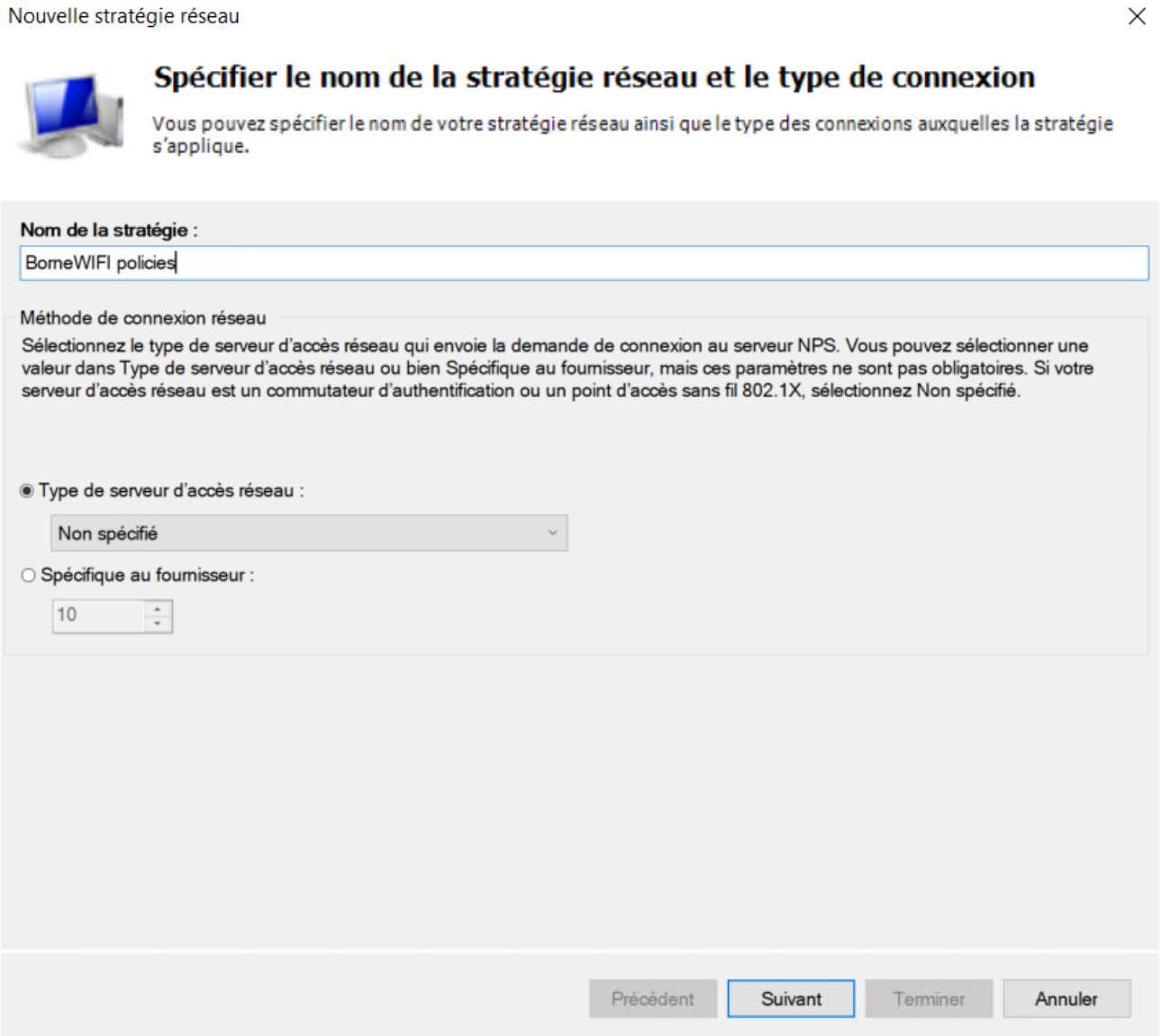


> Secret partagé = Roncenoir

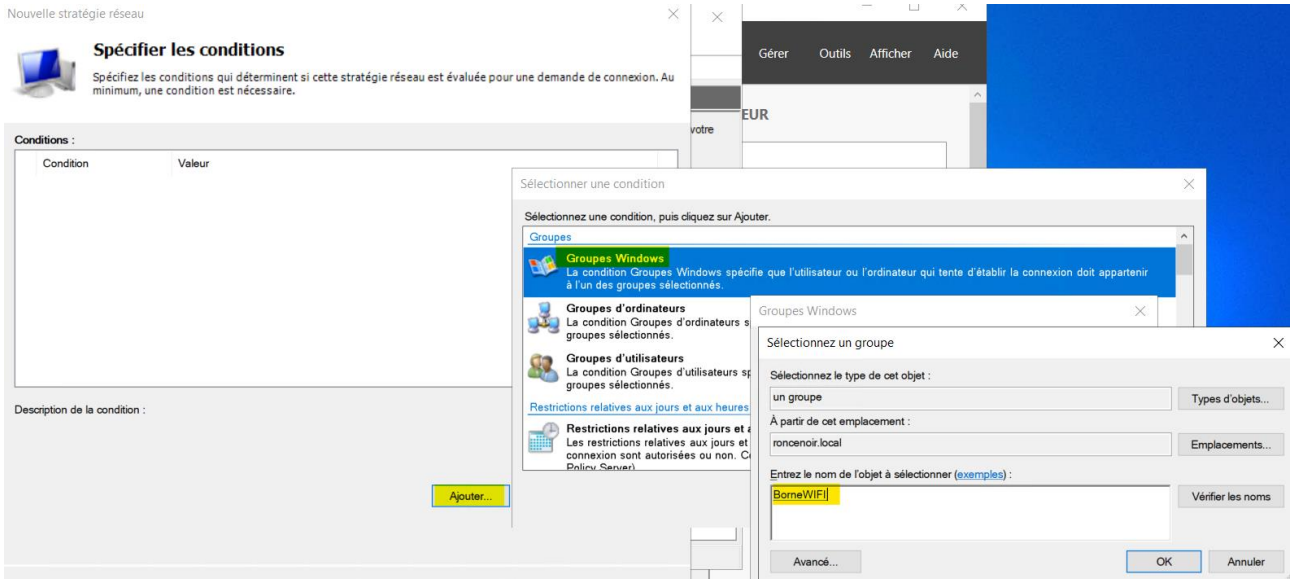
Je crée un groupe nommé « BorneWIFI » dans mon active directory et y ajoute pour membres les utilisateurs des OU Administration et Entrepôt. Puis on retourne sur NPS et on crée une nouvelle stratégie de réseau. Je l'appelle BorneWIFI policies.




Serveur NPS (Network Policy Server)
Fichier Action Affichage ?
NPS (Local)
Clients et serveurs RADIUS
Clients RADIUS
Groupes de serveurs RA
Stratégies
Stratégies de demande
Stratégie
Gestion
Gestion des
Nouveau
Actualiser
Aide
Clients RADIUS
Les clients RADIUS vous permettent de spécifier les serveurs d'accès réseau qui fournissent l'accès à votre réseau.
Nom convivial
Adresse IP
Fabricant du périphérique
État
WIFI
192.168.0.25
RADIUS Standard
Activé

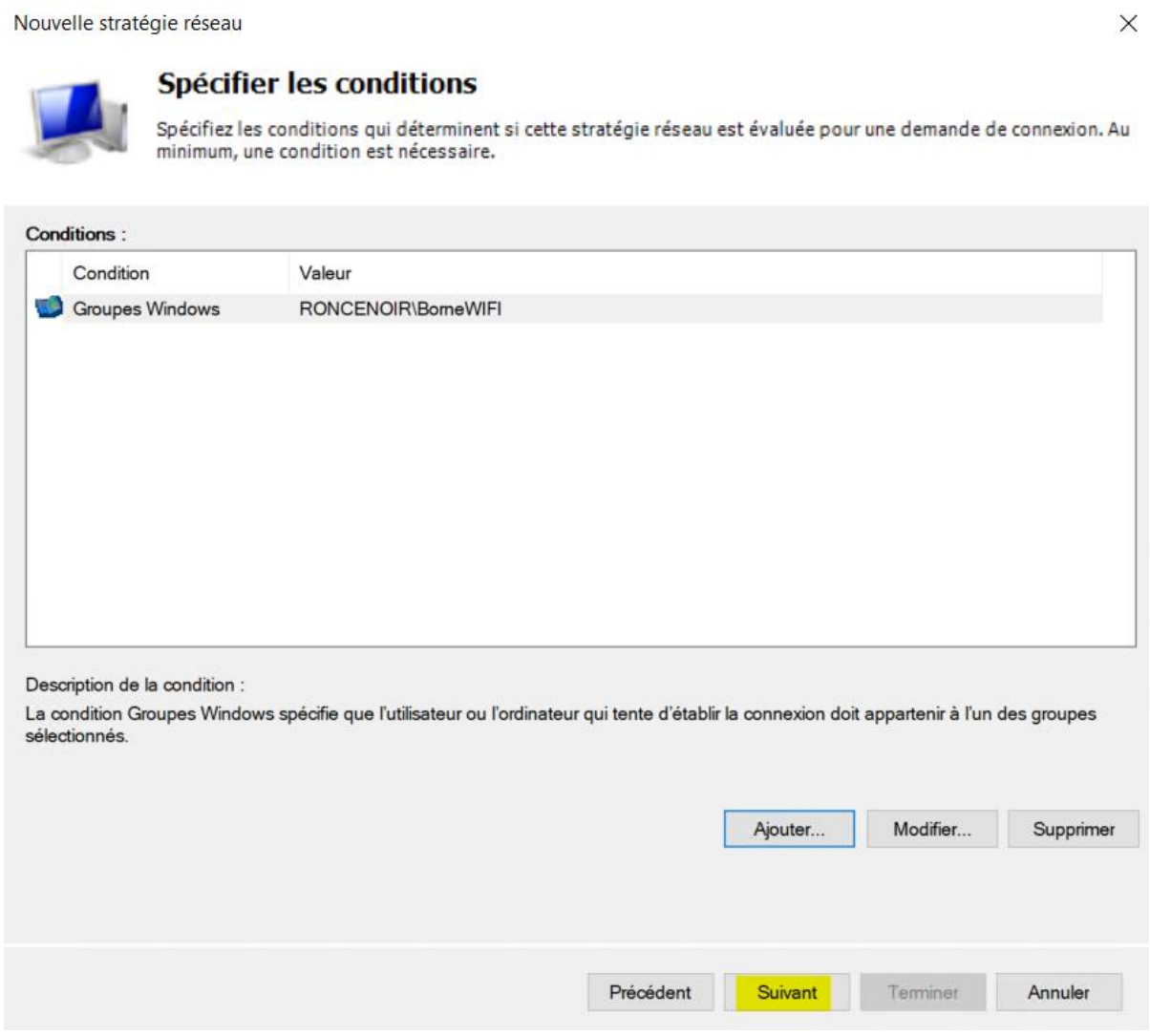

Nouvelle stratégie réseau
Spécifier le nom de la stratégie réseau et le type de connexion
Vous pouvez spécifier le nom de votre stratégie réseau ainsi que le type des connexions auxquelles la stratégie s'applique.
Nom de la stratégie :
BorneWIFI policies
Méthode de connexion réseau
Sélectionnez le type de serveur d'accès réseau qui envoie la demande de connexion au serveur NPS. Vous pouvez sélectionner une valeur dans Type de serveur d'accès réseau ou bien Spécifique au fournisseur, mais ces paramètres ne sont pas obligatoires. Si votre serveur d'accès réseau est un commutateur d'authentification ou un point d'accès sans fil 802.1X, sélectionnez Non spécifié.
Type de serveur d'accès réseau :
Non spécifié
Spécifique au fournisseur :
10
Précédent
Suivant
Terminer
Annuler

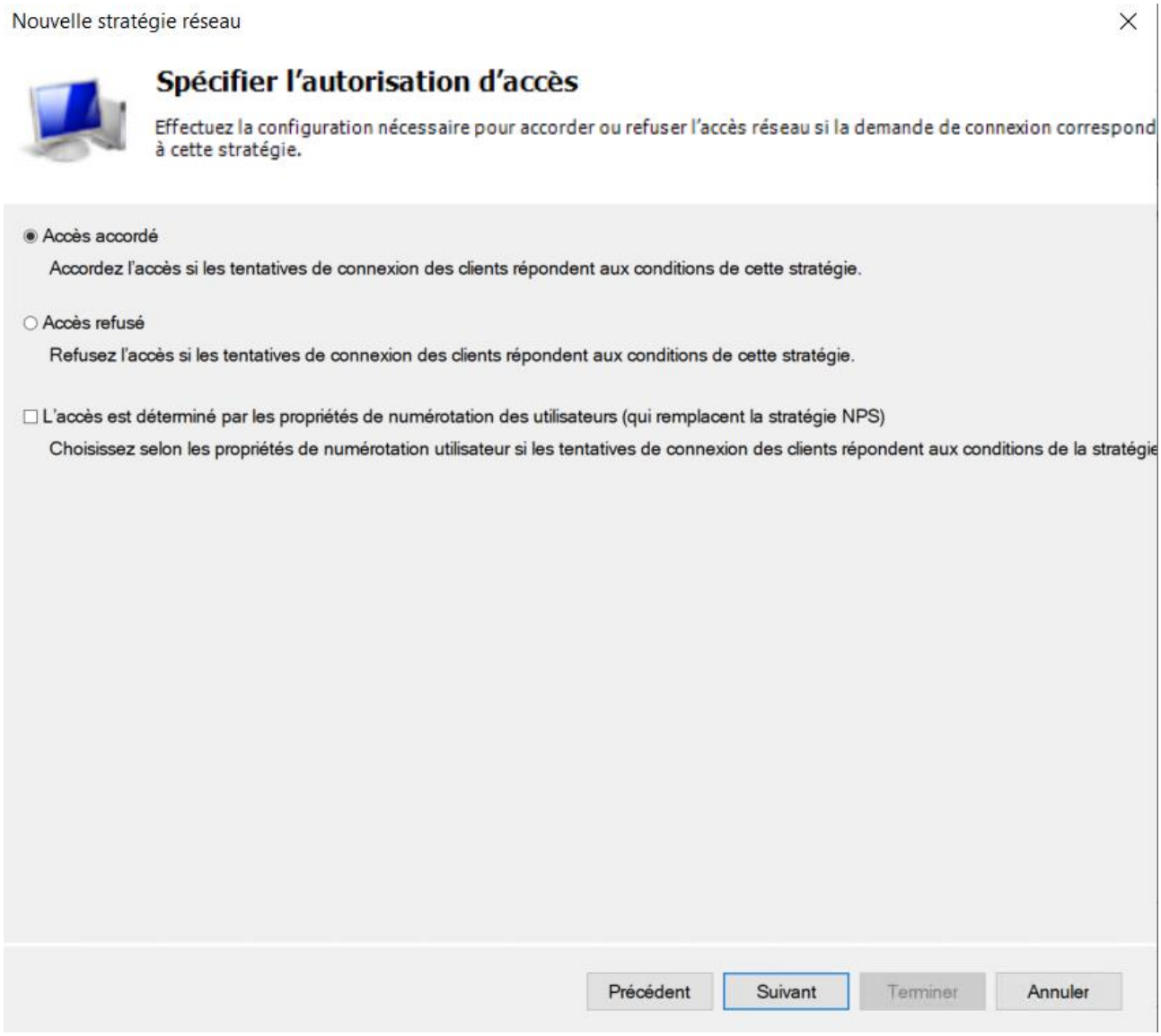
Puis, j'ajoute le groupe windows « BorneWIFI » créé précédemment aux conditions.



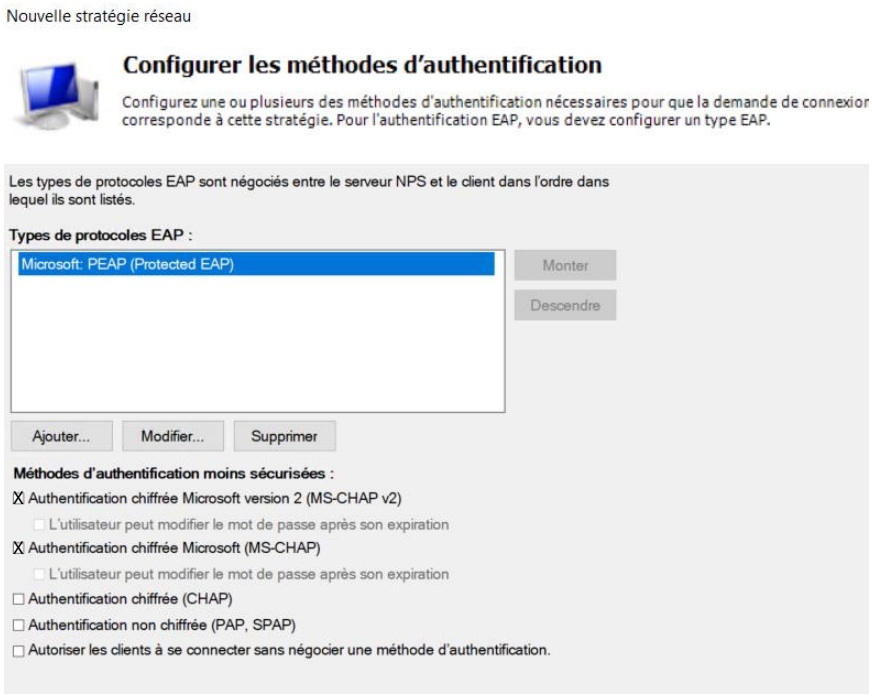
Je clic sur ok, je valide, et je continue avec « suivant ».

Sur la page suivante, je coche « Accès autorisé » pour autoriser la connexion aux personnes répondant à la condition précédemment définie.

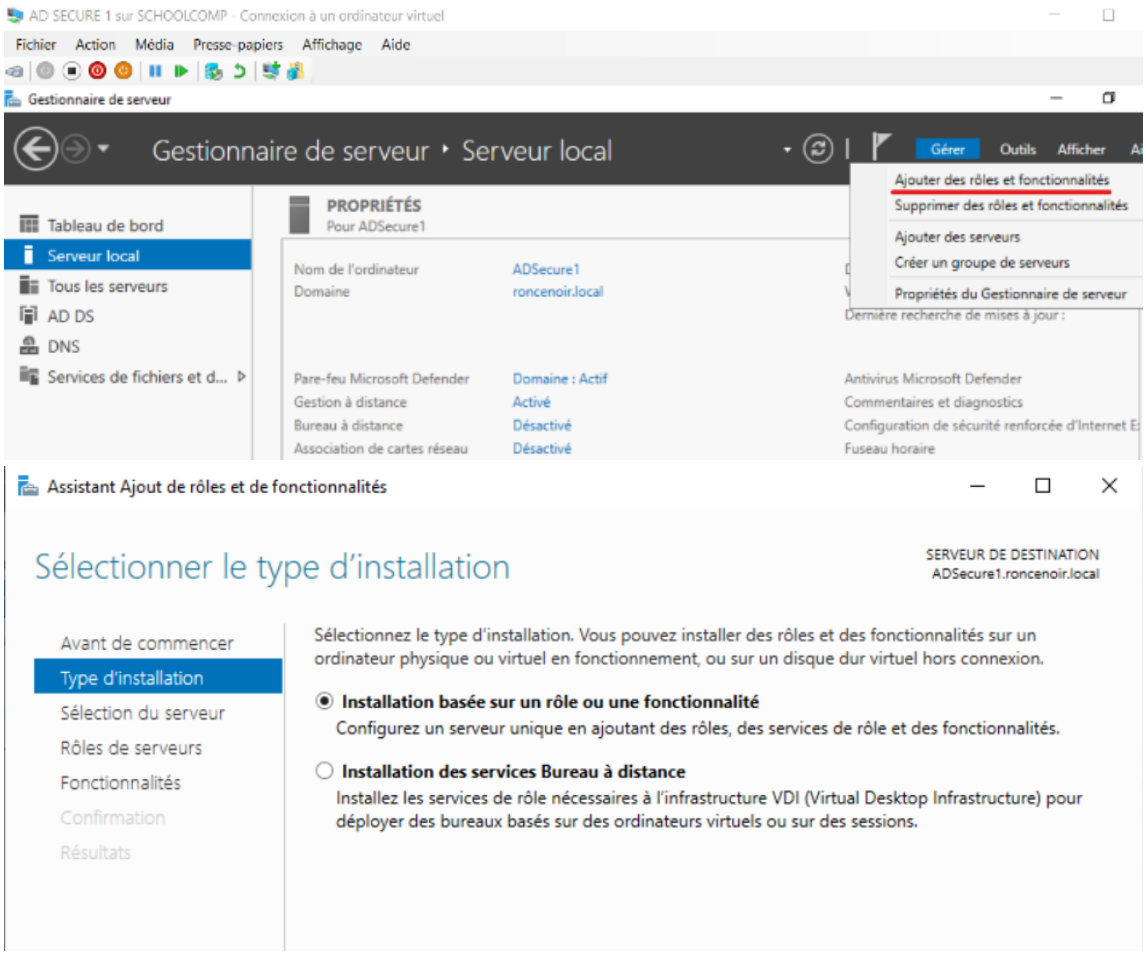


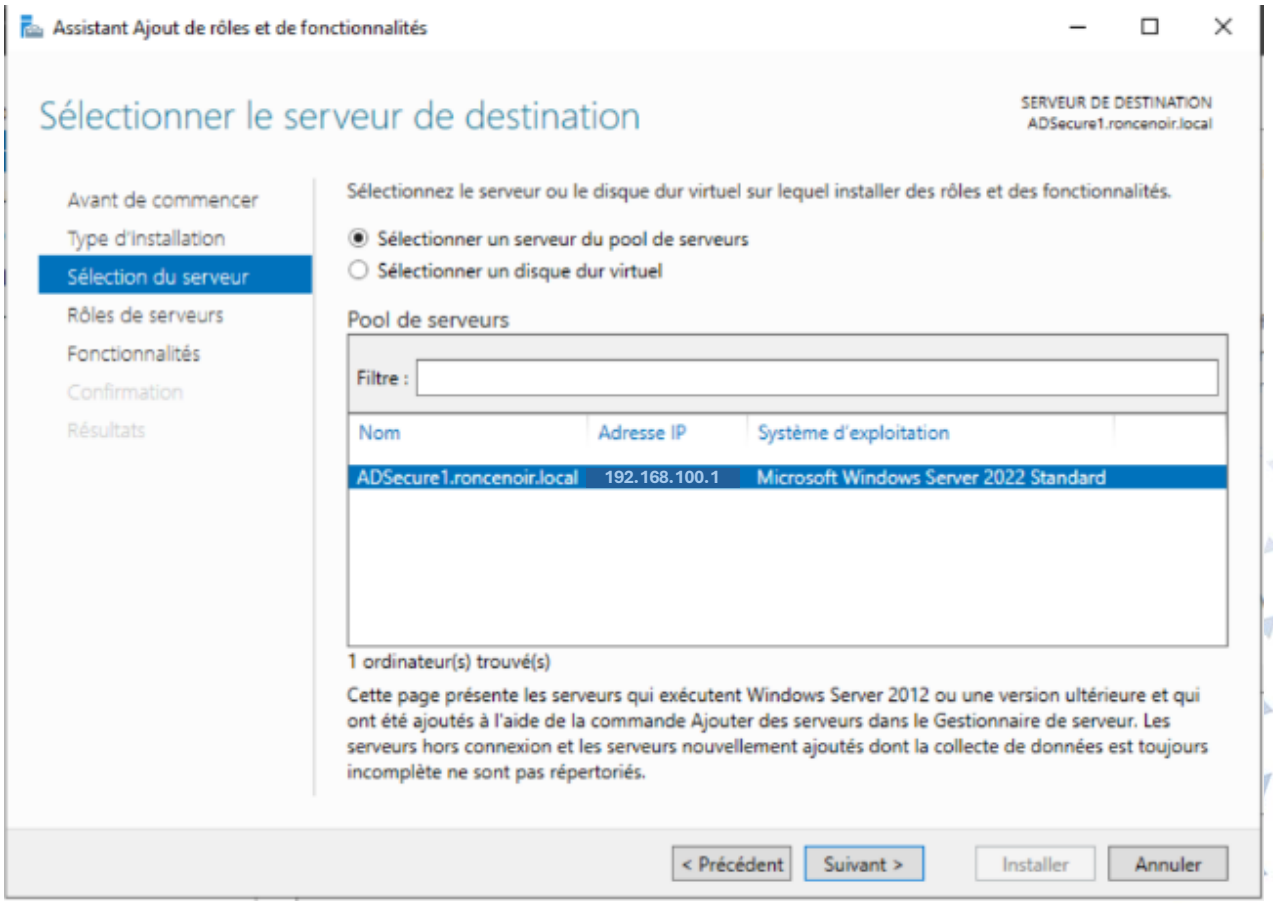


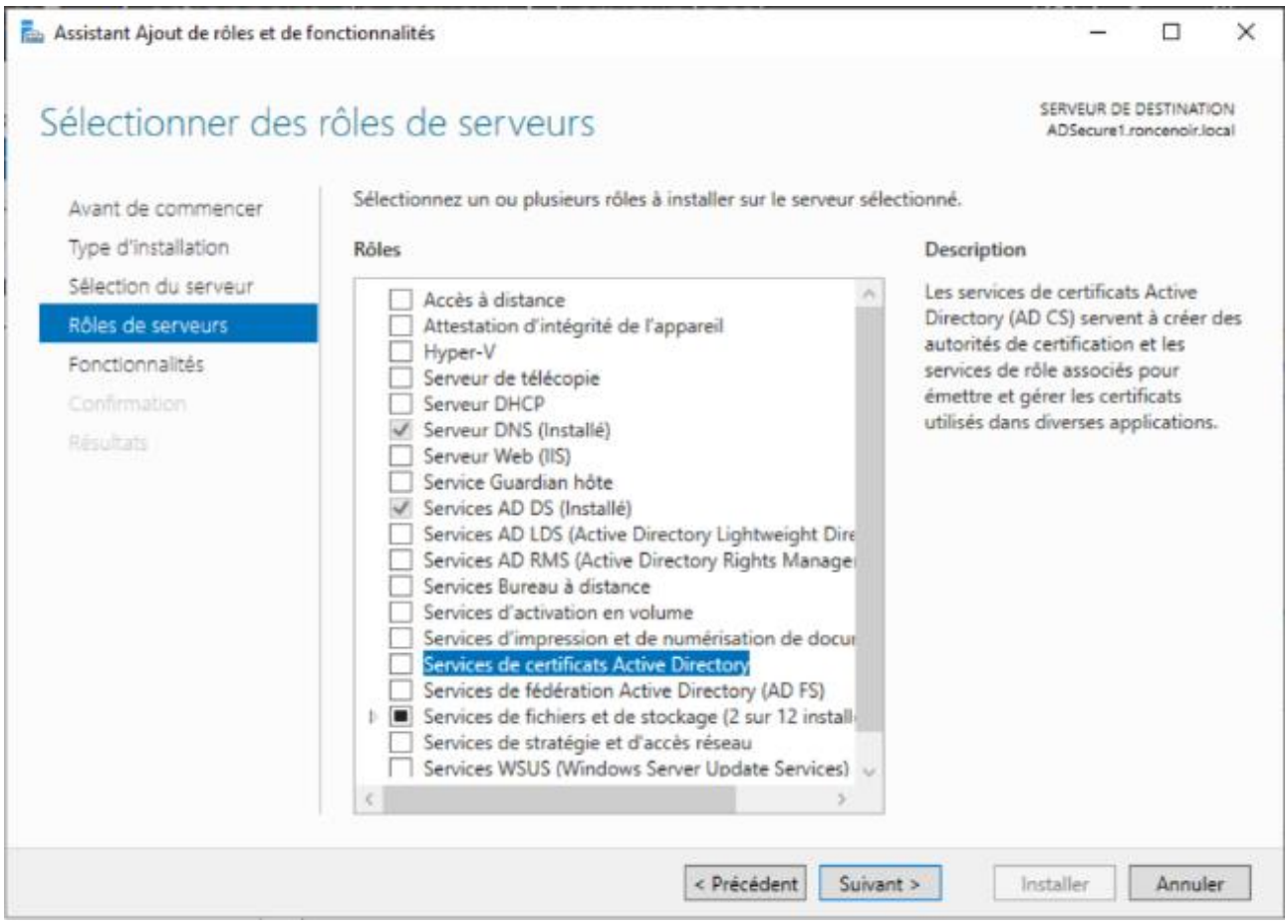
Je choisis l'authentification PEAP.

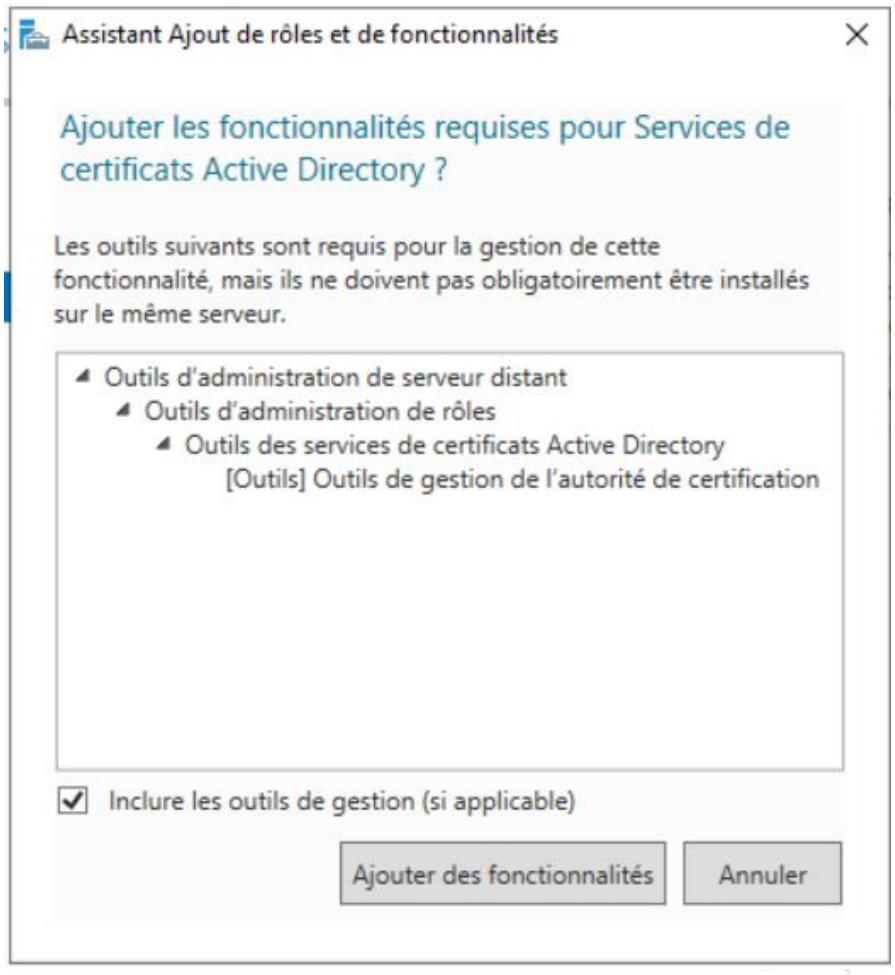


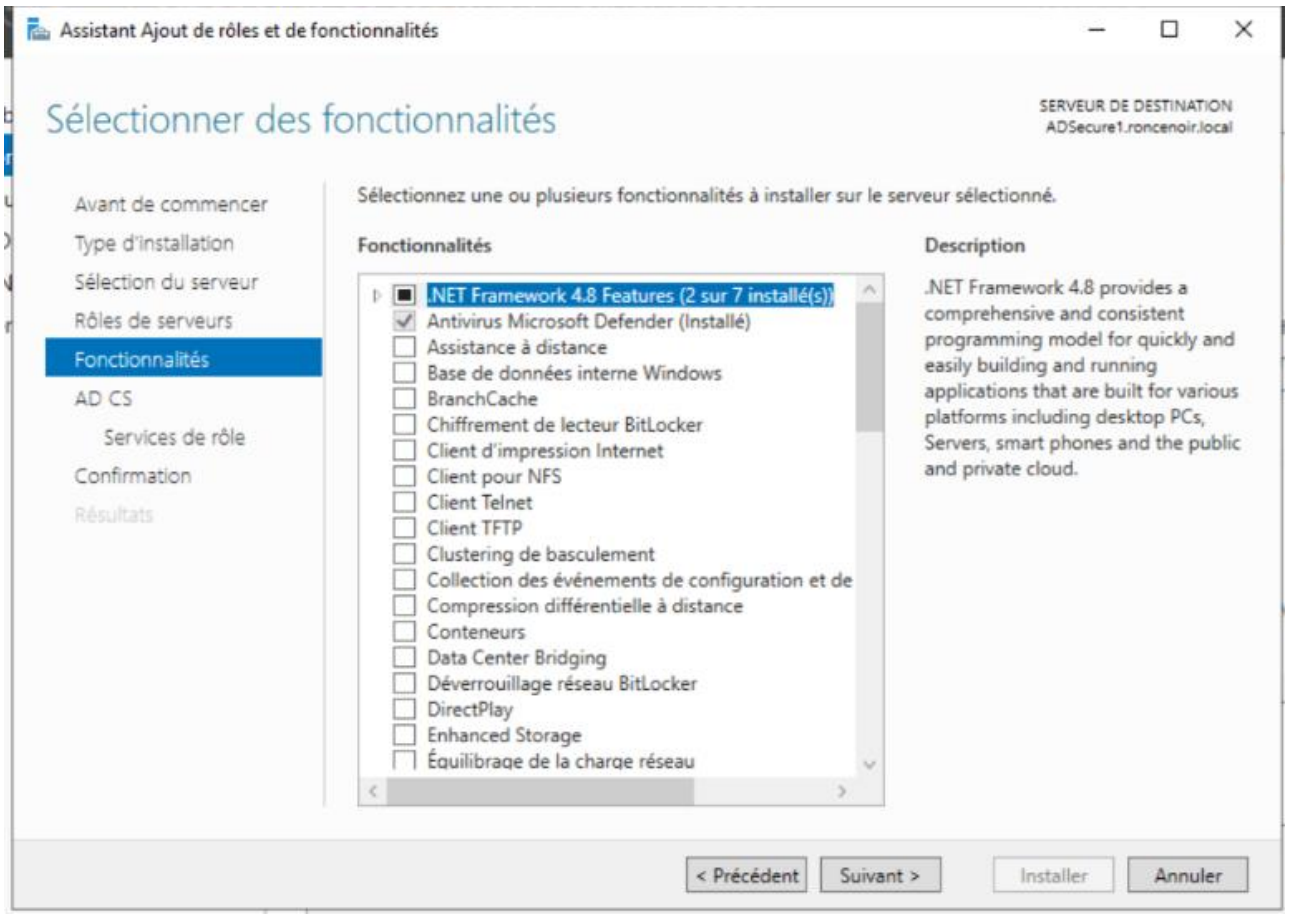
J'installe ADCS sur mon ad.



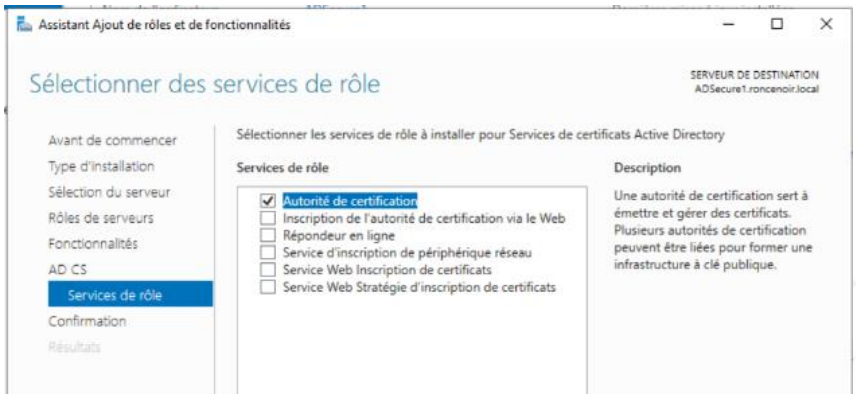


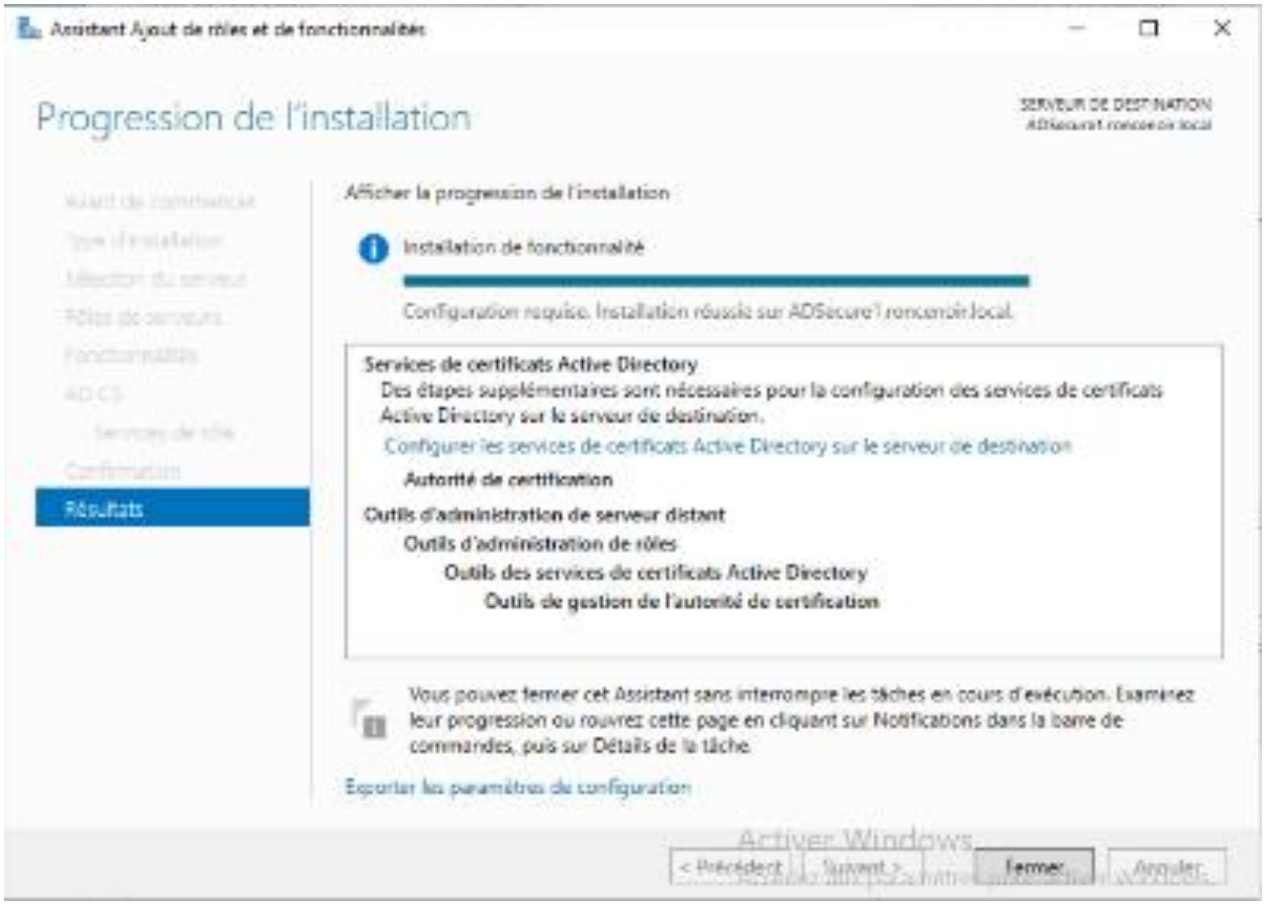

Assistant Ajout de rôles et de fonctionnalités
Sélectionner des rôles de serveurs
SERVEUR DE DESTINATION
ADSecure1.roncenoir.local
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats
Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.
Rôles
Accès à distance
Attestation d'intégrité de l'appareil
Hyper-V
Serveur de télécopie
Serveur DHCP
Serveur DNS (Installé)
Serveur Web (IIS)
Service Guardian hôte
Services AD DS (Installé)
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 (2 sur 12 install
Services de stratégie et d'accès réseau
Services WSUS (Windows Server Update Services)
Description
Les services de certificats Active Directory (AD CS) servent à créer des autorités de certification et les services de rôle associés pour émettre et gérer les certificats utilisés dans diverses applications.
< Précédent
Suivant >
Installer
Annuler

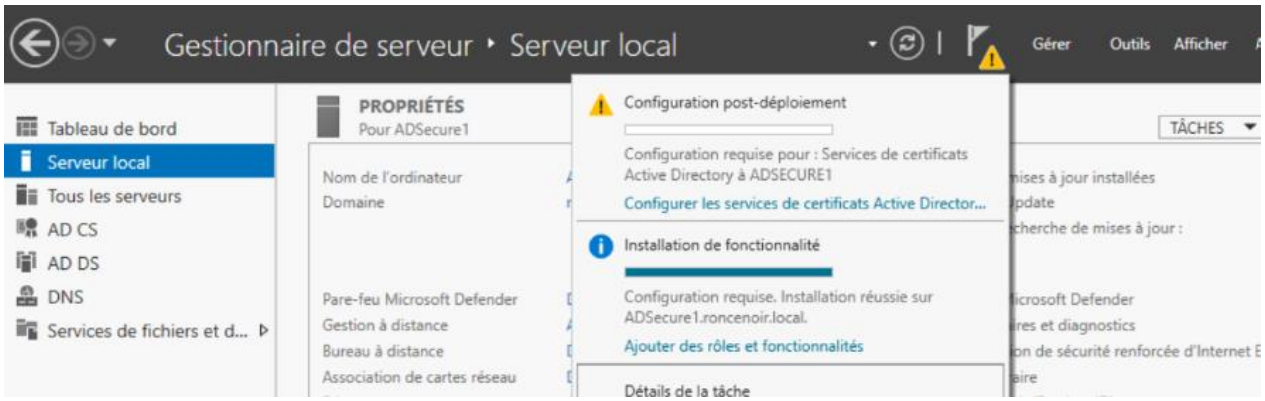

Assistant Ajout de rôles et de fonctionnalités
Ajouter les fonctionnalités requises pour Services de certificats Active Directory ?
Les outils suivants sont requis pour la gestion de cette fonctionnalité, mais ils ne doivent pas obligatoirement être installés sur le même serveur.
Outils d'administration de serveur distant
Outils d'administration de rôles
Outils des services de certificats Active Directory
[Outils] Outils de gestion de l'autorité de certification
Inclure les outils de gestion (si applicable)
Ajouter des fonctionnalités
Annuler

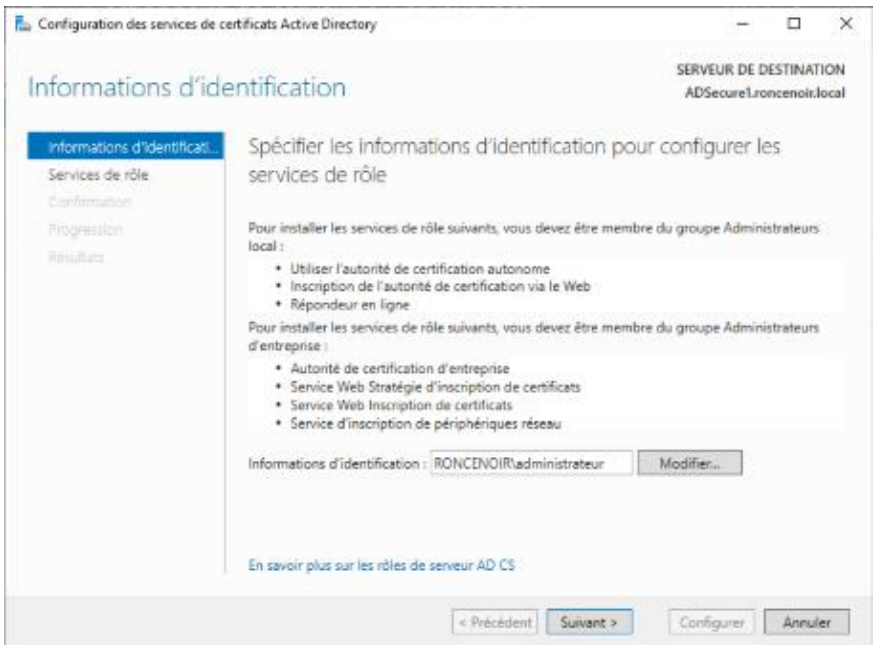

Assistant Ajout de rôles et de fonctionnalités
Sélectionner des fonctionnalités
SERVEUR DE DESTINATION
ADSecure1.roncenoir.local
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
AD CS
Services de rôle
Confirmation
Résultats
Sélectionnez une ou plusieurs fonctionnalités à installer sur le serveur sélectionné.
Fonctionnalités
.NET Framework 4.8 Features (2 sur 7 installé(s))
Antivirus Microsoft Defender (Installé)
Assistance à distance
Base de données interne Windows
BranchCache
Chiffrement de lecteur BitLocker
Client d'impression Internet
Client pour NFS
Client Telnet
Client TFTP
Clustering de basculement
Collection des événements de configuration et de
Compression différentielle à distance
Conteneurs
Data Center Bridging
Déverrouillage réseau BitLocker
DirectPlay
Enhanced Storage
Équilibrage de la charge réseau
Description
.NET Framework 4.8 provides a comprehensive and consistent programming model for quickly and easily building and running applications that are built for various platforms including desktop PCs, Servers, smart phones and the public and private cloud.
< Précédent
Suivant >
Installer
Annuler

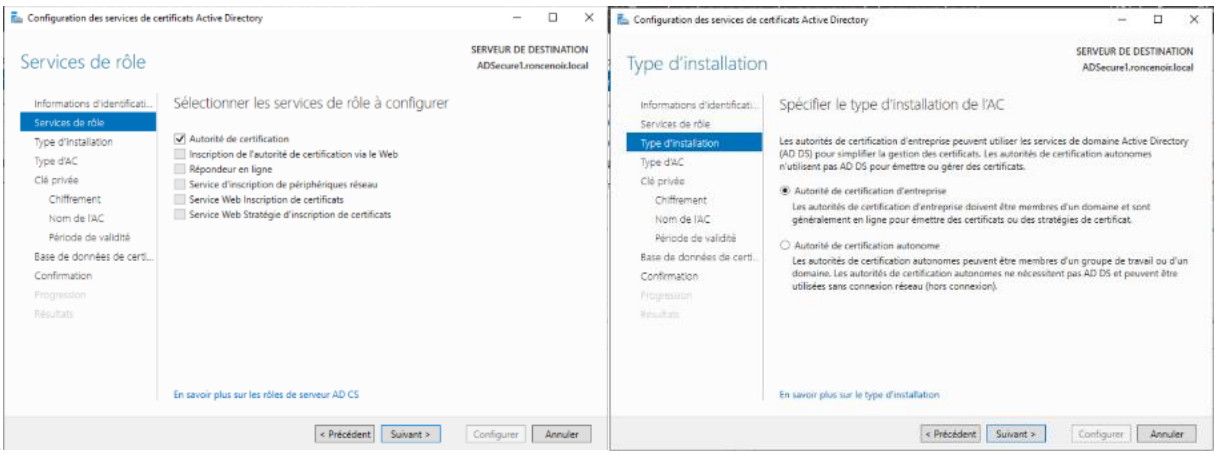

Assistant Ajout de rôles et de fonctionnalités
Services de certificats Active Directory
SERVEUR DE DESTINATION
ADSecure1.roncenoir.local
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
AD CS
Services de rôle
Confirmation
Résultats
Les services de certificats Active Directory (AD CS) fournissent l'infrastructure de certificats pour prendre en charge des scénarios tels que les réseaux sans fil sécurisés, les réseaux privés virtuels, la sécurité IPSec (Internet Protocol Security), la protection d'accès réseau (NAP), le système de fichiers EFS (Encrypting File System) et la connexion par carte à puce.
À noter :
• Les paramètres de nom et de domaine de cet ordinateur ne sont pas modifiables après l'installation d'une autorité de certification. Si vous voulez changer le nom de l'ordinateur, joindre un domaine ou promouvoir ce serveur en contrôleur de domaine, effectuez ces modifications avant d'installer l'autorité de certification. Pour plus d'informations, consultez Attribution d'un nom à une autorité de certification.

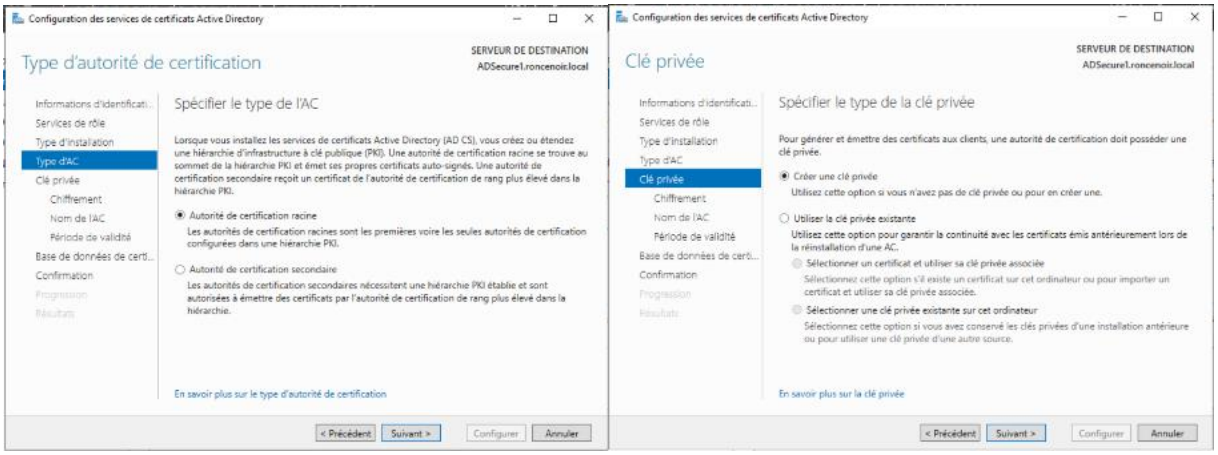

Assistant Ajout de rôles et de fonctionnalités
Sélectionner des services de rôle
SERVEUR DE DESTINATION
ADSecure1.roncenoir.local
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
AD CS
Services de rôle
Confirmation
Résultats
Sélectionner les services de rôle à installer pour Services de certificats Active Directory
Services de rôle
Autorité de certification
Inscription de l'autorité de certification via le Web
Répondeur en ligne
Service d'inscription de périphérique réseau
Service Web Inscription de certificats
Service Web Stratégie d'inscription de certificats
Description
Une autorité de certification sert à émettre et gérer des certificats. Plusieurs autorités de certification peuvent être liées pour former une infrastructure à clé publique.

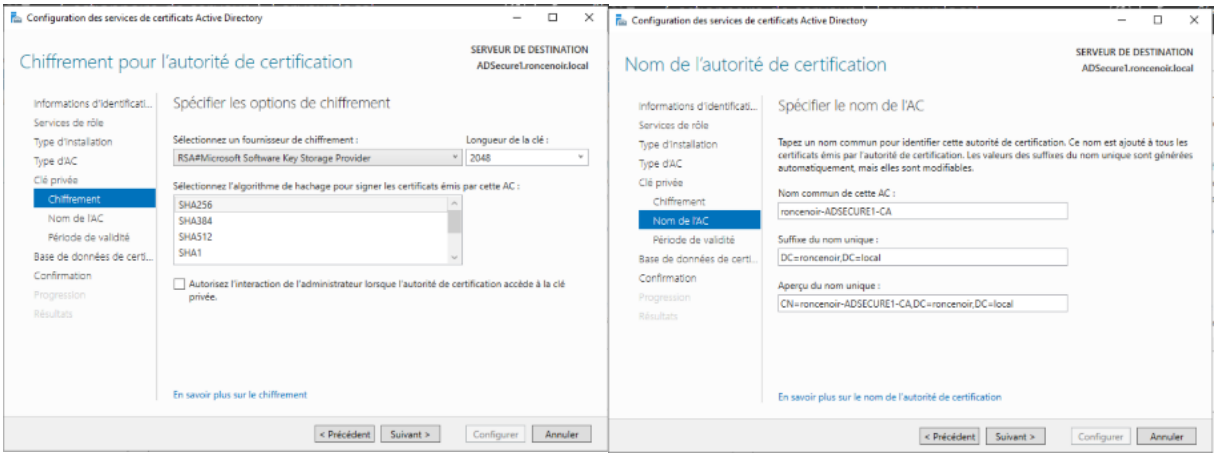

Assistant Ajout de rôles et de fonctionnalités
Progression de l'installation
SERVEUR DE DESTINATION
Afficher la progression de l'installation
Installation de fonctionnalité
Configuration requise. Installation réussie sur ADSecure1.roncenoir.local.
Services de certificats Active Directory
Des étapes supplémentaires sont nécessaires pour la configuration des services de certificats Active Directory sur le serveur de destination.
Configurer les services de certificats Active Directory sur le serveur de destination
Autorité de certification
Outils d'administration de serveur distant
Outils d'administration de rôles
Outils des services de certificats Active Directory
Outils de gestion de l'autorité de certification
Résultats
Vous pouvez fermer cet Assistant sans interrompre les tâches en cours d'exécution. Examinez leur progression ou rouvrez cette page en cliquant sur Notifications dans la barre de commandes, puis sur Détails de la tâche.
Exporter les paramètres de configuration
Activer Windows
< Précédent
Suivant >
Fermer
Annuler

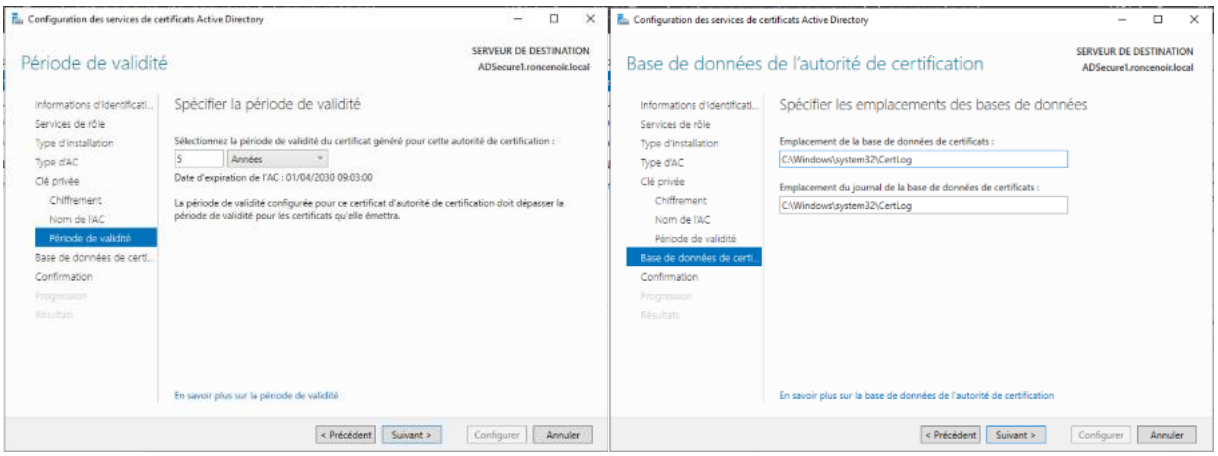

Gestionnaire de serveur • Serveur local
Gérer
Outils
Afficher
Tableau de bord
Serveur local
Tous les serveurs
AD CS
AD DS
DNS
Services de fichiers et d...
PROPRIÉTÉS
Pour ADSecure1
Nom de l'ordinateur
Domaine
Pare-feu Microsoft Defender
Gestion à distance
Bureau à distance
Association de cartes réseau
Configuration post-déploiement
Configuration requise pour : Services de certificats Active Directory à ADSECURE1
Configurer les services de certificats Active Director...
Installation de fonctionnalité
Configuration requise. Installation réussie sur ADSecure1.roncenoir.local.
Ajouter des rôles et fonctionnalités
Détails de la tâche
TÂCHES

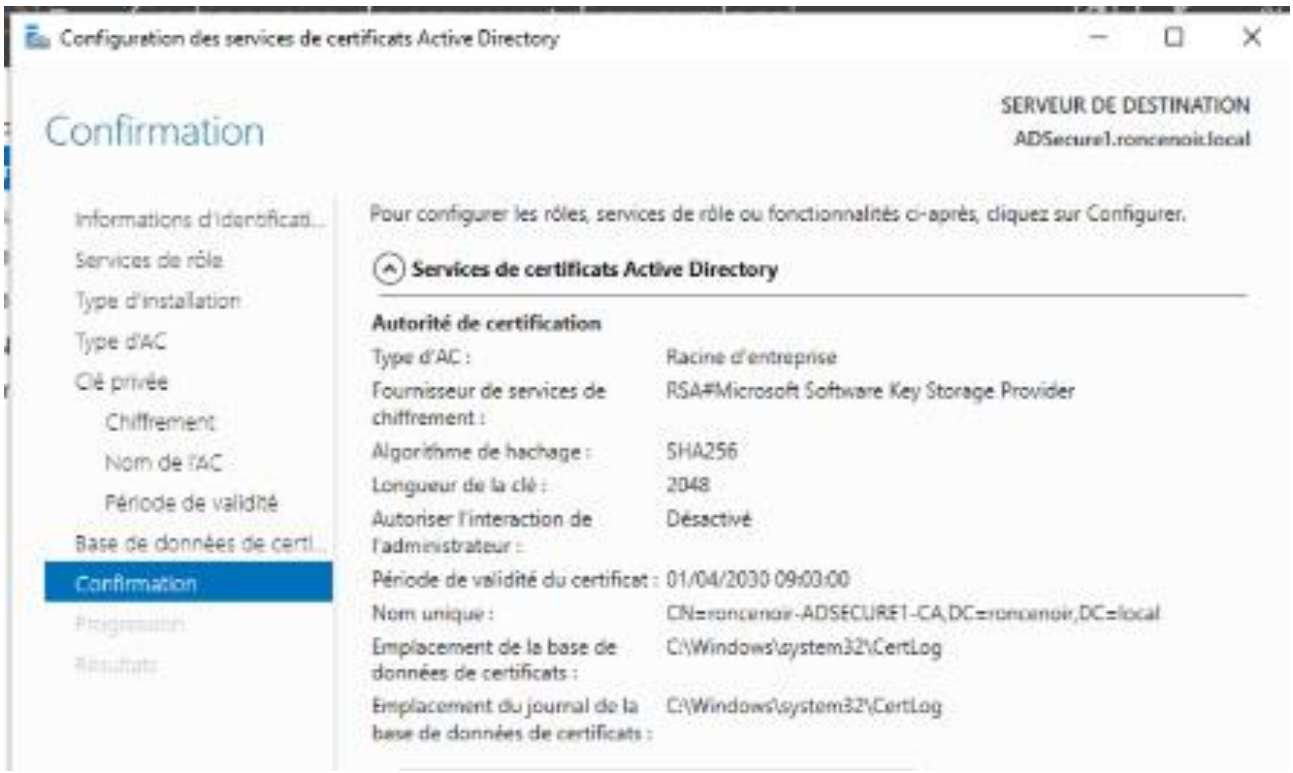

Configuration des services de certificats Active Directory
Informations d'identification
SERVEUR DE DESTINATION
ADSecure1.roncenoir.local
Informations d'identificati...
Services de rôle
Spécifier les informations d'identification pour configurer les services de rôle
Pour installer les services de rôle suivants, vous devez être membre du groupe Administrateurs local :
Utiliser l'autorité de certification autonome
Inscription de l'autorité de certification via le Web
Répondeur en ligne
Pour installer les services de rôle suivants, vous devez être membre du groupe Administrateurs d'entreprise :
Autorité de certification d'entreprise
Service Web Stratégie d'inscription de certificats
Service Web Inscription de certificats
Service d'inscription de périphériques réseau
Informations d'identification :
RONCENOIR\administrateur
Modifier...
En savoir plus sur les rôles de serveur AD CS
< Précédent
Suivant >
Configurer
Annuler

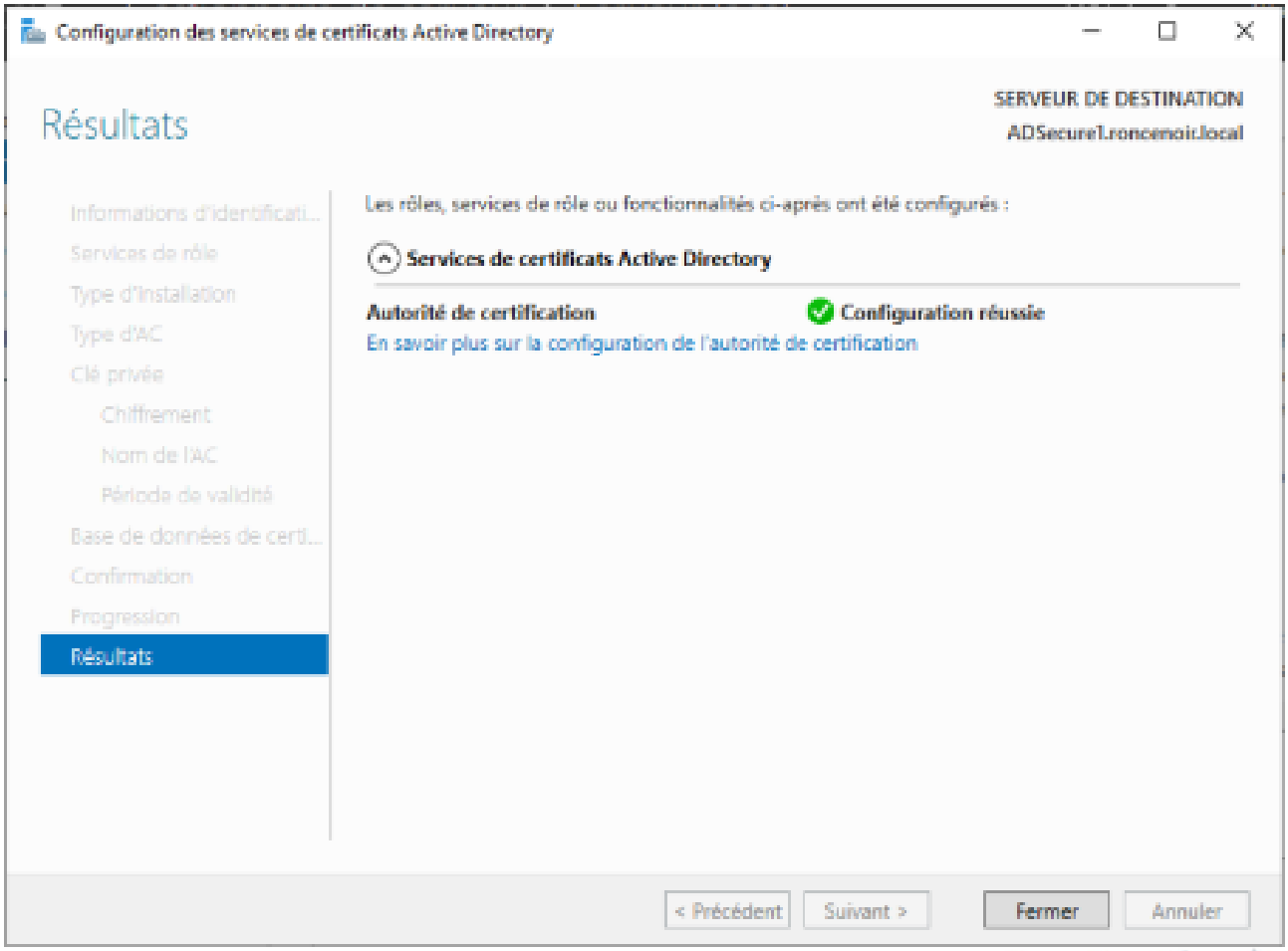

Configuration des services de certificats Active Directory
Services de rôle
SERVEUR DE DESTINATION
ADSecure1.roncenoir.local
Sélectionner les services de rôle à configurer
Autorité de certification
Inscription de l'autorité de certification via le Web
Répondeur en ligne
Service d'inscription de périphériques réseau
Service Web Inscription de certificats
Service Web Stratégie d'inscription de certificats
En savoir plus sur les rôles de serveur AD CS
< Précédent
Suivant >
Configurer
Annuler
Configuration des services de certificats Active Directory
Type d'installation
SERVEUR DE DESTINATION
ADSecure1.roncenoir.local
Spécifier le type d'installation de l'AC
Les autorités de certification d'entreprise peuvent utiliser les services de domaine Active Directory (AD DS) pour simplifier la gestion des certificats. Les autorités de certification autonomes n'utilisent pas AD DS pour émettre ou gérer des certificats.
Autorité de certification d'entreprise
Les autorités de certification d'entreprise doivent être membres d'un domaine et sont généralement en ligne pour émettre des certificats ou des stratégies de certificat.
Autorité de certification autonome
Les autorités de certification autonomes peuvent être membres d'un groupe de travail ou d'un domaine. Les autorités de certification autonomes ne nécessitent pas AD DS et peuvent être utilisées sans connexion réseau (hors connexion).
En savoir plus sur le type d'installation
< Précédent
Suivant >
Configurer
Annuler


Configuration des services de certificats Active Directory
Type d'autorité de certification
SERVEUR DE DESTINATION
ADSecure1.roncenoir.local
Spécifier le type de l'AC
Lorsque vous installez les services de certificats Active Directory (AD CS), vous créez ou étendez une hiérarchie d'infrastructure à clé publique (PKI). Une autorité de certification racine se trouve au sommet de la hiérarchie PKI et émet ses propres certificats auto-signés. Une autorité de certification secondaire reçoit un certificat de l'autorité de certification de rang plus élevé dans la hiérarchie PKI.
Autorité de certification racine
Les autorités de certification racines sont les premières voire les seules autorités de certification configurées dans une hiérarchie PKI.
Autorité de certification secondaire
Les autorités de certification secondaires nécessitent une hiérarchie PKI établie et sont autorisées à émettre des certificats par l'autorité de certification de rang plus élevé dans la hiérarchie.
En savoir plus sur le type d'autorité de certification
< Précédent
Suivant >
Configurer
Annuler
Configuration des services de certificats Active Directory
Clé privée
SERVEUR DE DESTINATION
ADSecure1.roncenoir.local
Spécifier le type de la clé privée
Pour générer et émettre des certificats aux clients, une autorité de certification doit posséder une clé privée.
Créer une clé privée
Utilisez cette option si vous n'avez pas de clé privée ou pour en créer une.
Utiliser la clé privée existante
Utilisez cette option pour garantir la continuité avec les certificats émis antérieurement lors de la réinstallation d'une AC.
Sélectionner un certificat et utiliser sa clé privée associée
Sélectionnez cette option s'il existe un certificat sur cet ordinateur ou pour importer un certificat et utiliser sa clé privée associée.
Sélectionner une clé privée existante sur cet ordinateur
Sélectionnez cette option si vous avez conservé les clés privées d'une installation antérieure ou pour utiliser une clé privée d'une autre source.
En savoir plus sur la clé privée
< Précédent
Suivant >
Configurer
Annuler


Configuration des services de certificats Active Directory
Chiffrement pour l'autorité de certification
SERVEUR DE DESTINATION
ADSecure1.roncenoir.local
Spécifier les options de chiffrement
Sélectionnez un fournisseur de chiffrement :
RSA#Microsoft Software Key Storage Provider
Longueur de la clé :
2048
Sélectionnez l'algorithme de hachage pour signer les certificats émis par cette AC :
SHA256
SHA384
SHA512
SHA1
Autorisez l'interaction de l'administrateur lorsque l'autorité de certification accède à la clé privée.
En savoir plus sur le chiffrement
< Précédent
Suivant >
Configurer
Annuler
Configuration des services de certificats Active Directory
Nom de l'autorité de certification
SERVEUR DE DESTINATION
ADSecure1.roncenoir.local
Spécifier le nom de l'AC
Tapez un nom commun pour identifier cette autorité de certification. Ce nom est ajouté à tous les certificats émis par l'autorité de certification. Les valeurs des suffixes du nom unique sont générées automatiquement, mais elles sont modifiables.
Nom commun de cette AC :
roncenoir-ADSECURE1-CA
Suffixe du nom unique :
DC=roncenoir,DC=local
Aperçu du nom unique :
CN=roncenoir-ADSECURE1-CA,DC=roncenoir,DC=local
En savoir plus sur le nom de l'autorité de certification
< Précédent
Suivant >
Configurer
Annuler

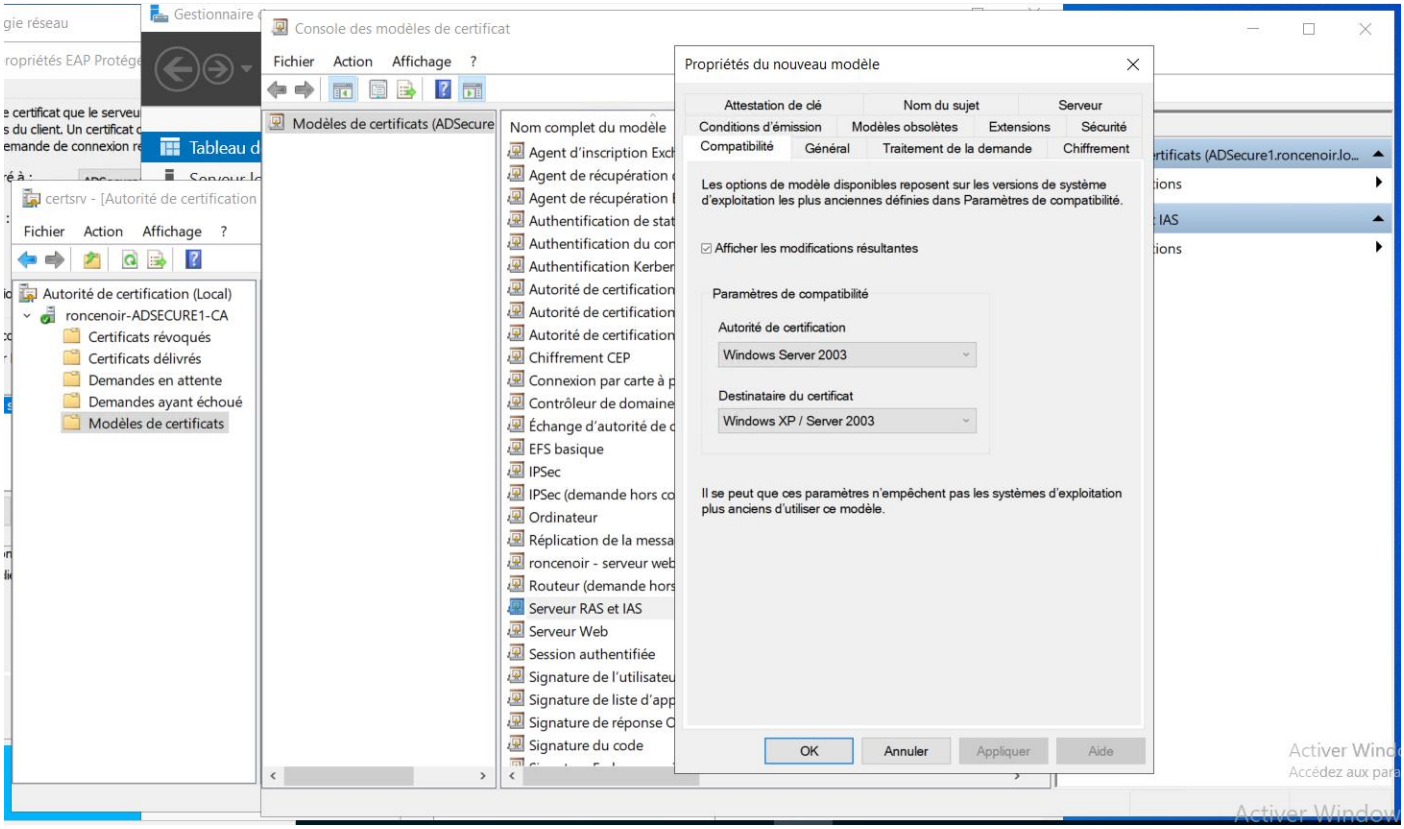

Configuration des services de certificats Active Directory
Période de validité
SERVEUR DE DESTINATION
ADSecure1.roncenoir.local
Spécifier la période de validité
Sélectionnez la période de validité du certificat généré pour cette autorité de certification :
5
Années
Date d'expiration de l'AC : 01/04/2030 09:03:00
La période de validité configurée pour ce certificat d'autorité de certification doit dépasser la période de validité pour les certificats qu'elle émettra.
En savoir plus sur la période de validité
< Précédent
Suivant >
Configurer
Annuler
Configuration des services de certificats Active Directory
Base de données de l'autorité de certification
SERVEUR DE DESTINATION
ADSecure1.roncenoir.local
Spécifier les emplacements des bases de données
Emplacement de la base de données de certificats :
C:\Windows\system32\CertLog
Emplacement du journal de la base de données de certificats :
C:\Windows\system32\CertLog
En savoir plus sur la base de données de l'autorité de certification
< Précédent
Suivant >
Configurer
Annuler



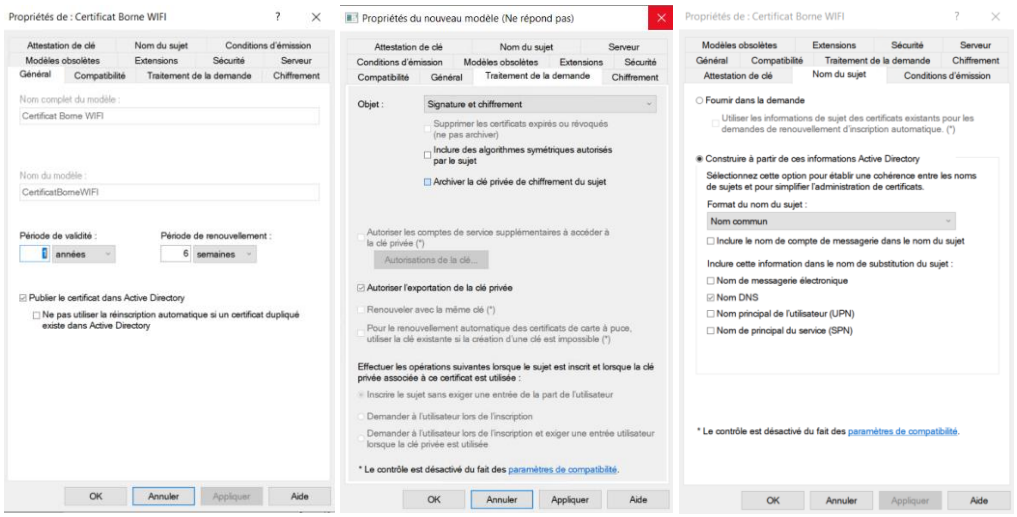


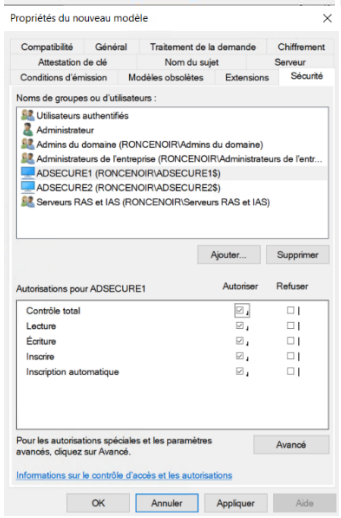
Je crée un nouveau certificat pour mes utilisateurs se connectant à ma borne WIFI.

Je commence par aller dans certsrv, clic droit sur « modèles de certificats », « gérer », trouver le modèle « serveur RAS et IAS », clic droit dessus, dupliquer.



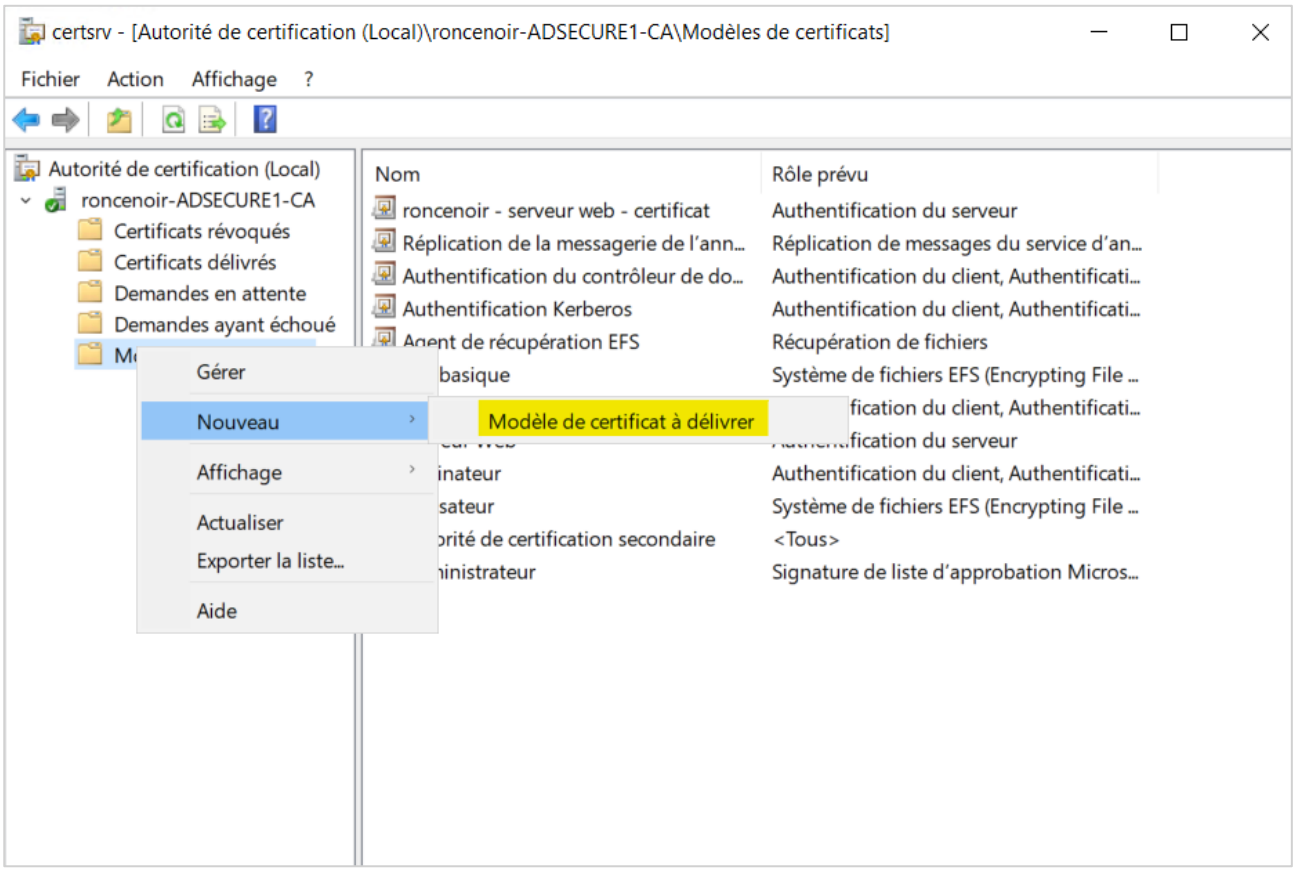
On le configure ainsi :

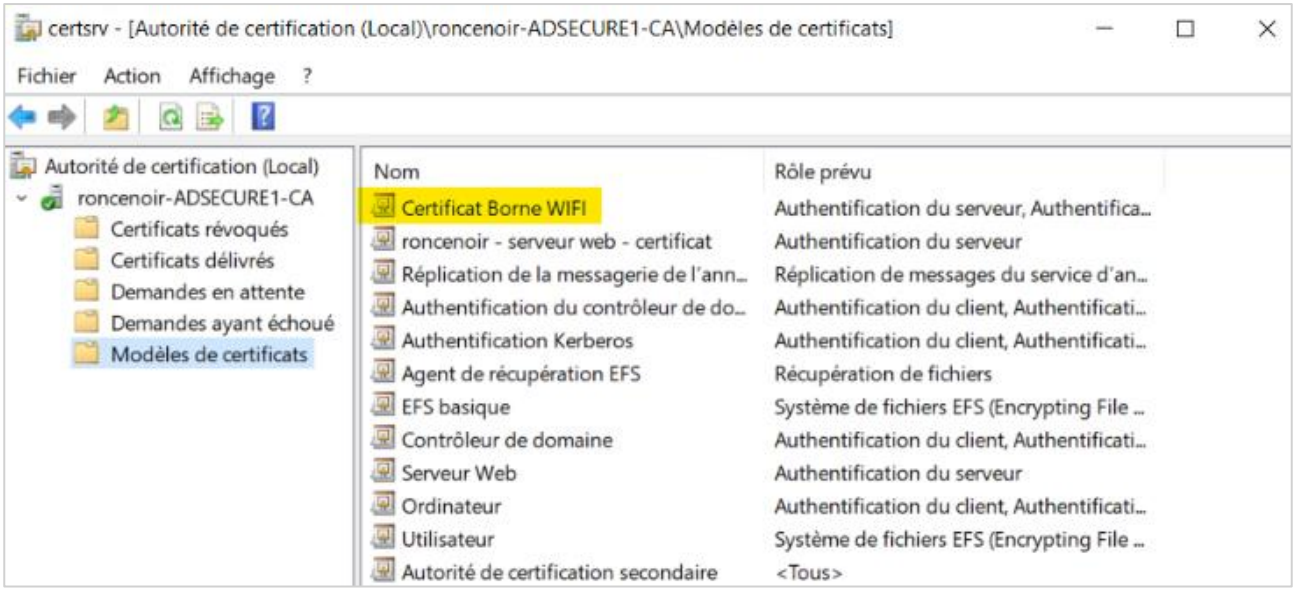




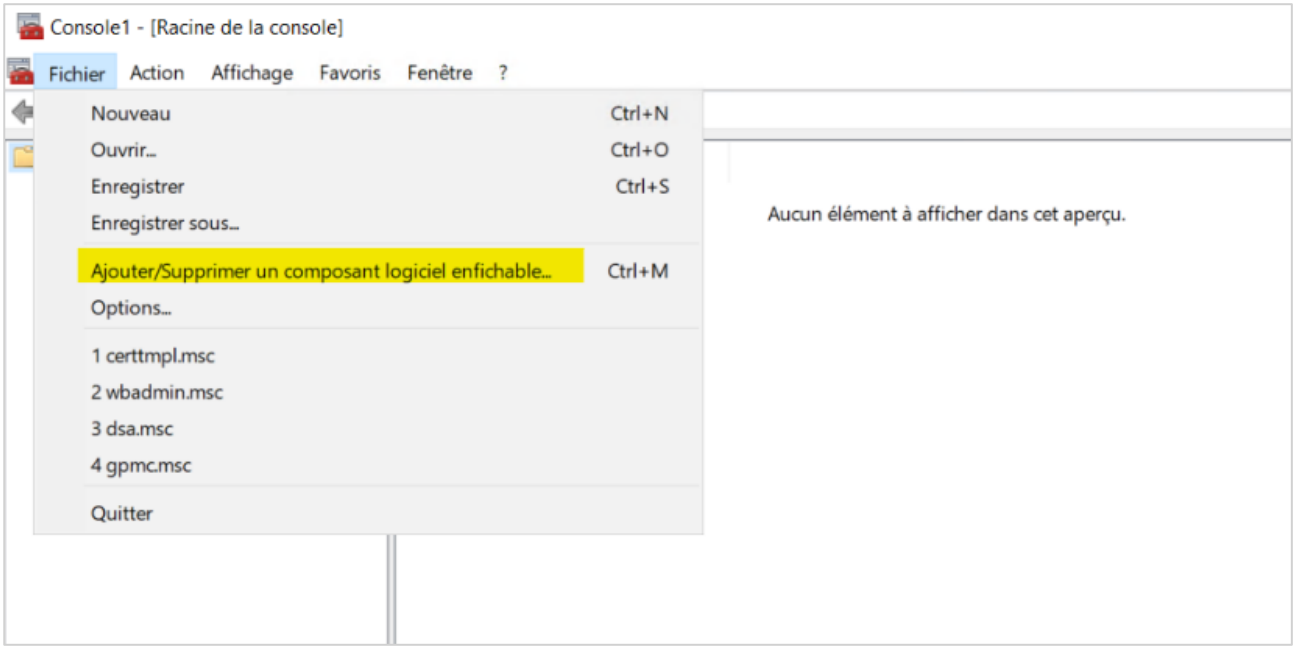
>On applique et on sort.

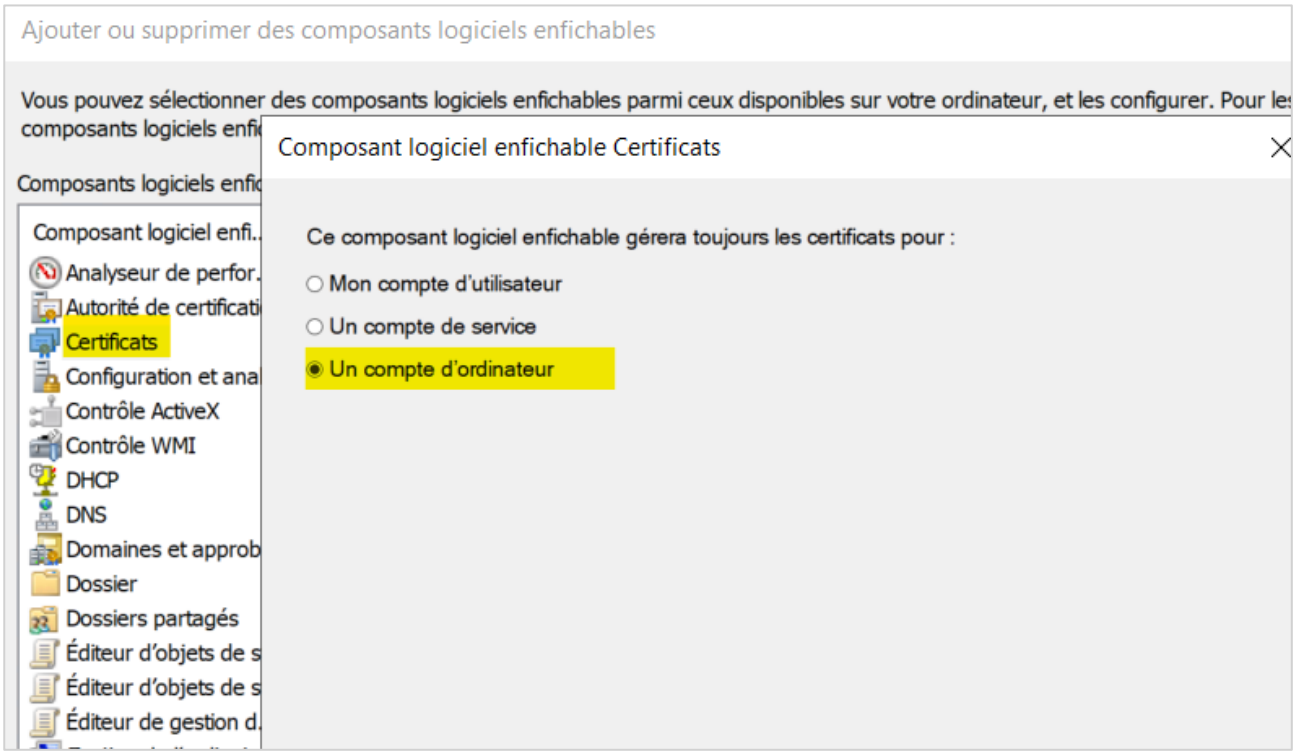
On publie le certificat :

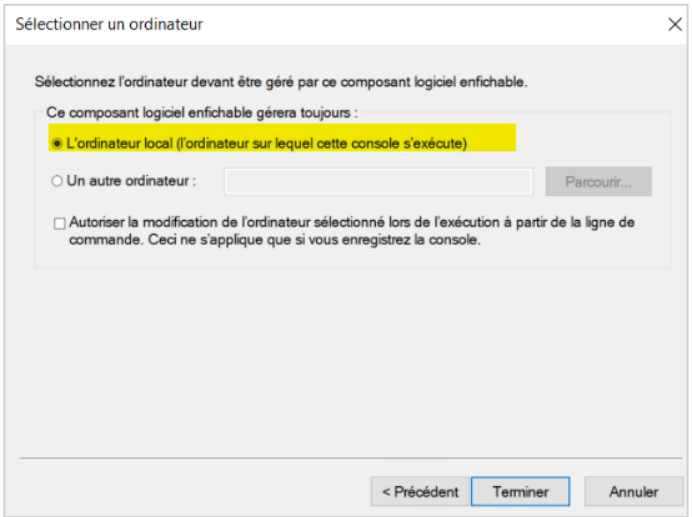


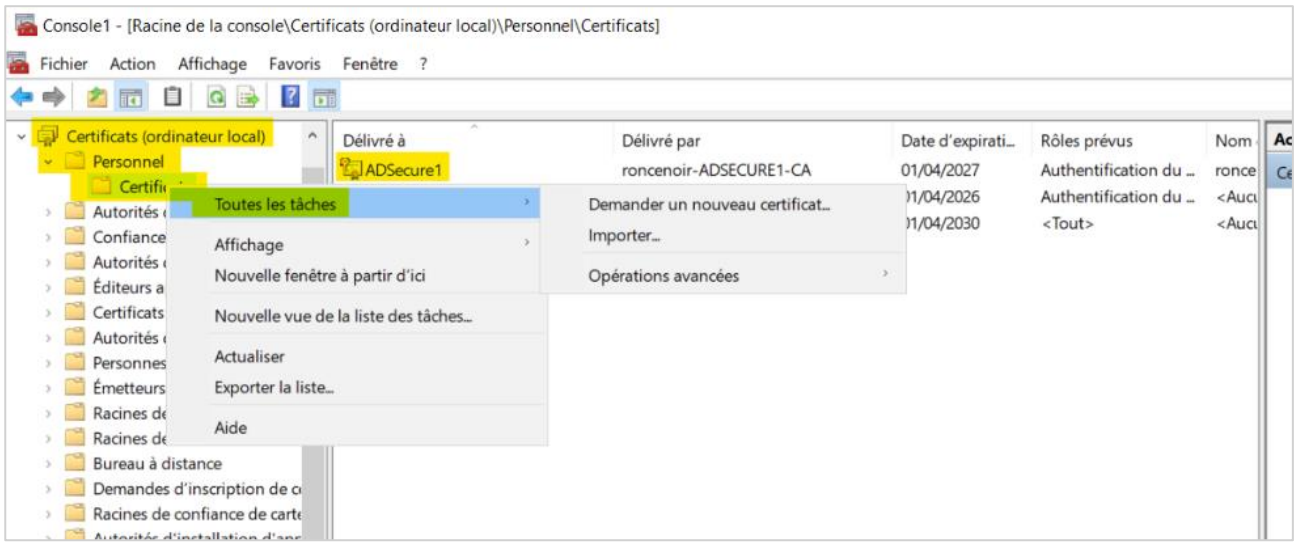


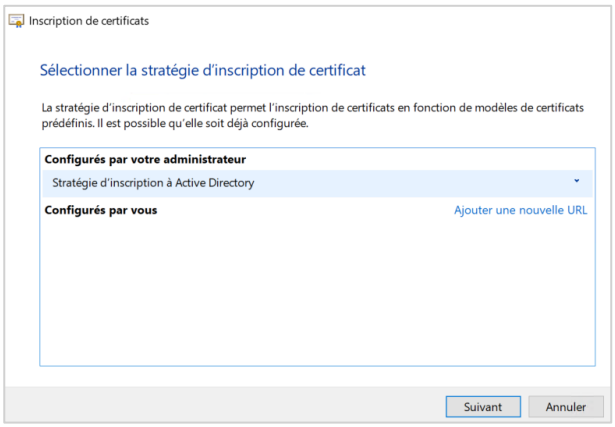
Windows + R >>> Ecrire MMC

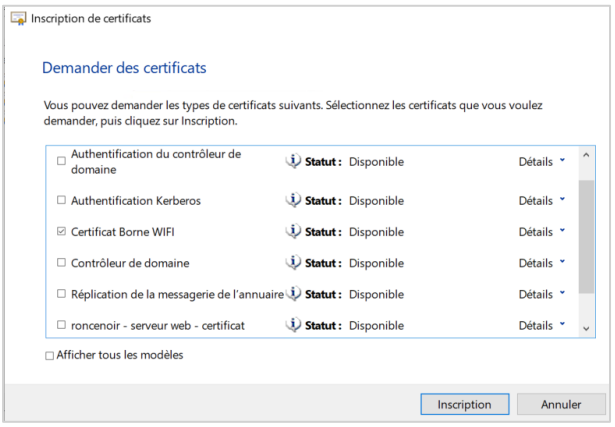

Console1 - [Racine de la console]
Fichier
Action
Affichage
Favoris
Fenêtre
?
Nouveau Ctrl+N
Ouvrir... Ctrl+O
Enregistrer Ctrl+S
Enregistrer sous...
Ajouter/Supprimer un composant logiciel enfichable... Ctrl+M
Options...
1 certtmpl.msc
2 wbadmin.msc
3 dsa.msc
4 gpmc.msc
Quitter
Aucun élément à afficher dans cet aperçu.


Ajouter ou supprimer des composants logiciels enfichables
Vous pouvez sélectionner des composants logiciels enfichables parmi ceux disponibles sur votre ordinateur, et les configurer. Pour les
composants logiciels enfi
Composants logiciels enfic
Composant logiciel enfi...
Analyseur de perfor...
Autorité de certificati
Certificats
Configuration et anal
Contrôle ActiveX
Contrôle WMI
DHCP
DNS
Domaines et approb
Dossier
Dossiers partagés
Éditeur d'objets de s
Éditeur d'objets de s
Éditeur de gestion d...
Composant logiciel enfichable Certificats
Ce composant logiciel enfichable gérera toujours les certificats pour :
Mon compte d'utilisateur
Un compte de service
Un compte d'ordinateur

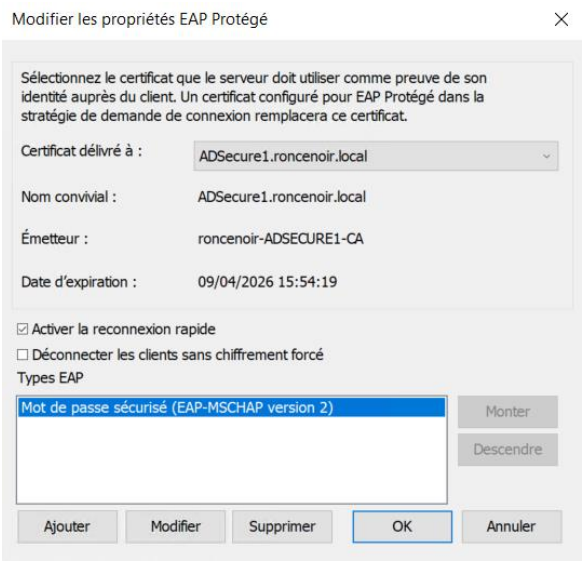

Sélectionner un ordinateur
Sélectionnez l'ordinateur devant être géré par ce composant logiciel enfichable.
Ce composant logiciel enfichable gérera toujours :
L'ordinateur local (l'ordinateur sur lequel cette console s'exécute)
Un autre ordinateur :
Parcourir...
Autoriser la modification de l'ordinateur sélectionné lors de l'exécution à partir de la ligne de commande. Ceci ne s'applique que si vous enregistrez la console.
< Précédent
Terminer
Annuler





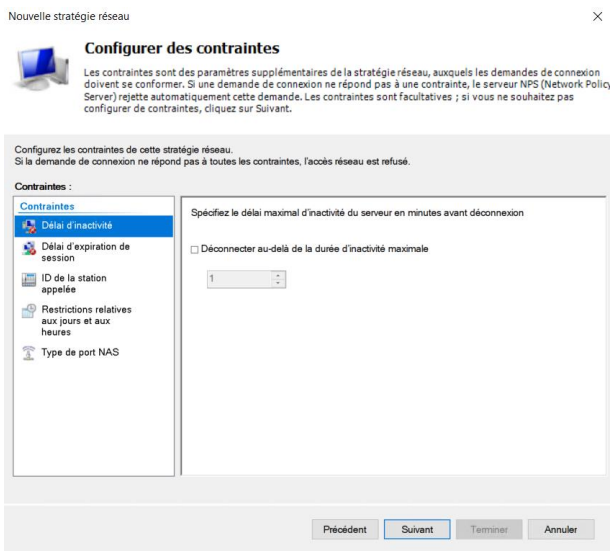


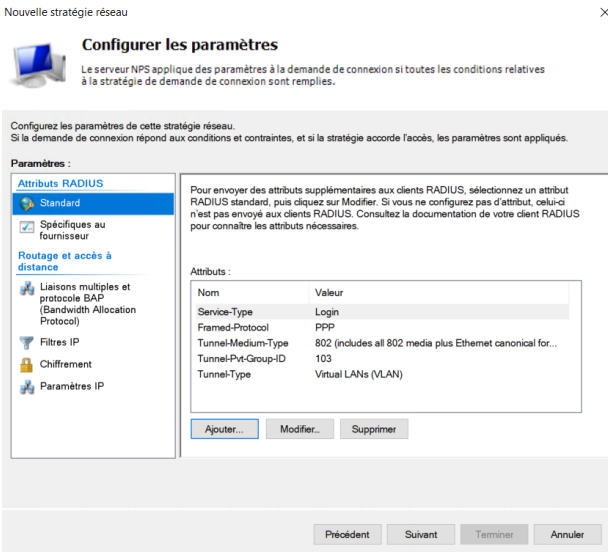
On applique le certificat :



Je peux ensuite configurer différents paramètres de connexion. Cela ne nous intéresse pas pour le moment.

On clic sur suivant, puis on supprime les attributs déjà entrés dans la configuration des paramètres pour ajouter « service type » à la place. Pour les informations d'attributs, on clic sur « autres » et on sélectionne login.

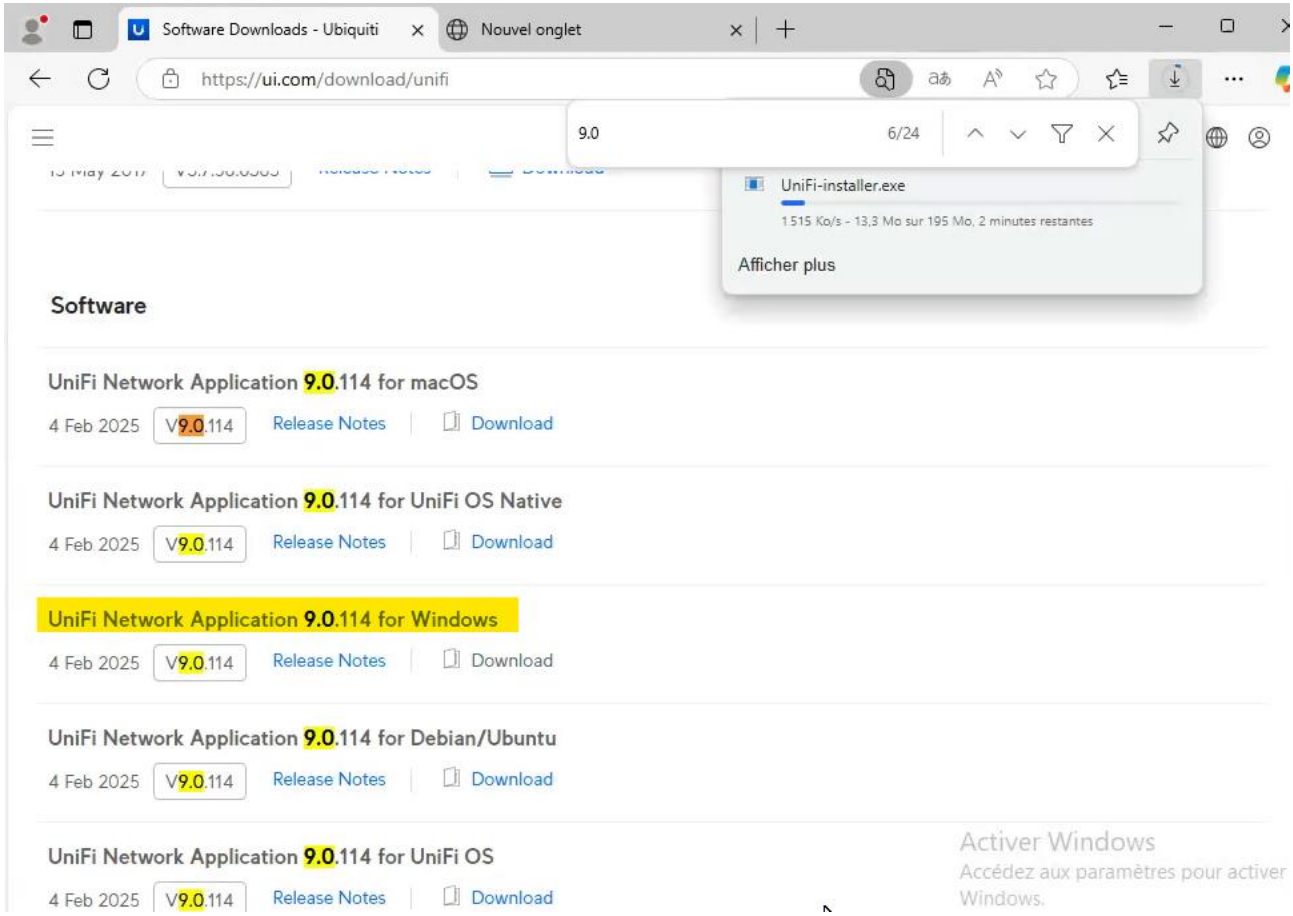




C’est bon c’est paramétré !

Configurons notre borne wifi

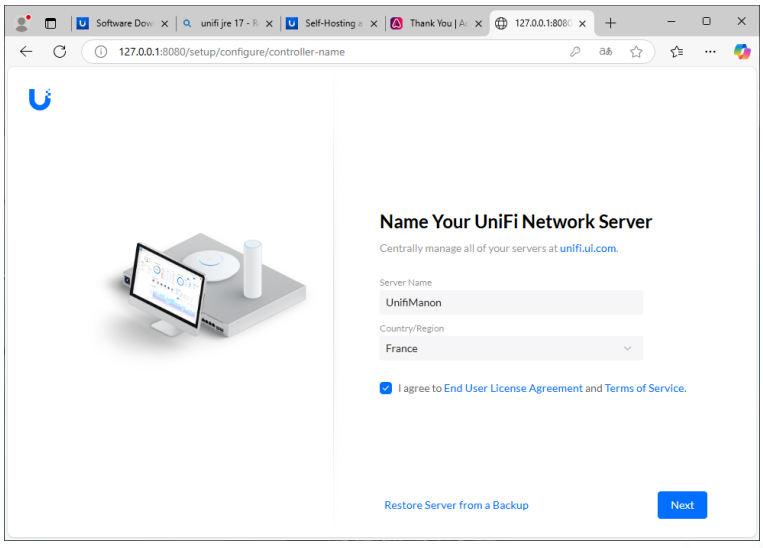
Sur une vm windows 10 installer unifi network application.

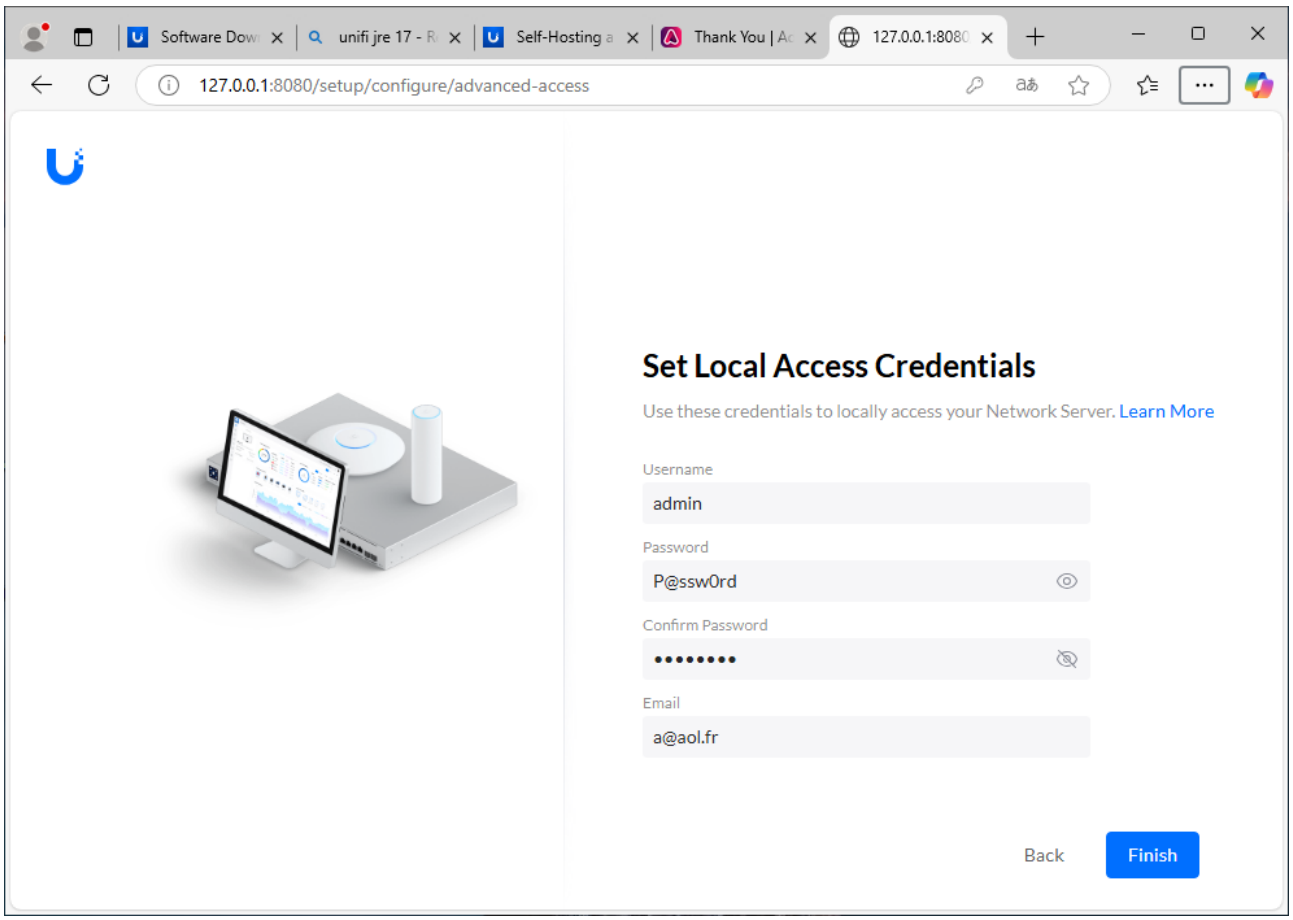


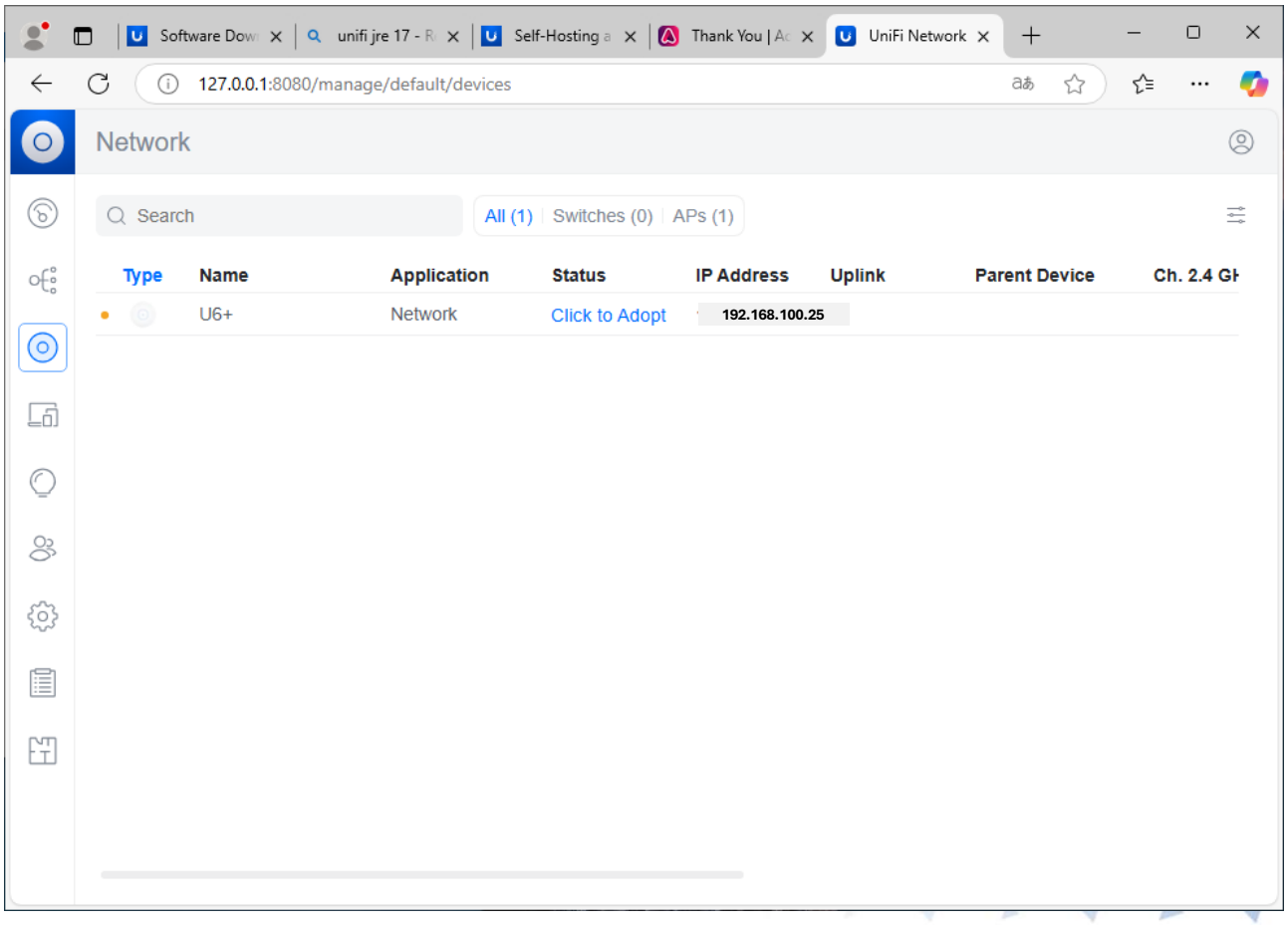
On lance l'installeur : UniFi-installer

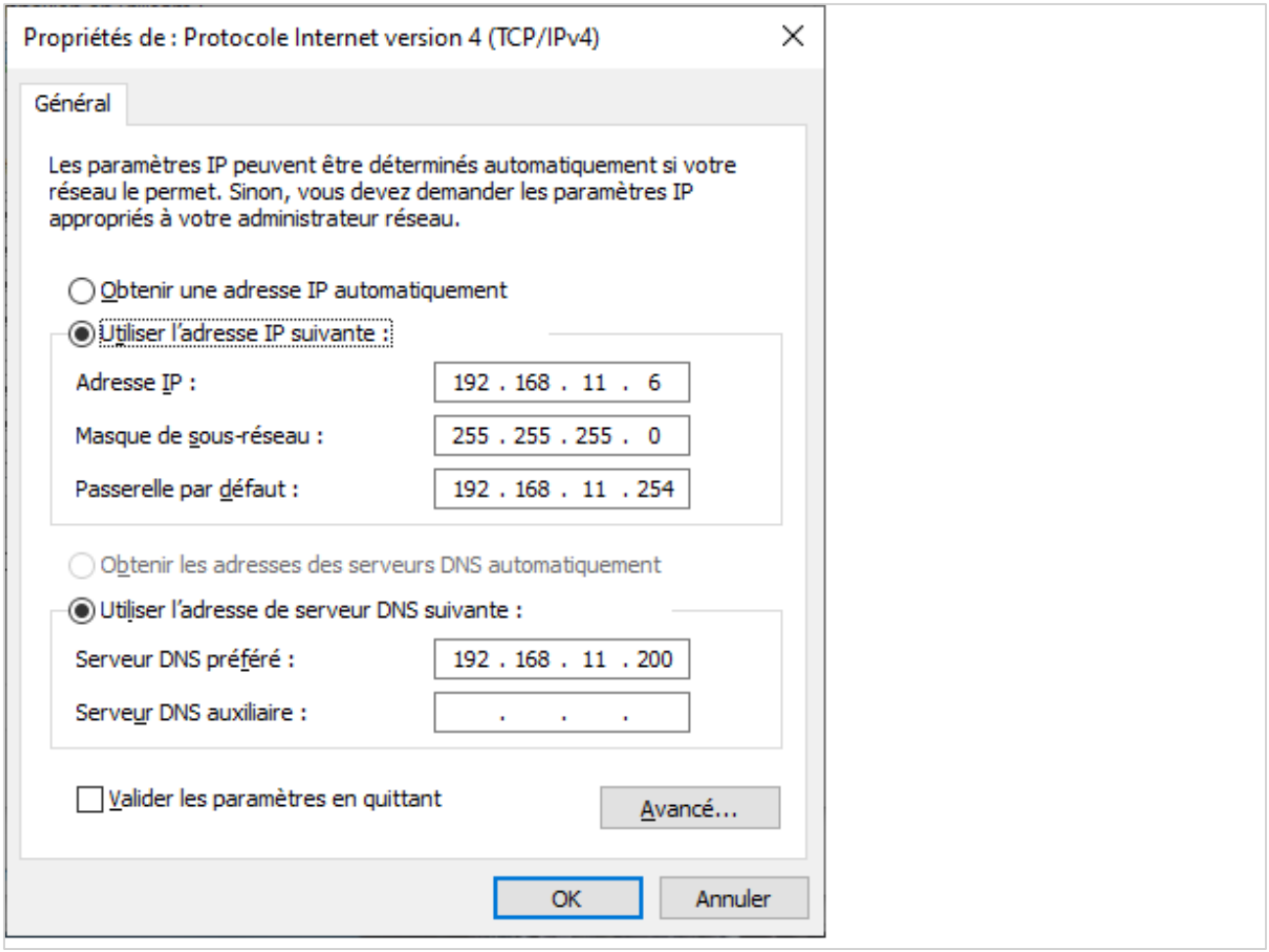
On installe en suivant ce que le logiciel nous dit.

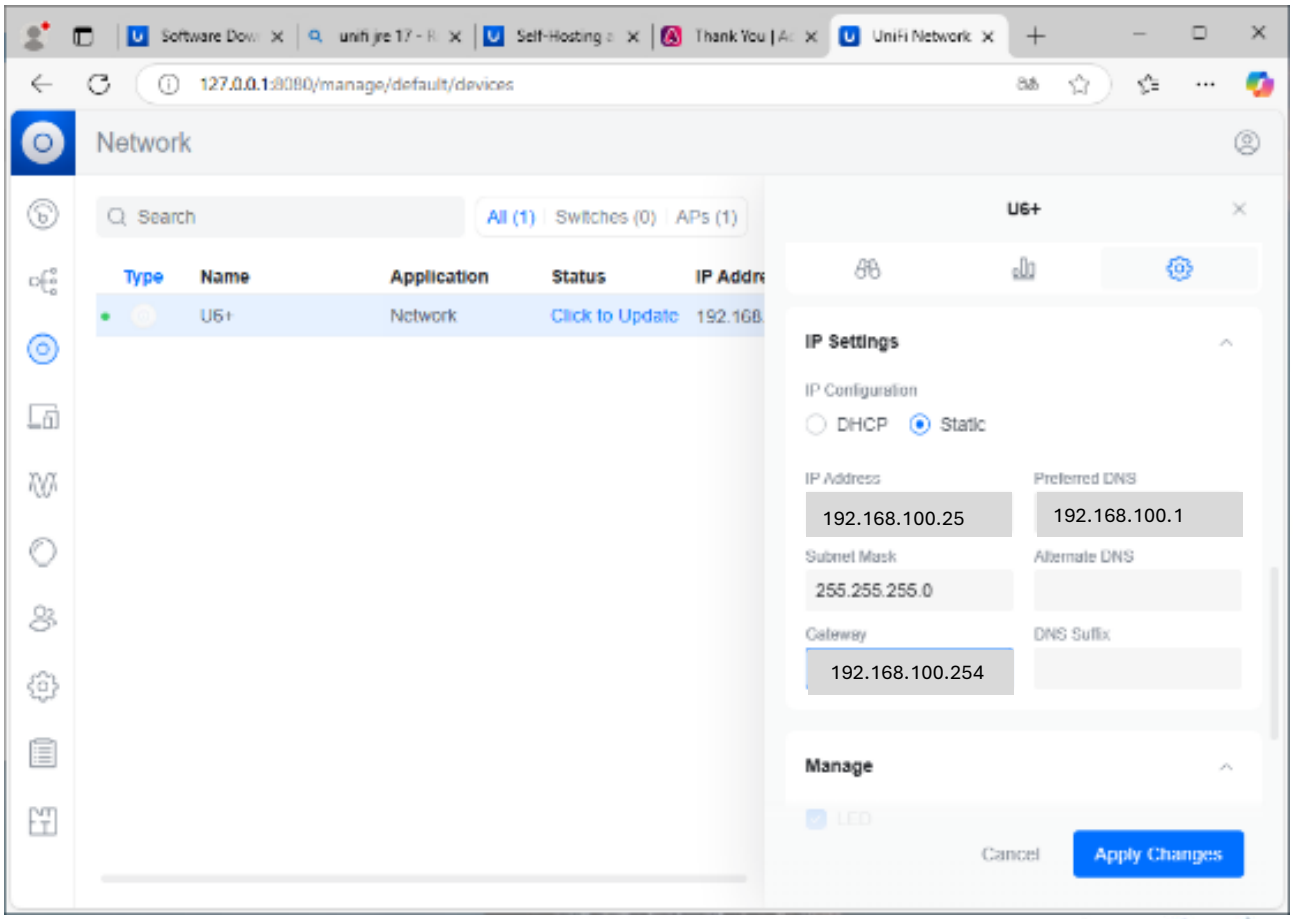
On lance unifi et on le configure :

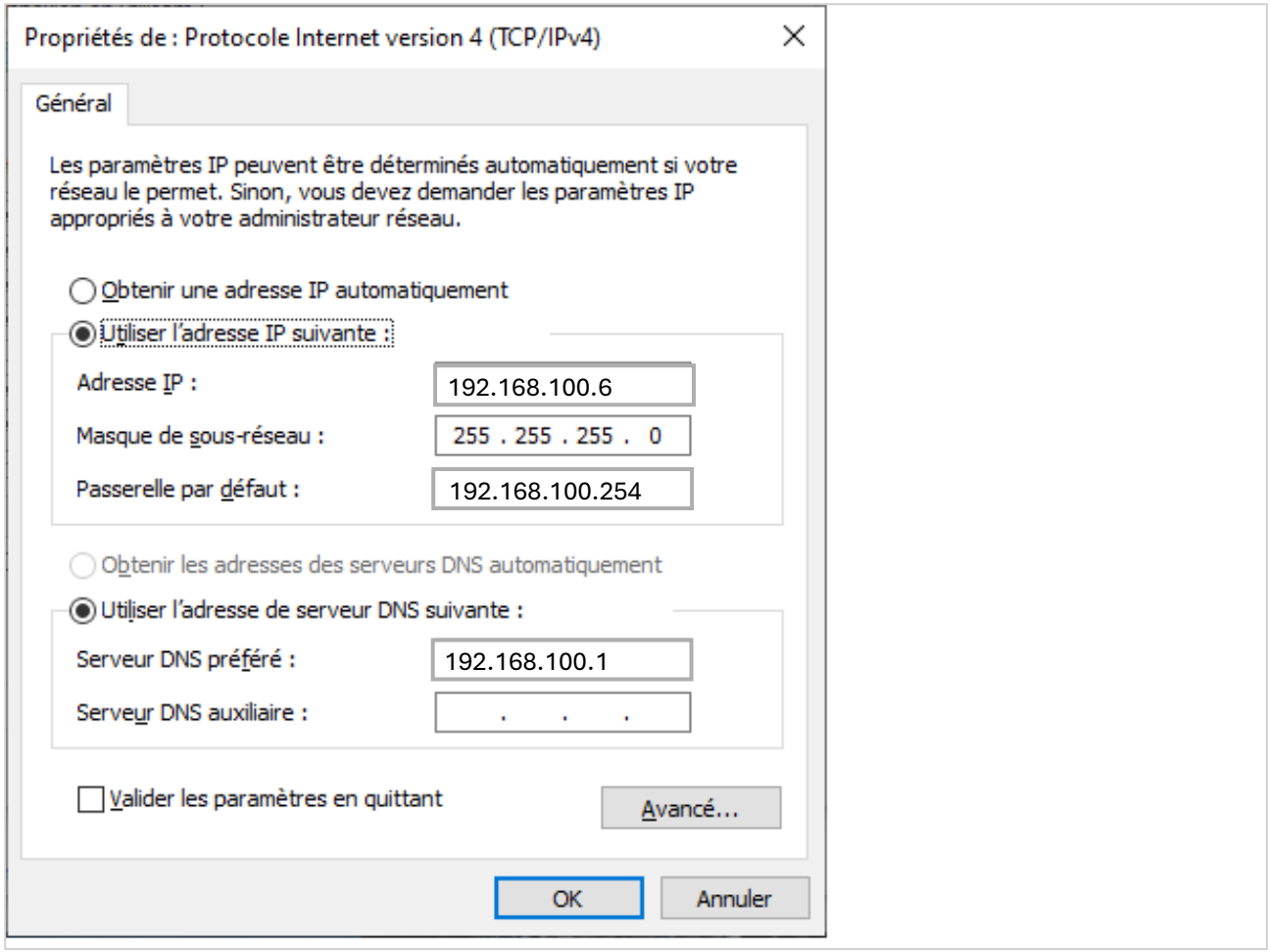


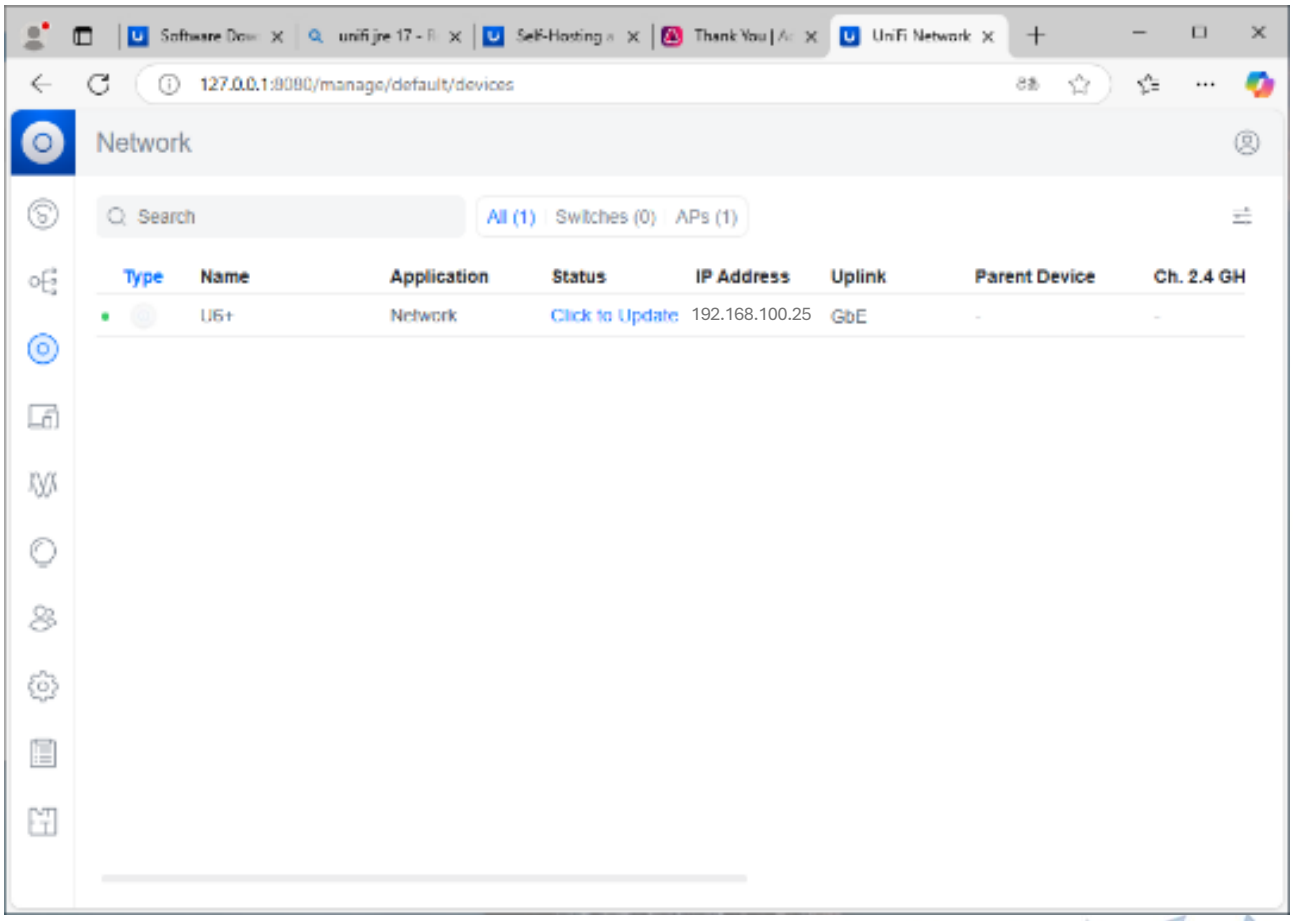

Software Dow
unifi jre 17 - R
Self-Hosting a
Thank You | Ac
127.0.0.1:8080
127.0.0.1:8080/setup/configure/advanced-access
Set Local Access Credentials
Use these credentials to locally access your Network Server. Learn More
Username
admin
Password
P@ssw0rd
Confirm Password
Email
a@aol.fr
Back
Finish

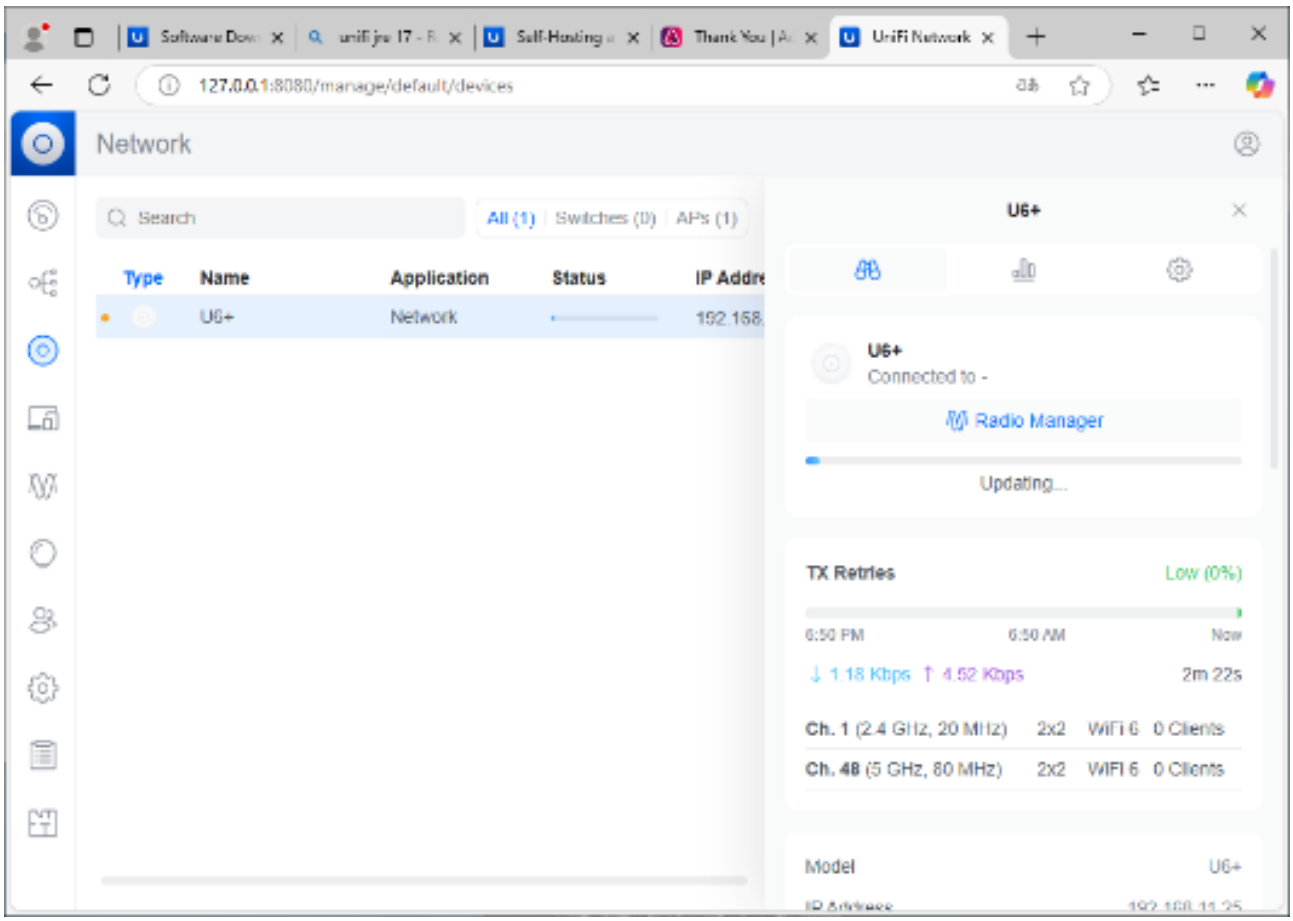

Software Dow
unifi jre 17 - R
Self-Hosting a
Thank You | Ac
UniFi Network
127.0.0.1:8080/manage/default/devices
Network
Search
All (1)
Switches (0)
APs (1)
Type
Name
Application
Status
IP Address
Uplink
Parent Device
Ch. 2.4 GH
U6+
Network
Click to Adopt
192.168.100.25


Propriétés de : Protocole Internet version 4 (TCP/IPv4)
Général
Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.
Obtenir une adresse IP automatiquement
Utiliser l'adresse IP suivante :
Adresse IP : 192 . 168 . 11 . 6
Masque de sous-réseau : 255 . 255 . 255 . 0
Passerelle par défaut : 192 . 168 . 11 . 254
Obtenir les adresses des serveurs DNS automatiquement
Utiliser l'adresse de serveur DNS suivante :
Serveur DNS préféré : 192 . 168 . 11 . 200
Serveur DNS auxiliaire :
Valider les paramètres en quittant
Avancé...
OK
Annuler

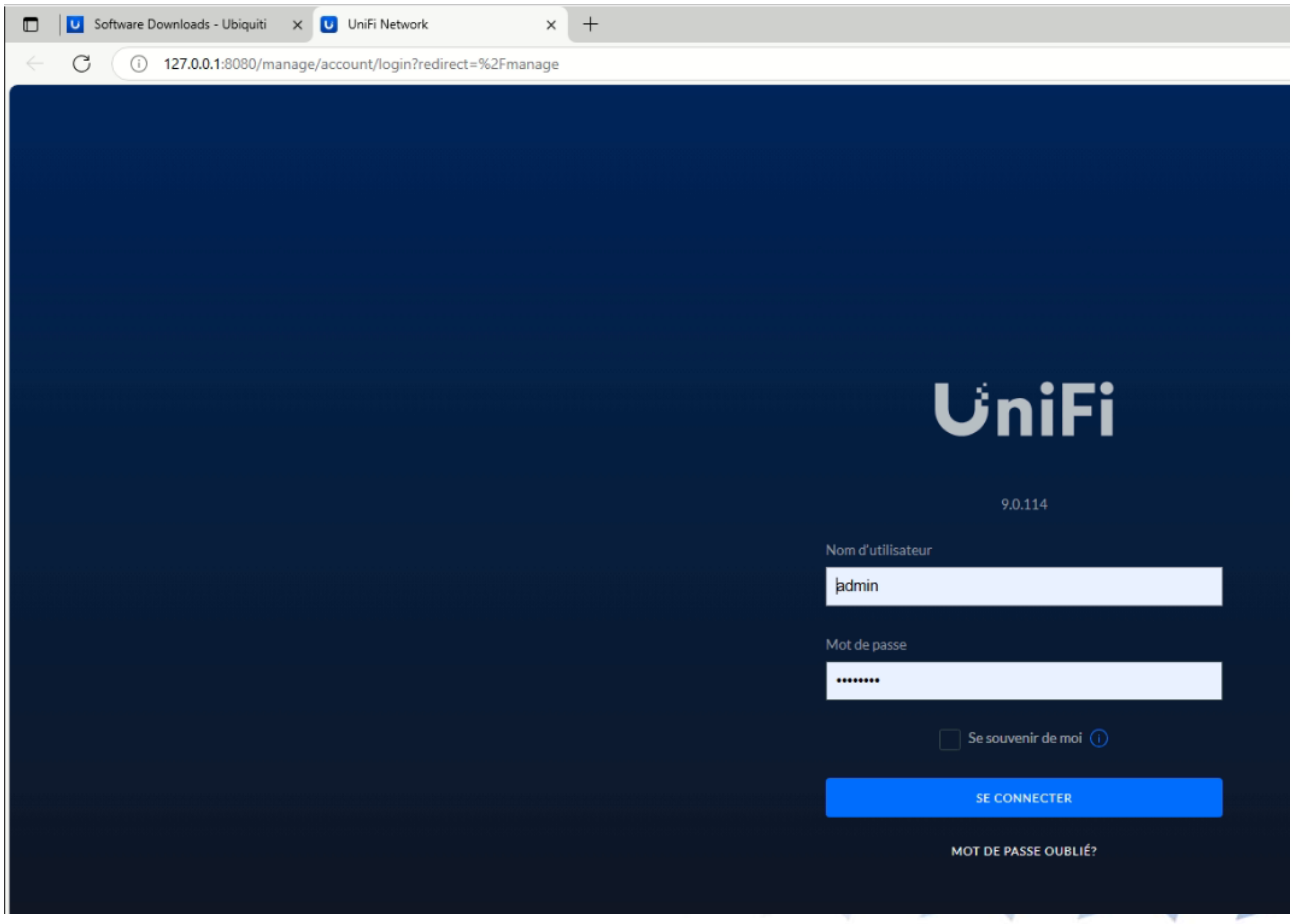

UniFi Network
127.0.0.1:8080/manage/default/devices
Network
Search
All (1)
Switches (0)
APs (1)
Type
Name
Application
Status
IP Addr
U6+
Network
Click to Update
192.168.
U6+
IP Settings
IP Configuration
DHCP
Static
IP Address
192.168.100.25
Preferred DNS
192.168.100.1
Subnet Mask
255.255.255.0
Alternate DNS
Gateway
192.168.100.254
DNS Suffix
Manage
Cancel
Apply Changes


Propriétés de : Protocole Internet version 4 (TCP/IPv4)
Général
Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.
Obtenir une adresse IP automatiquement
Utiliser l'adresse IP suivante :
Adresse IP : 192.168.100.6
Masque de sous-réseau : 255 . 255 . 255 . 0
Passerelle par défaut : 192.168.100.254
Obtenir les adresses des serveurs DNS automatiquement
Utiliser l'adresse de serveur DNS suivante :
Serveur DNS préféré : 192.168.100.1
Serveur DNS auxiliaire :
Valider les paramètres en quittant
Avancé...
OK
Annuler

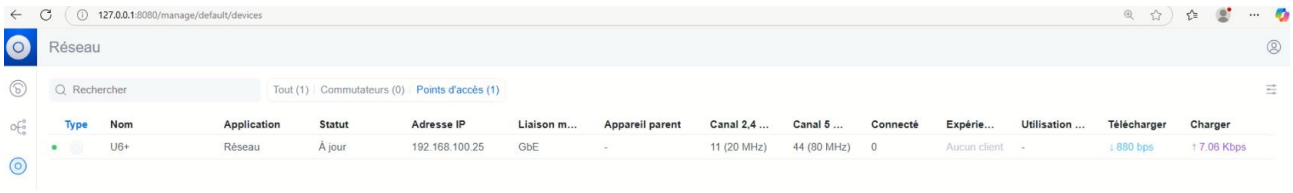

UniFi Network
127.0.0.1:8080/manage/default/devices
Network
Search
All (1)
Switches (0)
APs (1)
Type
Name
Application
Status
IP Address
Uplink
Parent Device
Ch. 2.4 GH
U6+
Network
Click to Update
192.168.100.25
GbE

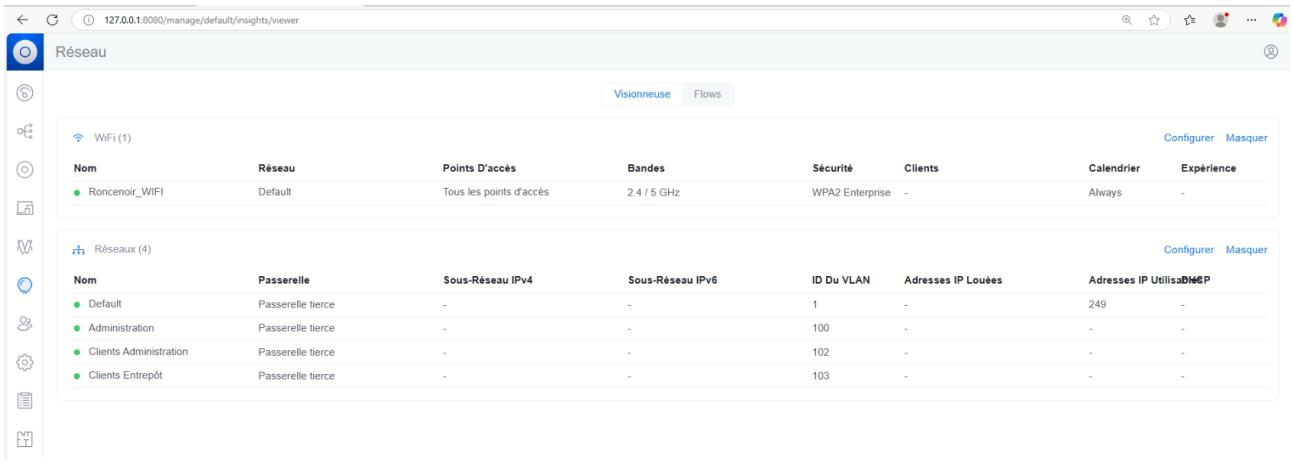


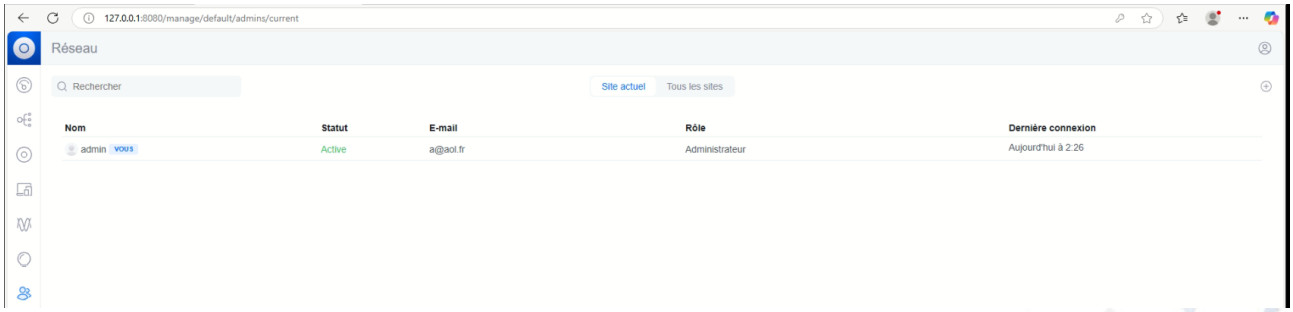
Se connecter à l'application :

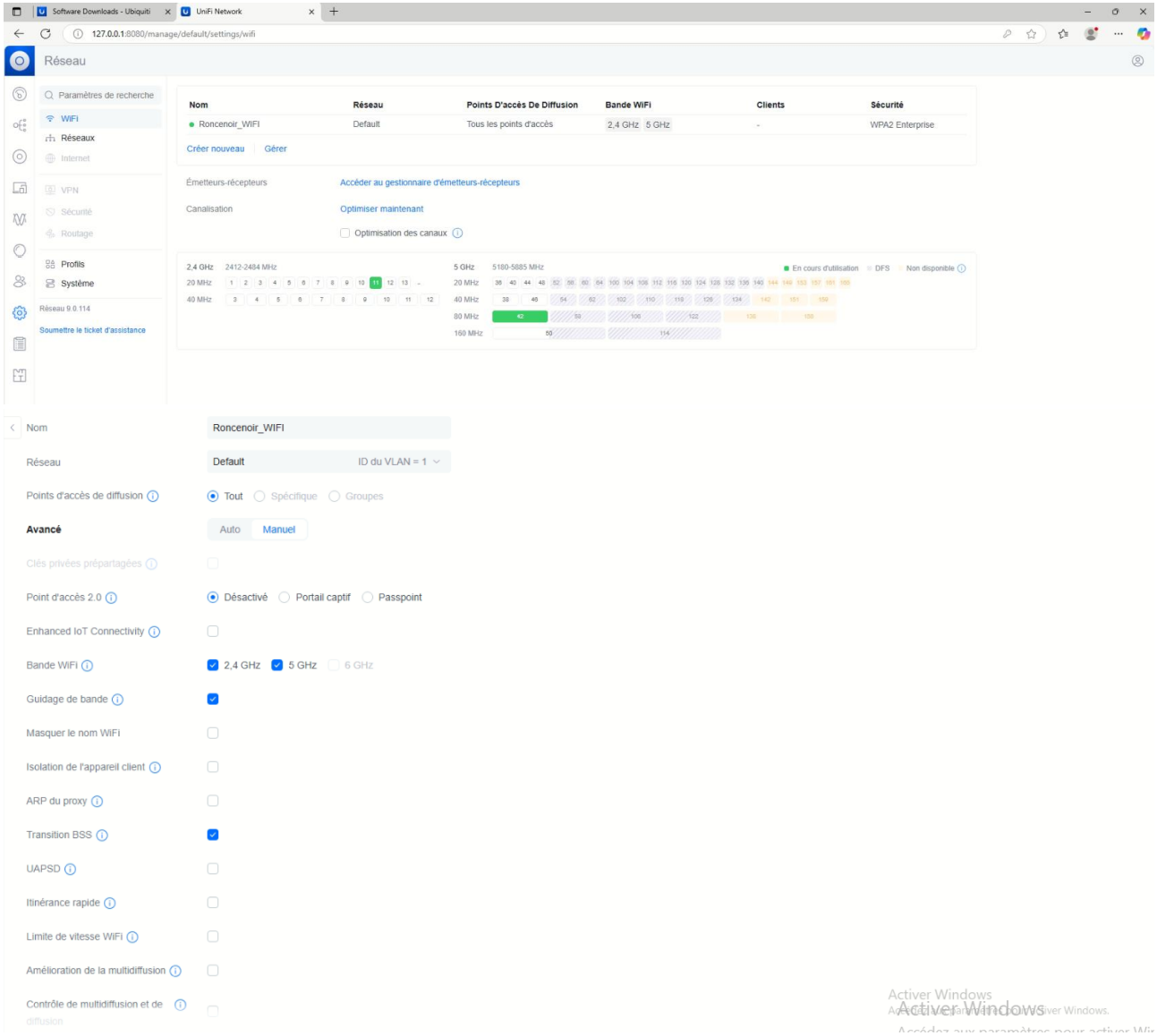


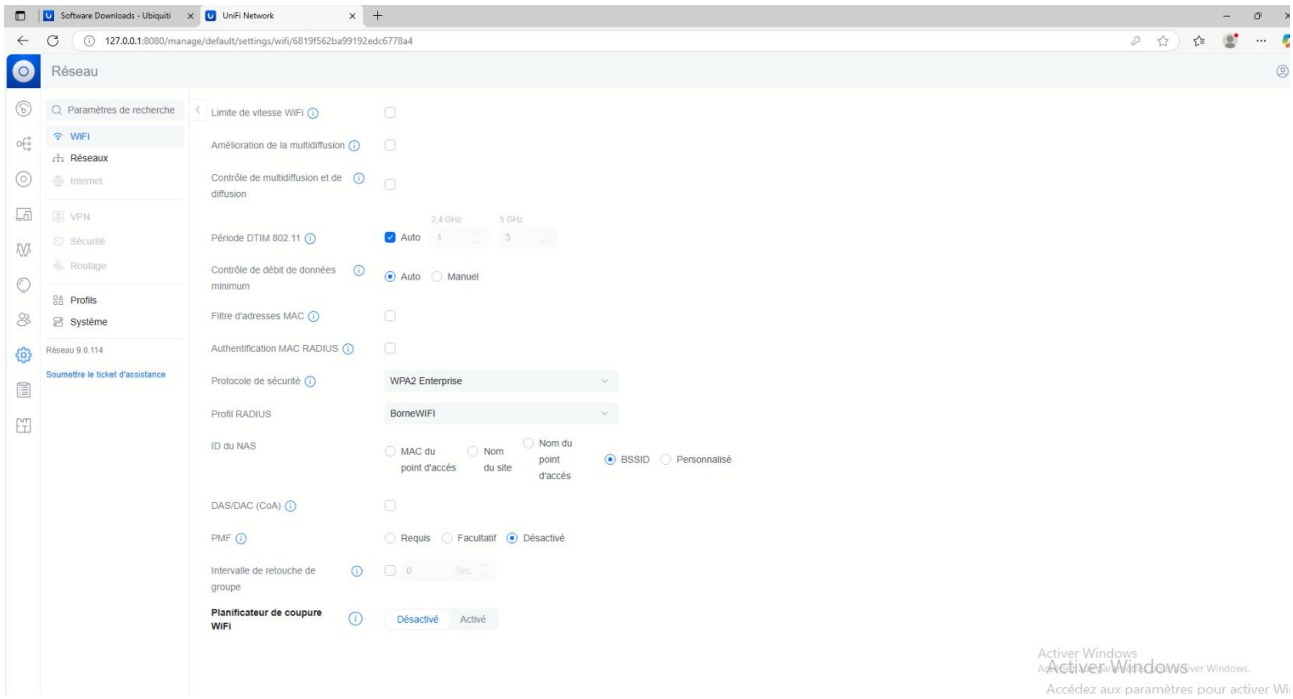
Configuration après liaison au radius :

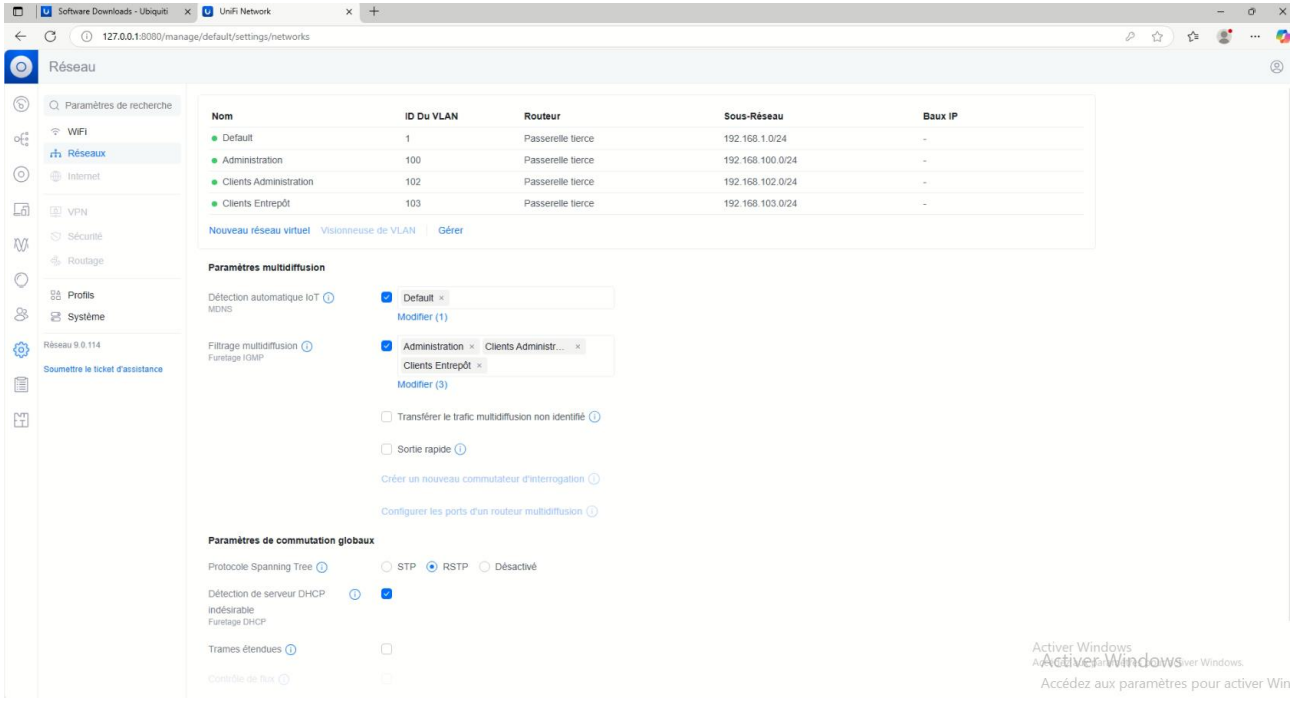


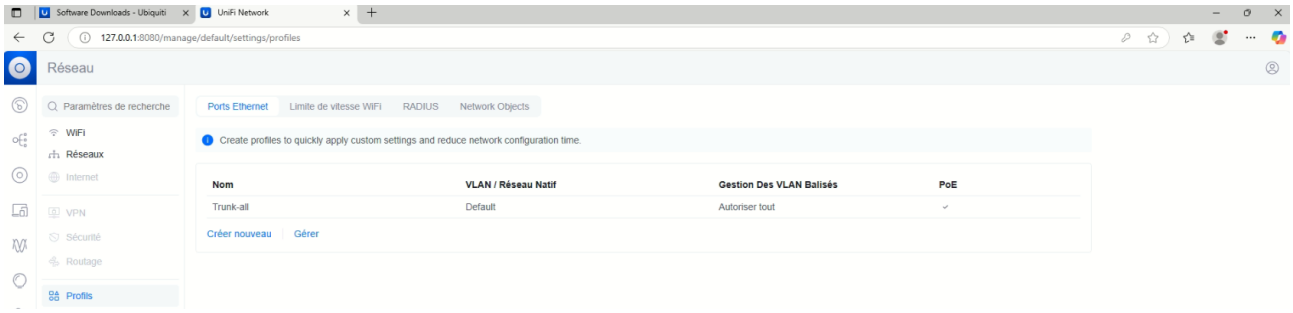


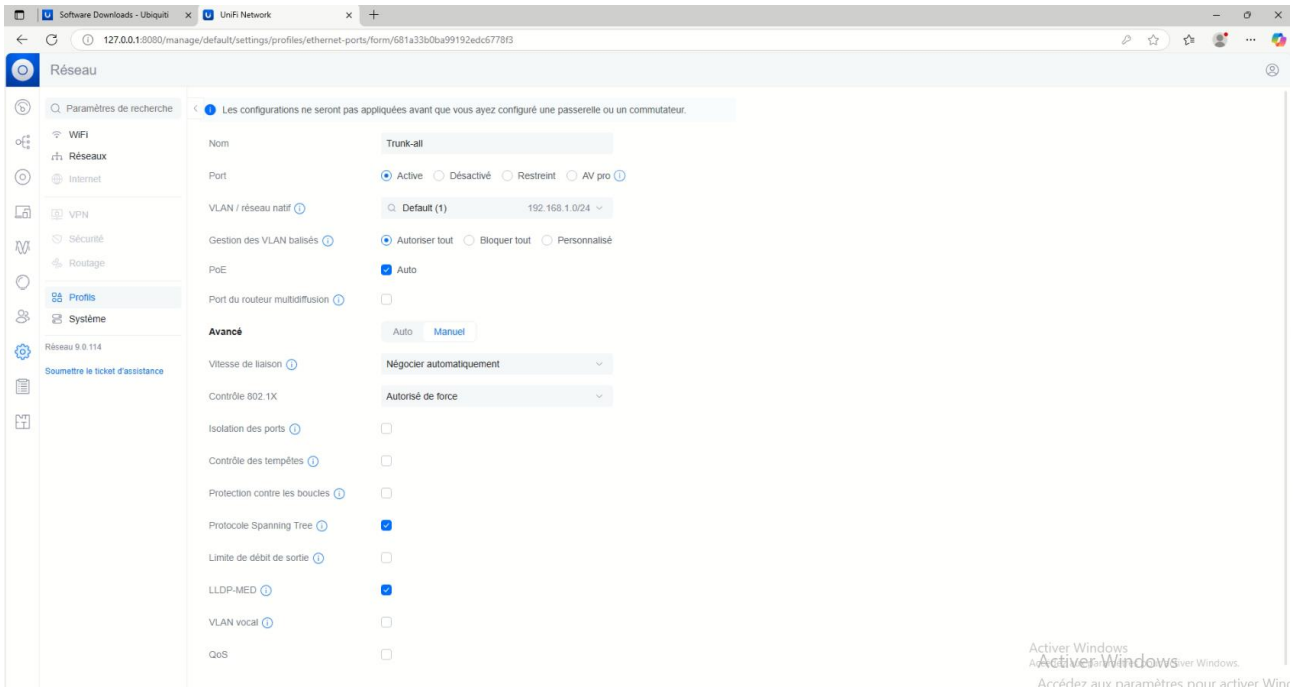


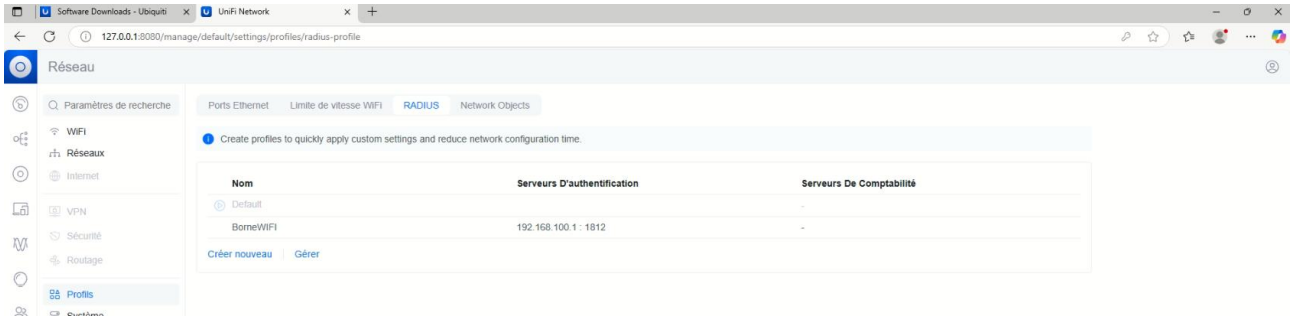


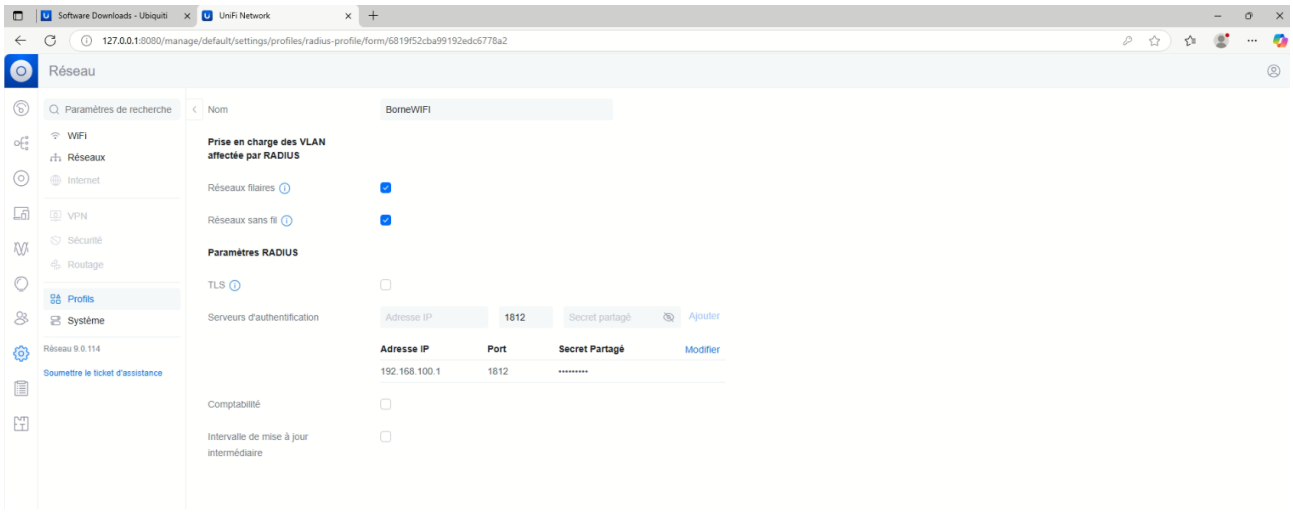


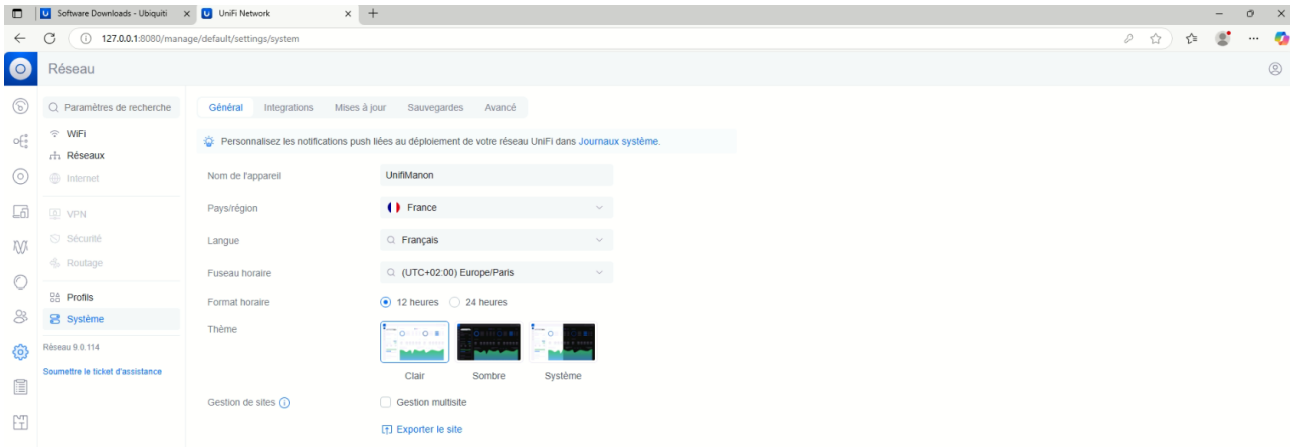

Software Downloads - Ubiquiti
UniFi Network
127.0.0.1:8080/manage/default/settings/networks
Réseau
Paramètres de recherche
WiFi
Réseaux
Internet
VPN
Sécurité
Routage
Profils
Système
Réseau 9.0.114
Soumettre le ticket d'assistance
Nom
ID Du VLAN
Routeur
Sous-Réseau
Baux IP
Default
1
Passerelle tierce
192.168.1.0/24
Administration
100
Passerelle tierce
192.168.100.0/24
Clients Administration
102
Passerelle tierce
192.168.102.0/24
Clients Entrepôt
103
Passerelle tierce
192.168.103.0/24
Nouveau réseau virtuel
Visionneuse de VLAN
Gérer
Paramètres multidiffusion
Détection automatique IoT
MDNS
Default
Modifier (1)
Filtrage multidiffusion
Furetage IGMP
Administration
Clients Entrepôt
Modifier (3)
Transférer le trafic multidiffusion non identifié
Sortie rapide
Créer un nouveau commutateur d'interrogation
Configurer les ports d'un routeur multidiffusion
Paramètres de commutation globaux
Protocole Spanning Tree
STP
RSTP
Désactivé
Détection de serveur DHCP indésirable
Furetage DHCP
Trames étendues
Activer Windows


Software Downloads - Ubiquiti
UniFi Network
127.0.0.1:8080/manage/default/settings/profiles
Réseau
Paramètres de recherche
WiFi
Réseaux
Internet
VPN
Sécurité
Routage
Profils
Ports Ethernet
Limite de vitesse WiFi
RADIUS
Network Objects
Create profiles to quickly apply custom settings and reduce network configuration time.
Nom
VLAN / Réseau Natif
Gestion Des VLAN Balisés
PoE
Trunk-all
Default
Autoriser tout
Créer nouveau
Gérer


Software Downloads - Ubiquiti
UniFi Network
127.0.0.1:8080/manage/default/settings/profiles/ethernet-ports/form/681a33b0ba99192edc6778f3
Réseau
Paramètres de recherche
WiFi
Réseaux
Internet
VPN
Sécurité
Routage
Profils
Système
Réseau 9.0.114
Soumettre le ticket d'assistance
Les configurations ne seront pas appliquées avant que vous ayez configuré une passerelle ou un commutateur.
Nom
Trunk-all
Port
Active
Désactivé
Restreint
AV pro
VLAN / réseau natif
Default (1)
192.168.1.0/24
Gestion des VLAN balisés
Autoriser tout
Bloquer tout
Personnalisé
PoE
Auto
Port du routeur multidiffusion
Avancé
Auto
Manuel
Vitesse de liaison
Négocier automatiquement
Contrôle 802.1X
Autorisé de force
Isolation des ports
Contrôle des tempêtes
Protection contre les boucles
Protocole Spanning Tree
Limite de débit de sortie
LLDP-MED
VLAN vocal
QoS
Activer Windows


Software Downloads - Ubiquiti
UniFi Network
127.0.0.1:8080/manage/default/settings/profiles/radius-profile
Réseau
Paramètres de recherche
WiFi
Réseaux
Internet
VPN
Sécurité
Routage
Profils
Ports Ethernet
Limite de vitesse WiFi
RADIUS
Network Objects
Create profiles to quickly apply custom settings and reduce network configuration time.
Nom
Serveurs D'authentification
Serveurs De Comptabilité
Default
BorneWIFI
192.168.100.1 : 1812
Créer nouveau
Gérer


Software Downloads - Ubiquiti
UniFi Network
127.0.0.1:8080/manage/default/settings/profiles/radius-profile/form/6819f52cba99192edc6778a2
Réseau
Paramètres de recherche
WiFi
Réseaux
Internet
VPN
Sécurité
Routage
Profils
Système
Réseau 9.0.114
Soumettre le ticket d'assistance
Nom
BorneWIFI
Prise en charge des VLAN affectée par RADIUS
Réseaux filaires
Réseaux sans fil
Paramètres RADIUS
TLS
Serveurs d'authentification
Adresse IP
1812
Secret partagé
Ajouter
Adresse IP
Port
Secret Partagé
Modifier
192.168.100.1
1812
Comptabilité
Intervalle de mise à jour intermédiaire


Software Downloads - Ubiquiti
UniFi Network
127.0.0.1:8080/manage/default/settings/system
Réseau
Paramètres de recherche
WiFi
Réseaux
Internet
VPN
Sécurité
Routage
Profils
Système
Réseau 9.0.114
Soumettre le ticket d'assistance
Général
Integrations
Mises à jour
Sauvegardes
Avancé
Personnalisez les notifications push liées au déploiement de votre réseau UniFi dans Journaux système.
Nom de l'appareil
UnifiManon
Pays/région
France
Langue
Français
Fuseau horaire
(UTC+02:00) Europe/Paris
Format horaire
12 heures
24 heures
Thème
Clair
Sombre
Système
Gestion de sites
Gestion multisite
Exporter le site