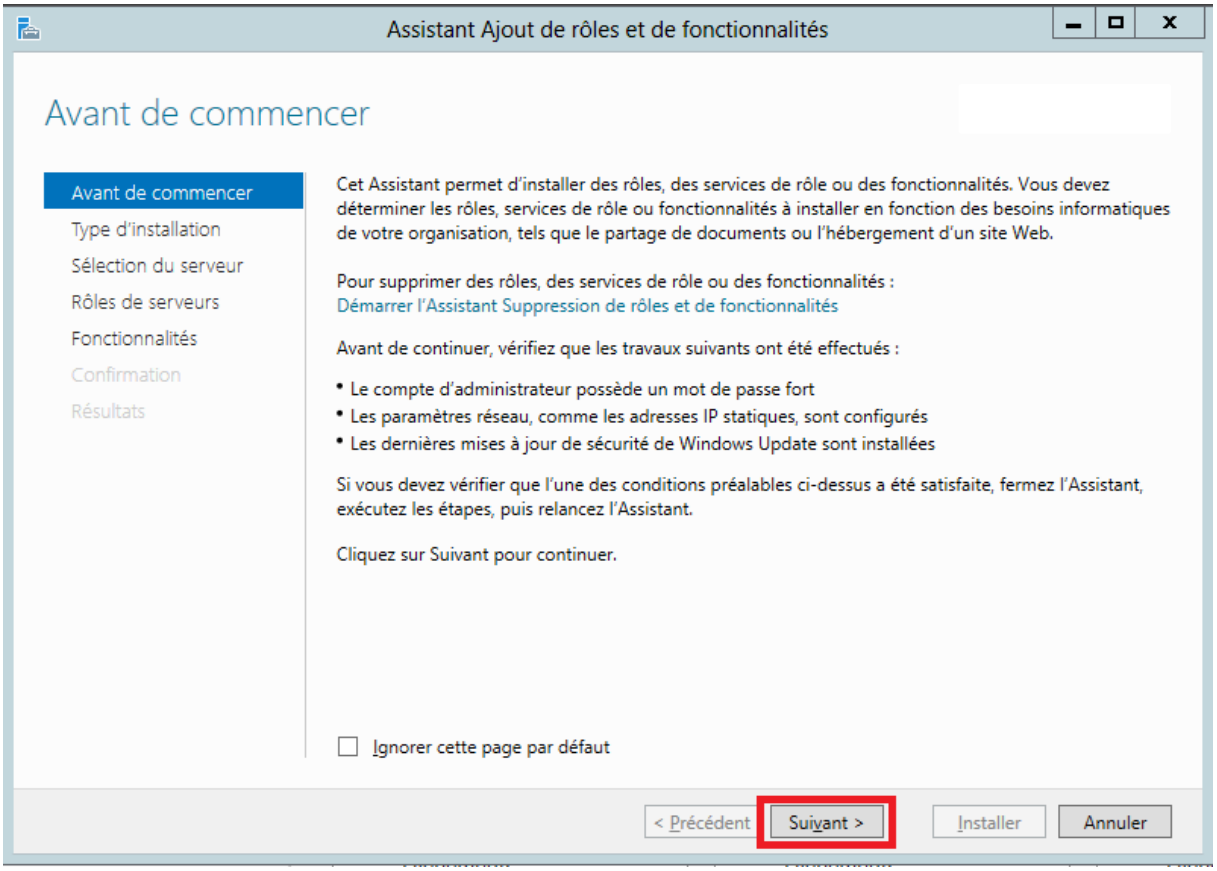
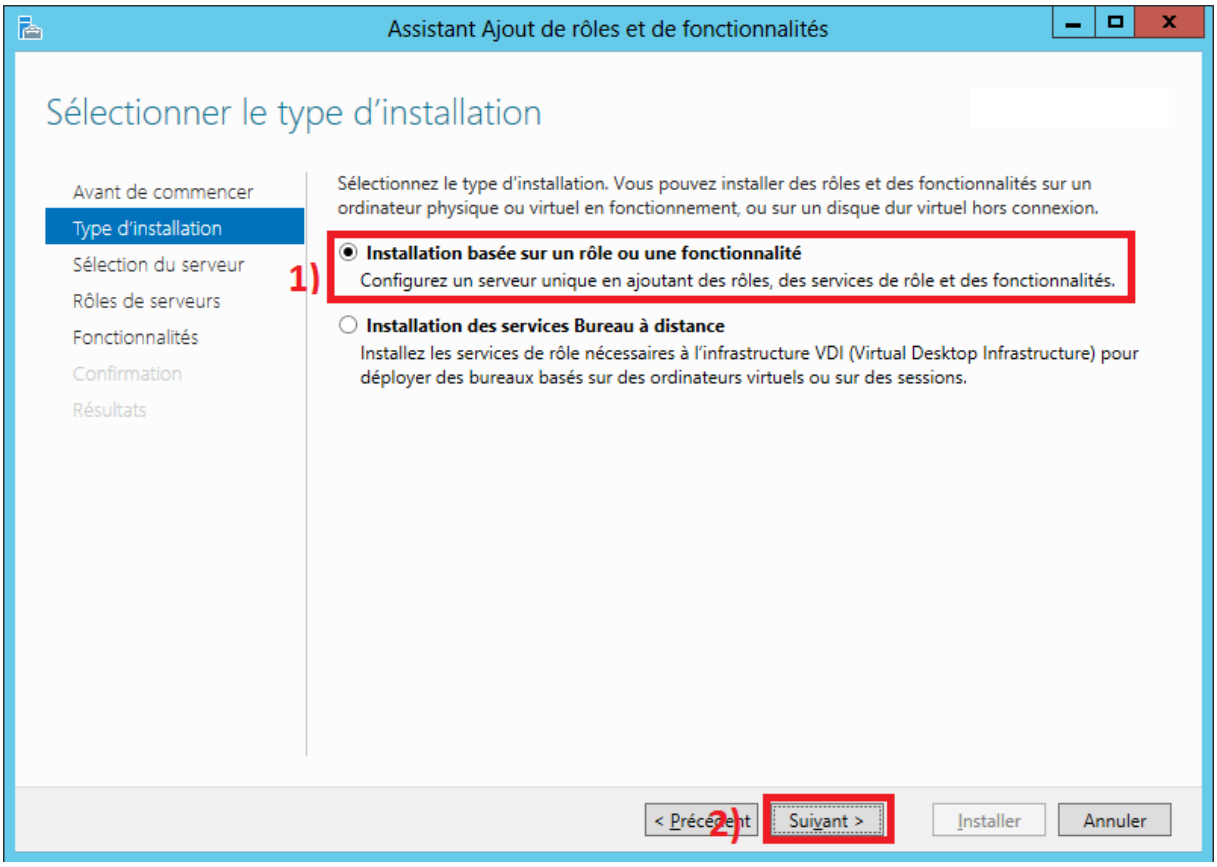
Installation du serveur RADIUS sur une machine
(Remote Authentication Dial-In User Service)

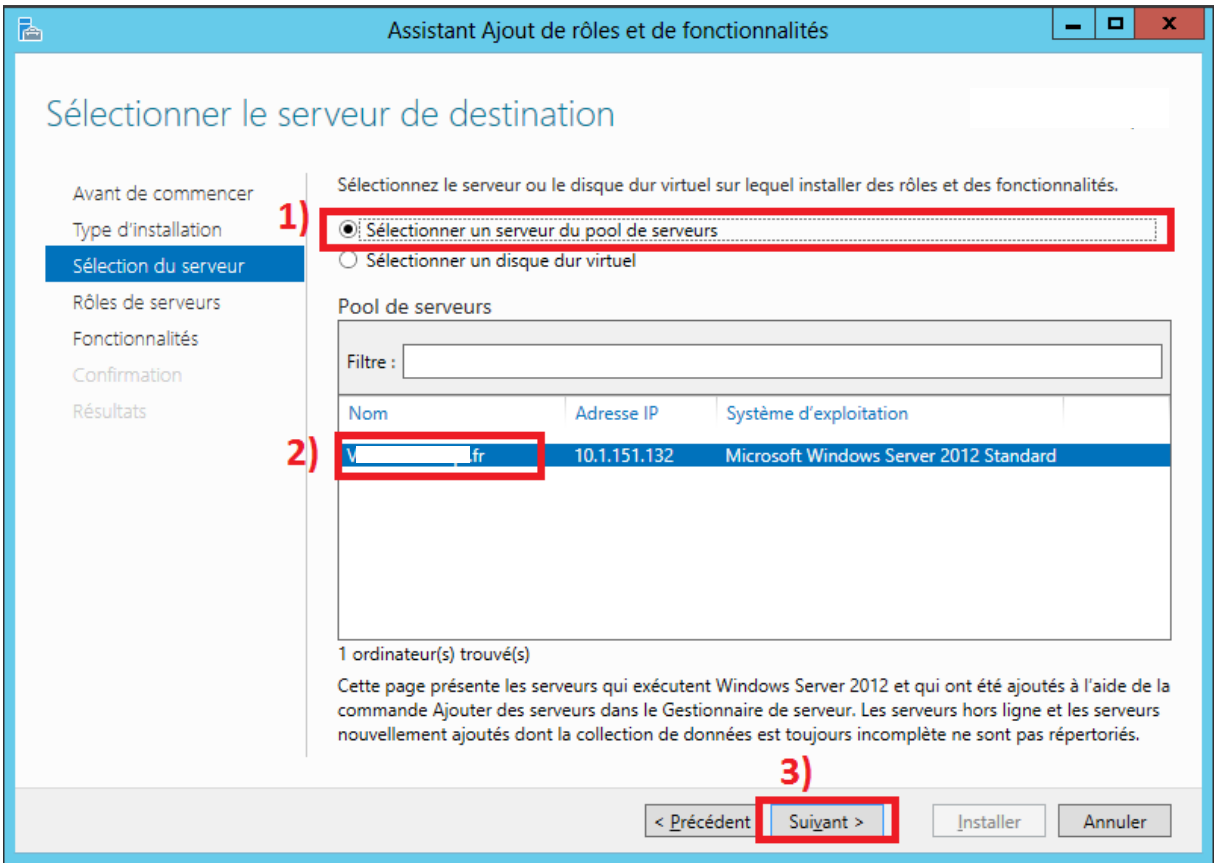
« Le serveur NPS effectue de manière centralisée l'authentification, l'autorisation et la gestion des connexions pour les connexions sans fil, les connexions de commutateurs d'authentification, les connexions d'accès à distance et les connexions VPN, ainsi que pour les connexions aux ordinateurs exécutant la passerelle des services Terminal Services (Passerelle TS). Lorsque vous utilisez le serveur NPS comme serveur RADIUS, vous devez configurer les serveurs d'accès réseau, tels que les points d'accès sans fil et les serveurs VPN, en tant que clients RADIUS sur le serveur NPS. Vous devez également configurer les stratégies réseau que le serveur NPS utilise pour autoriser les demandes de connexion. Vous pouvez configurer la gestion RADIUS de manière à ce que le serveur NPS enregistre les informations de gestion dans des fichiers journaux sur le disque dur local ou dans une base de données Microsoft® SQL Server™. »

Source : https://technet.microsoft.com/fr-fr/library/cc733085%28v=ws.10%29.aspx

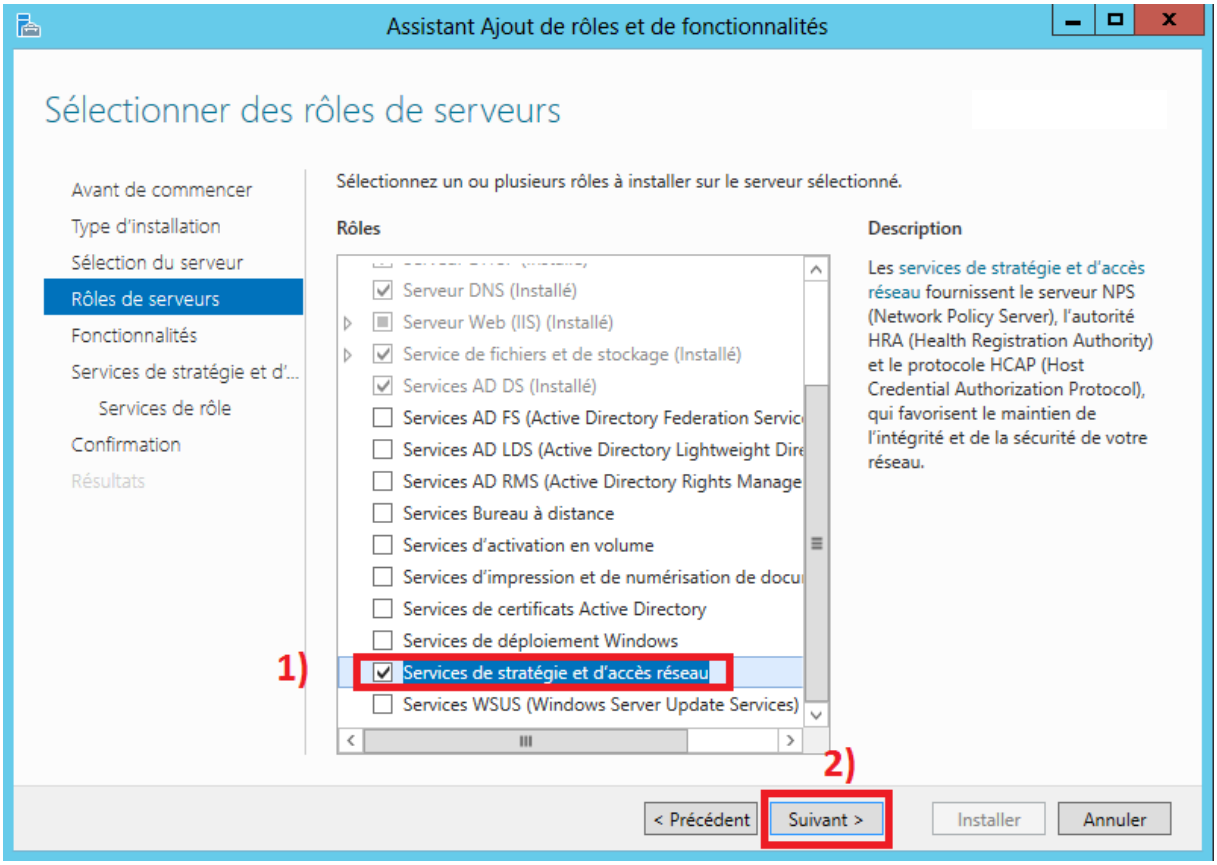
Pour installer le serveur RADIUS, lancer l'*Assistant ajout de rôles et de fonctionnalités* depuis le *Gestionnaire de serveur*.

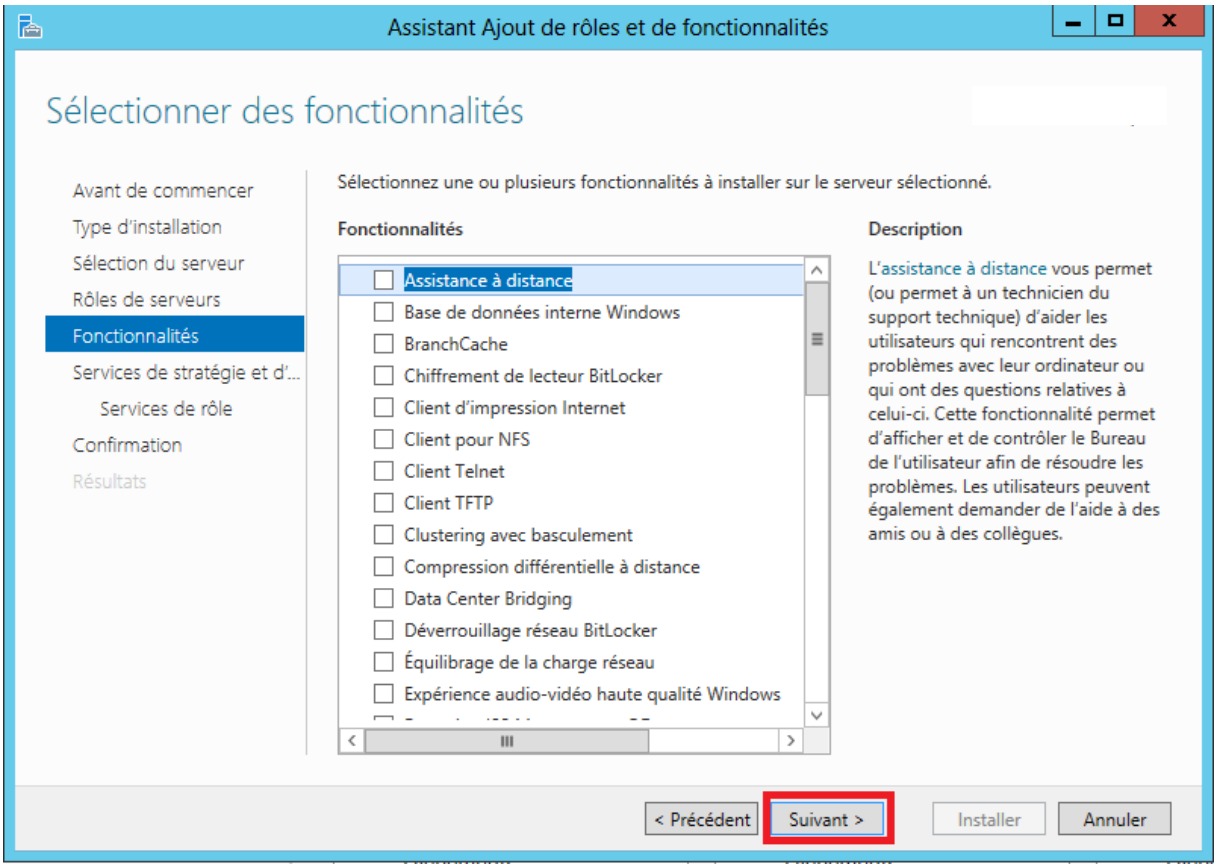


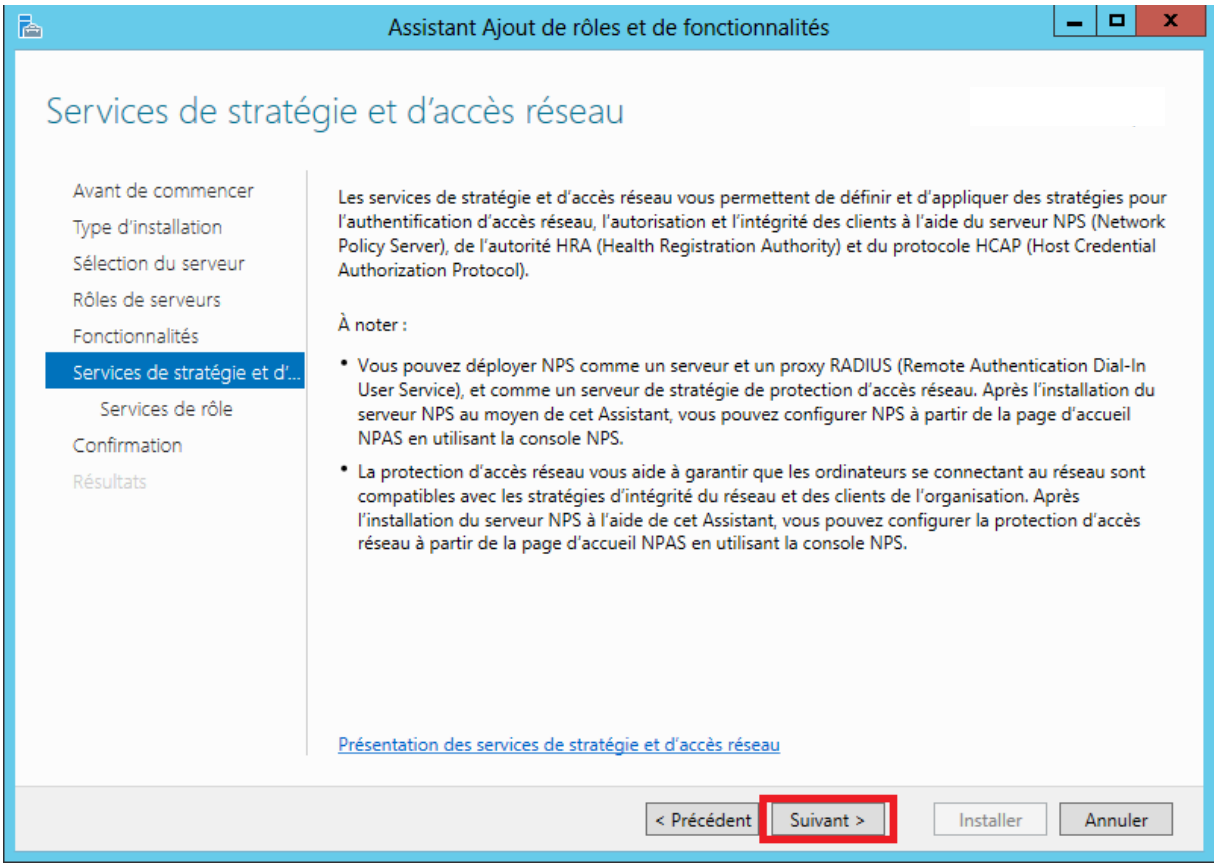

Assistant Ajout de rôles et de fonctionnalités
Sélectionner le type d'installation
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats
Sélectionnez le type d'installation. Vous pouvez installer des rôles et des fonctionnalités sur un ordinateur physique ou virtuel en fonctionnement, ou sur un disque dur virtuel hors connexion.
1)
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
2)
Suivant >
Installer
Annuler


Assistant Ajout de rôles et de fonctionnalités
Sélectionner le 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.
1)
Sélectionner un serveur du pool de serveurs
Sélectionner un disque dur virtuel
Pool de serveurs
Filtre :
Nom
Adresse IP
Système d'exploitation
2)
fr
10.1.151.132
Microsoft Windows Server 2012 Standard
1 ordinateur(s) trouvé(s)
Cette page présente les serveurs qui exécutent Windows Server 2012 et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors ligne et les serveurs nouvellement ajoutés dont la collection de données est toujours incomplète ne sont pas répertoriés.
3)
< Précédent
Suivant >
Installer
Annuler

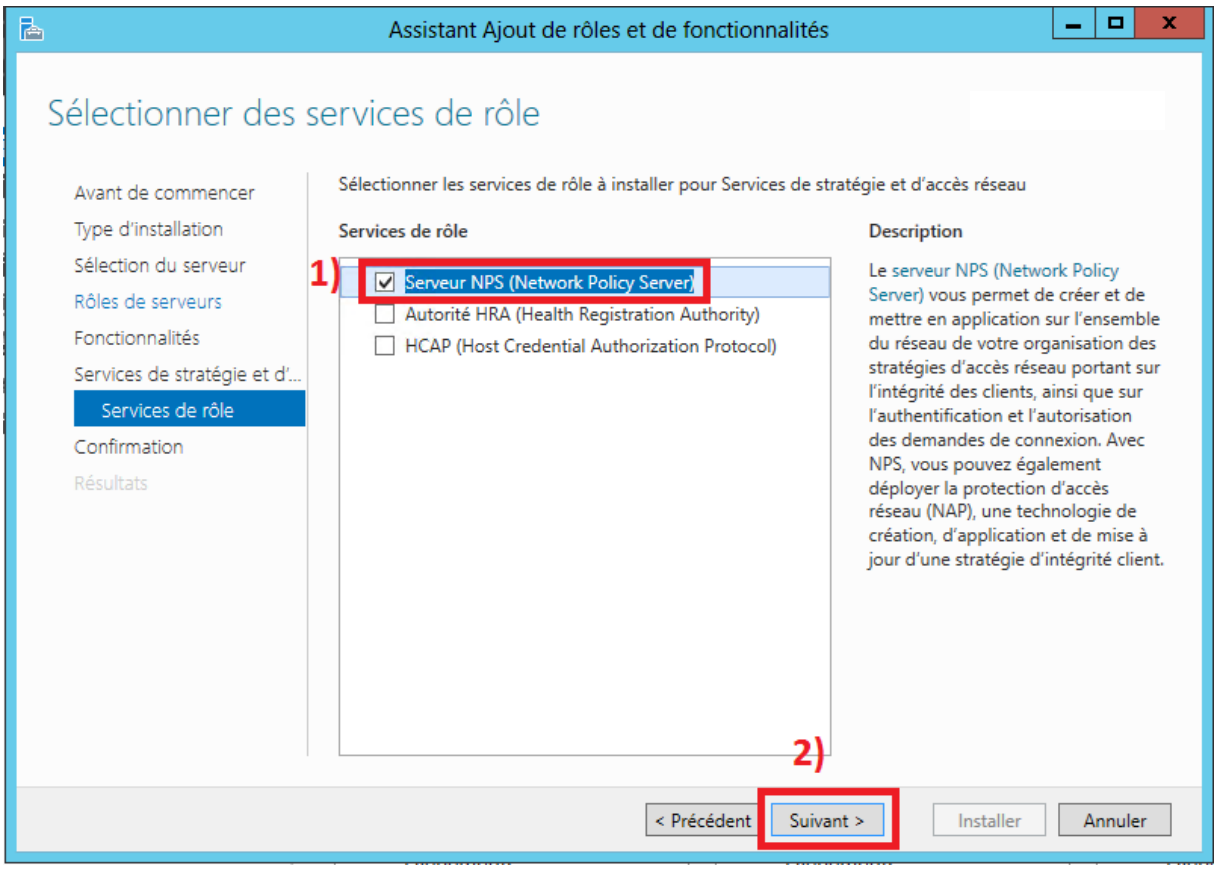
Sélectionner le rôle « Service de stratégie et d'accès réseau ».

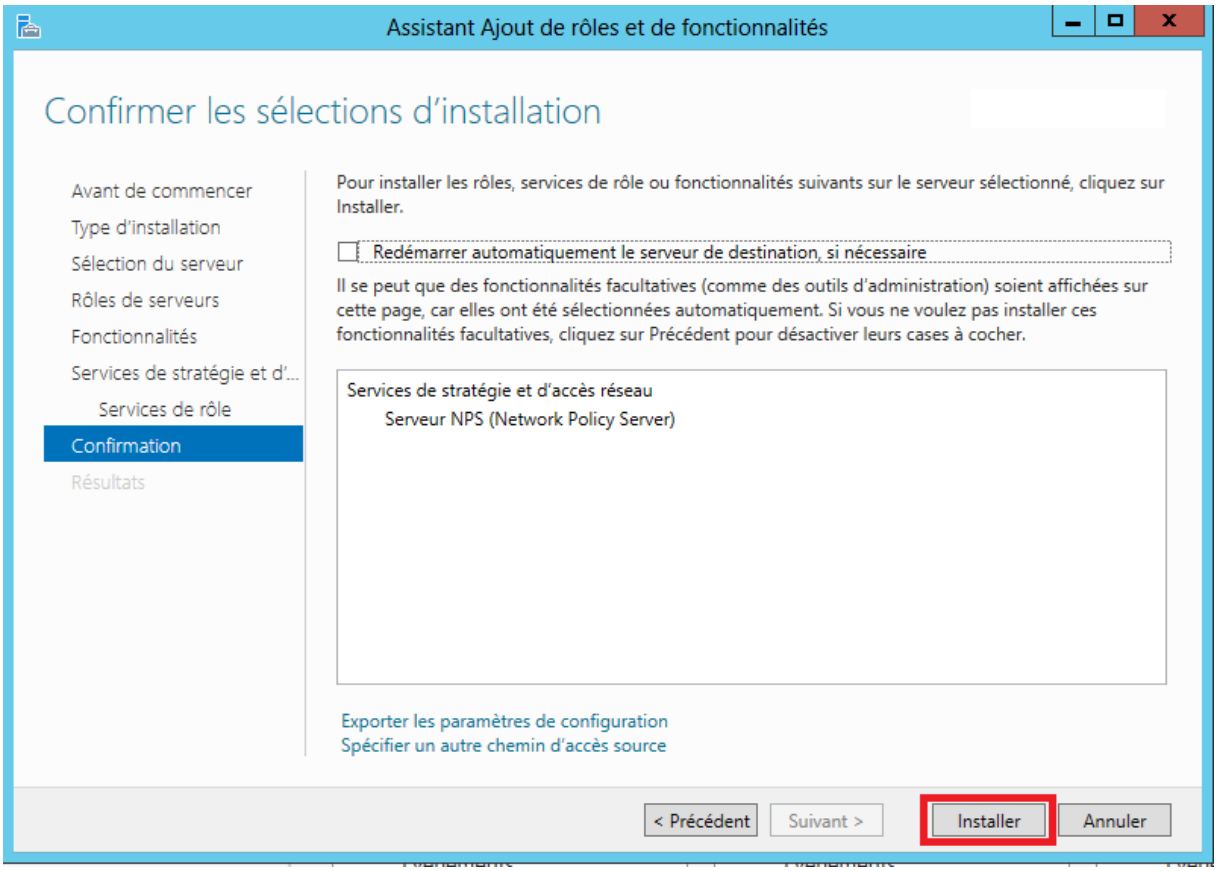


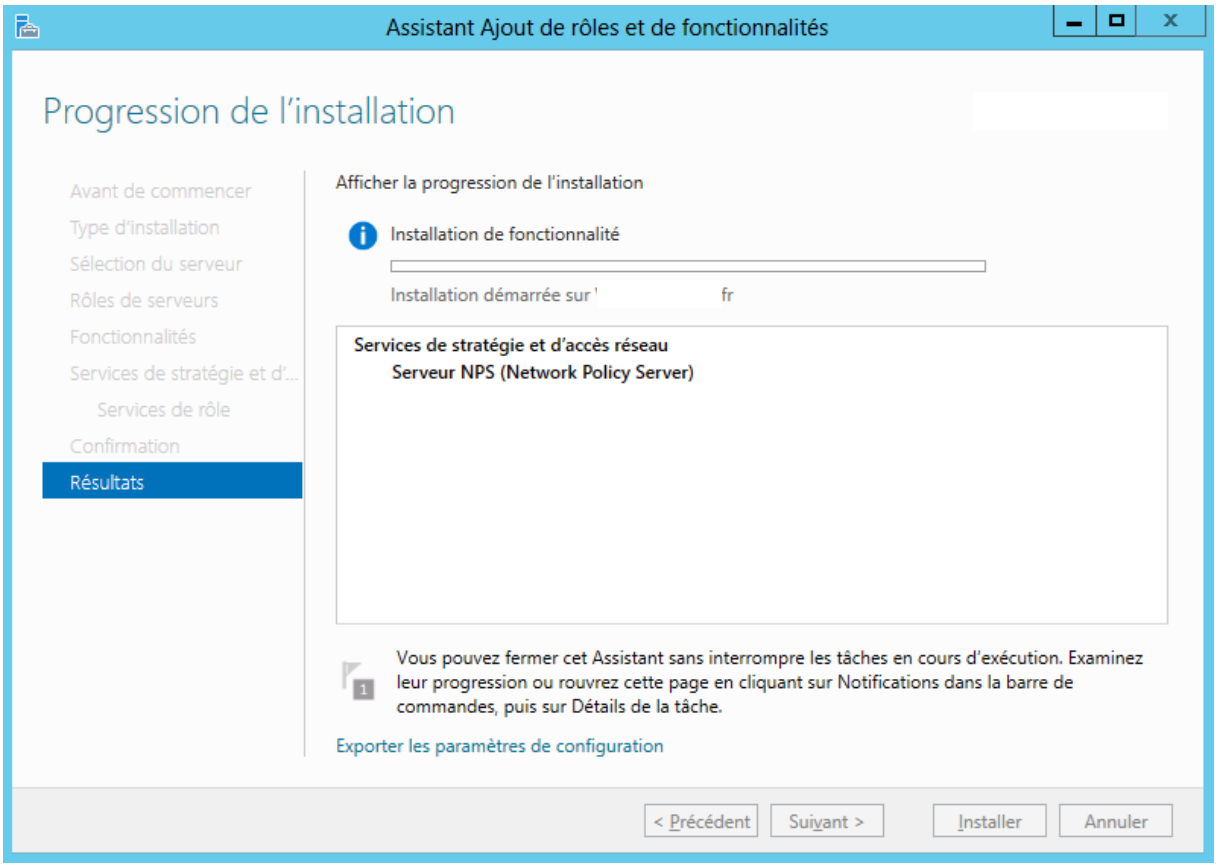




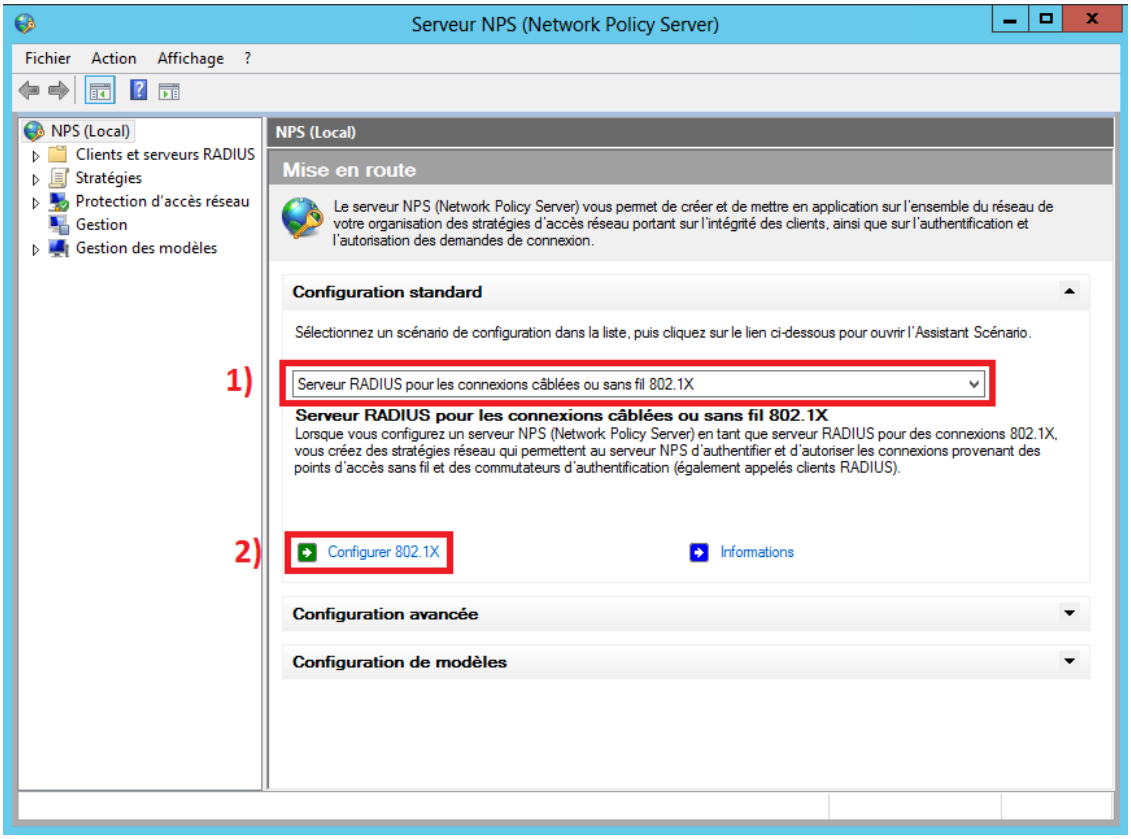
Sélectionner le service de rôle « Serveur NPS (Network Policy Server).

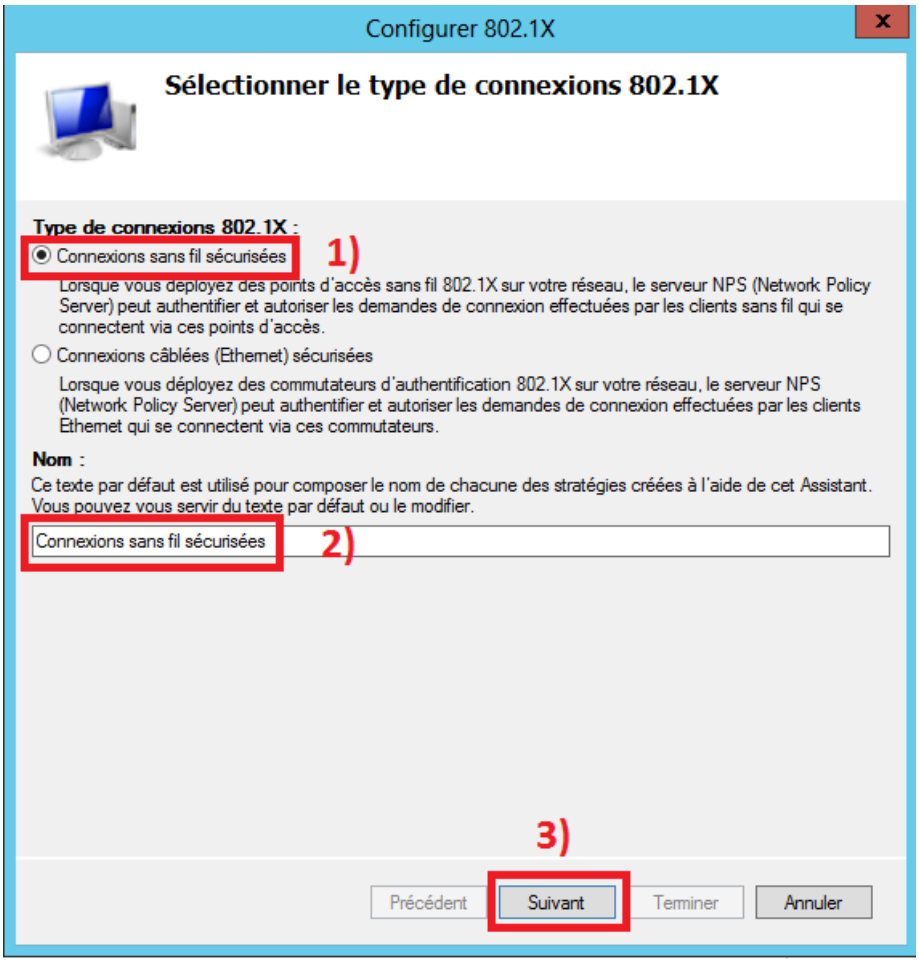



Assistant Ajout de rôles et de fonctionnalités
Confirmer les sélections d'installation
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Services de stratégie et d'...
Services de rôle
Confirmation
Résultats
Pour installer les rôles, services de rôle ou fonctionnalités 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.
Services de stratégie et d'accès réseau
Serveur NPS (Network Policy Server)
Exporter les paramètres de configuration
Spécifier un autre chemin d'accès source
< Précédent
Suivant >
Installer
Annuler

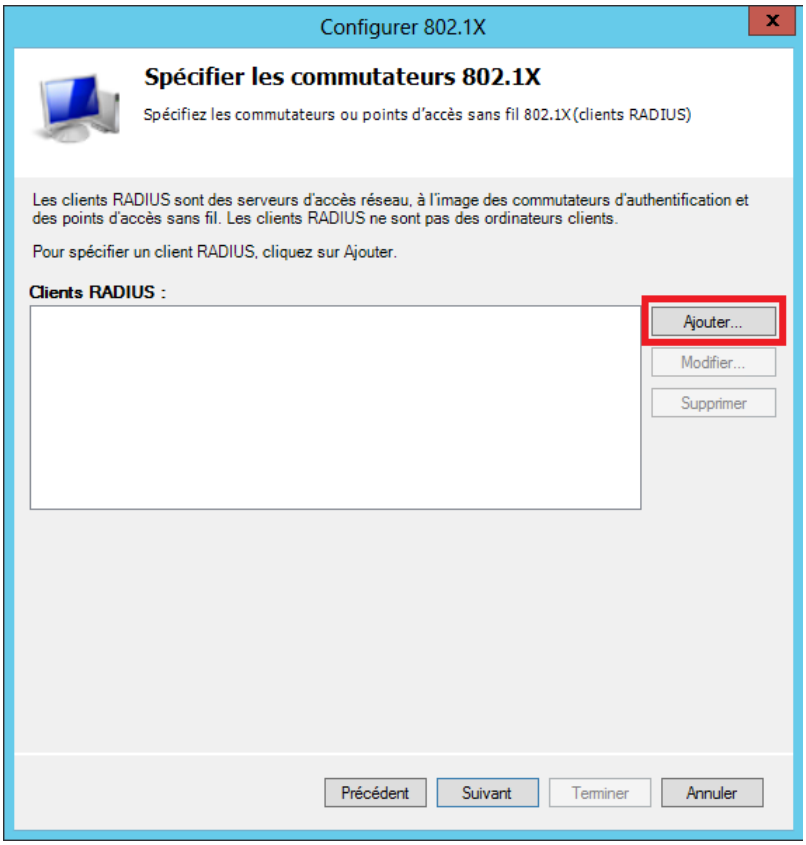

Assistant Ajout de rôles et de fonctionnalités
Progression de l'installation
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Services de stratégie et d'...
Services de rôle
Confirmation
Résultats
Afficher la progression de l'installation
Installation de fonctionnalité
Installation démarrée sur '
fr
Services de stratégie et d'accès réseau
Serveur NPS (Network Policy Server)
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
< Précédent
Suivant >
Installer
Annuler

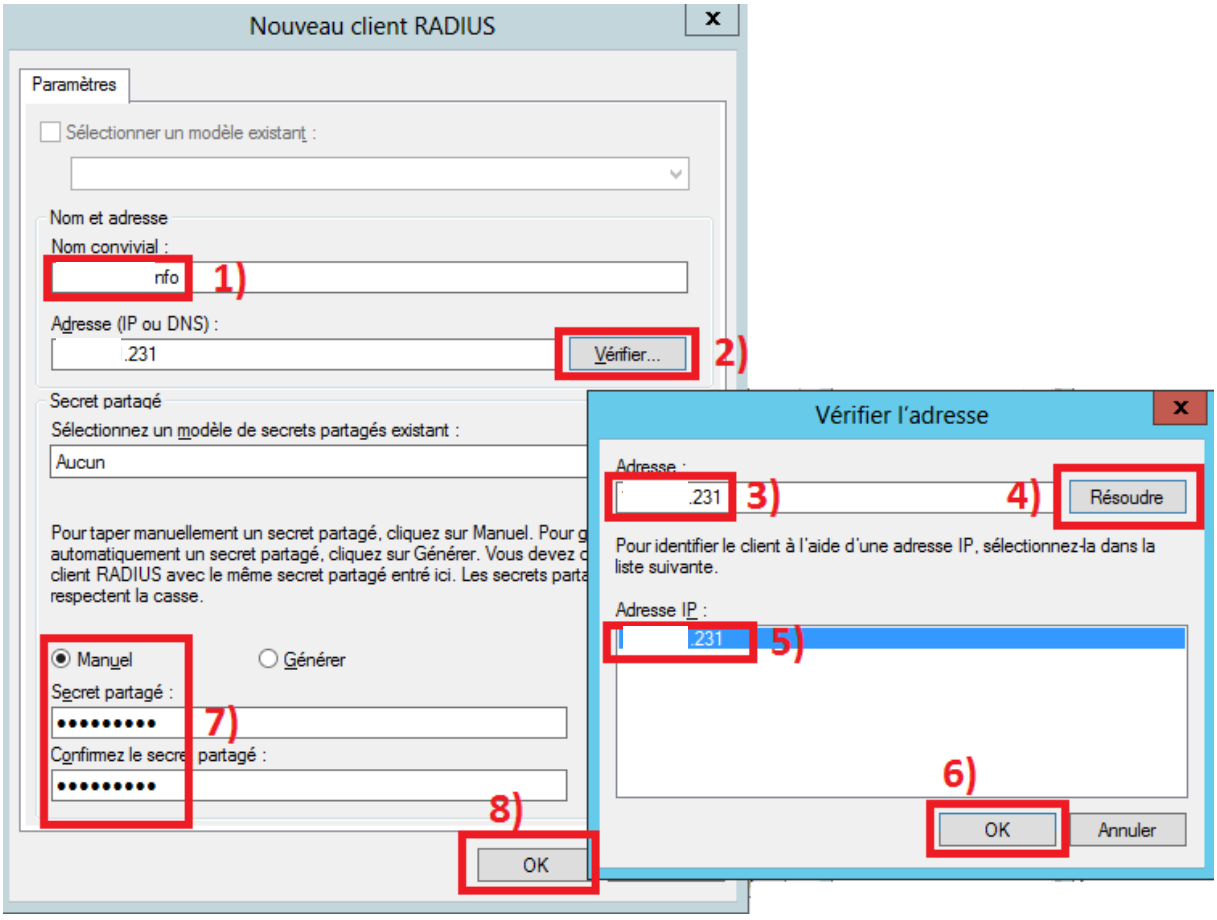
Une fois le rôle serveur NPS installé, il faut configurer le serveur RADIUS.

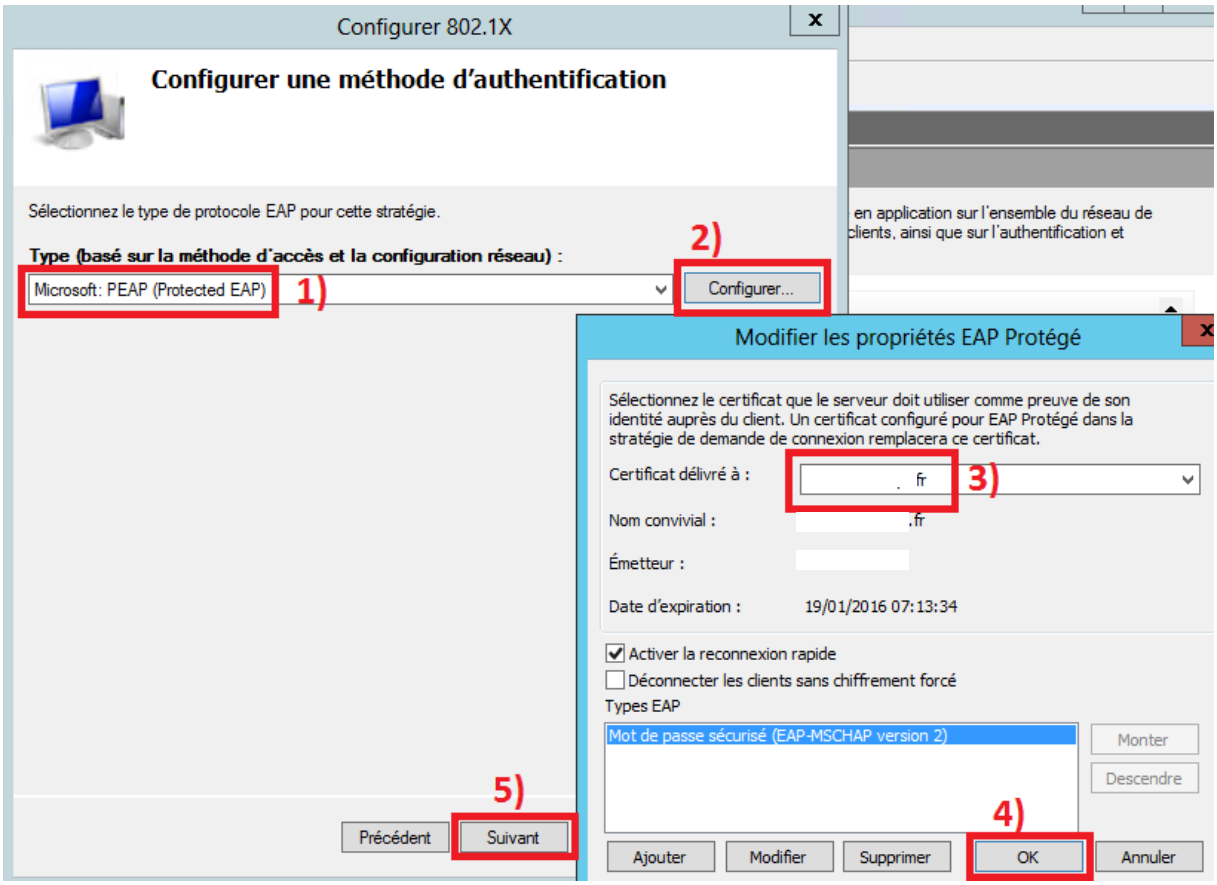



Configurer 802.1X
Sélectionner le type de connexions 802.1X
Type de connexions 802.1X :
Connexions sans fil sécurisées
1)
Lorsque vous déployez des points d'accès sans fil 802.1X sur votre réseau, le serveur NPS (Network Policy Server) peut authentifier et autoriser les demandes de connexion effectuées par les clients sans fil qui se connectent via ces points d'accès.
Connexions câblées (Ethernet) sécurisées
Lorsque vous déployez des commutateurs d'authentification 802.1X sur votre réseau, le serveur NPS (Network Policy Server) peut authentifier et autoriser les demandes de connexion effectuées par les clients Ethernet qui se connectent via ces commutateurs.
Nom :
Ce texte par défaut est utilisé pour composer le nom de chacune des stratégies créées à l'aide de cet Assistant. Vous pouvez vous servir du texte par défaut ou le modifier.
Connexions sans fil sécurisées
2)
3)
Précédent
Suivant
Terminer
Annuler

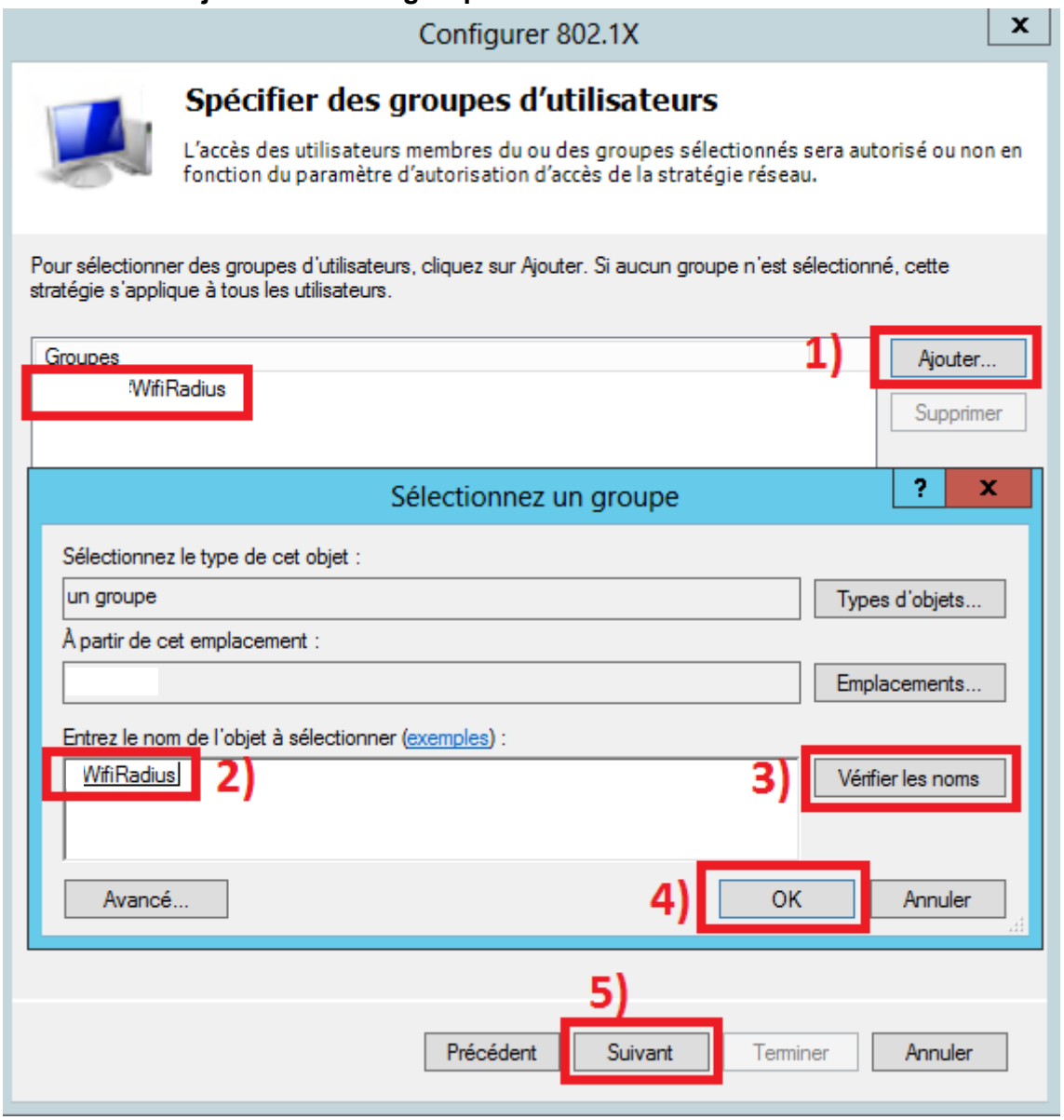
On peut alors ajouter un ou plusieurs clients Radius :

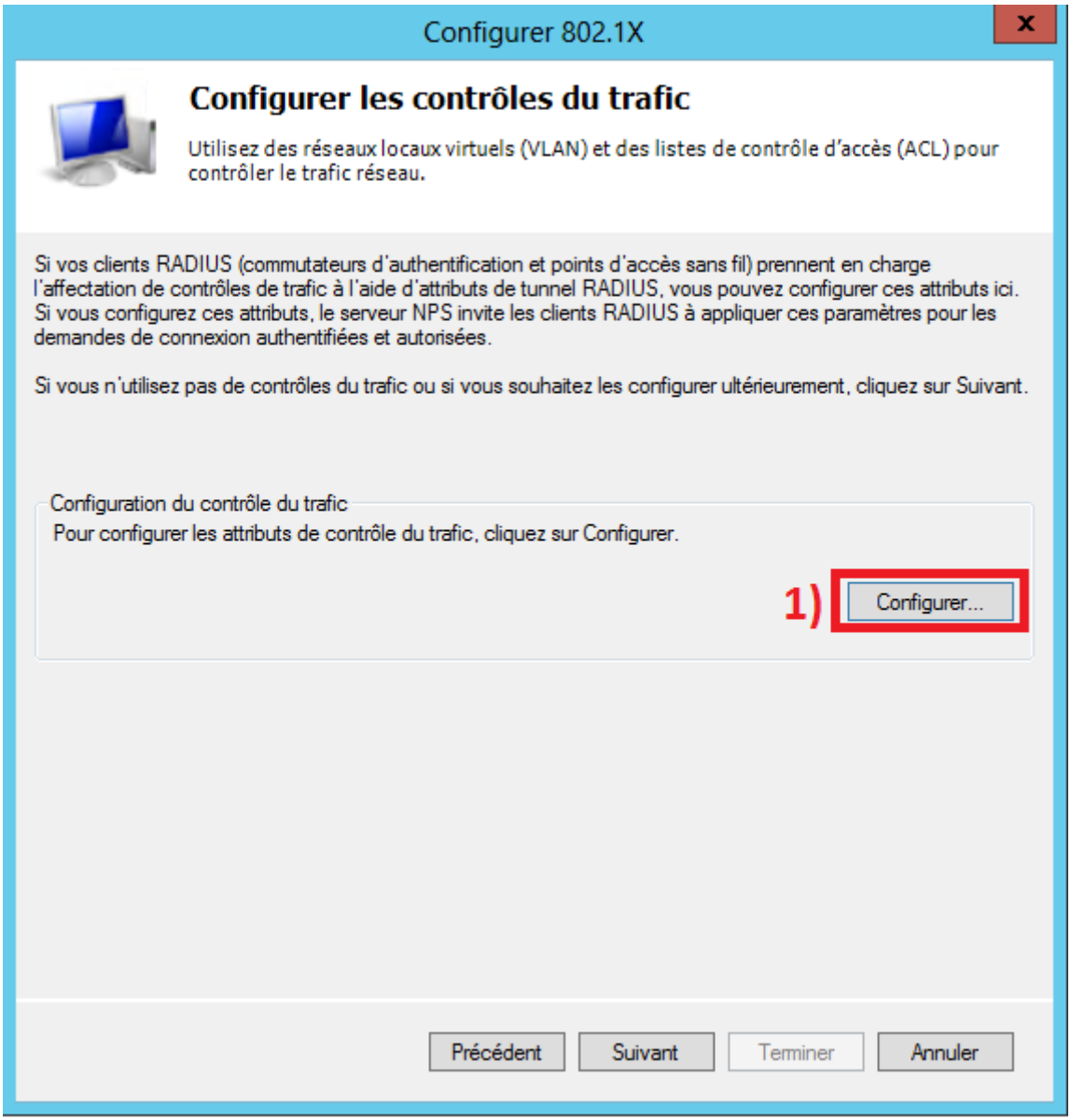


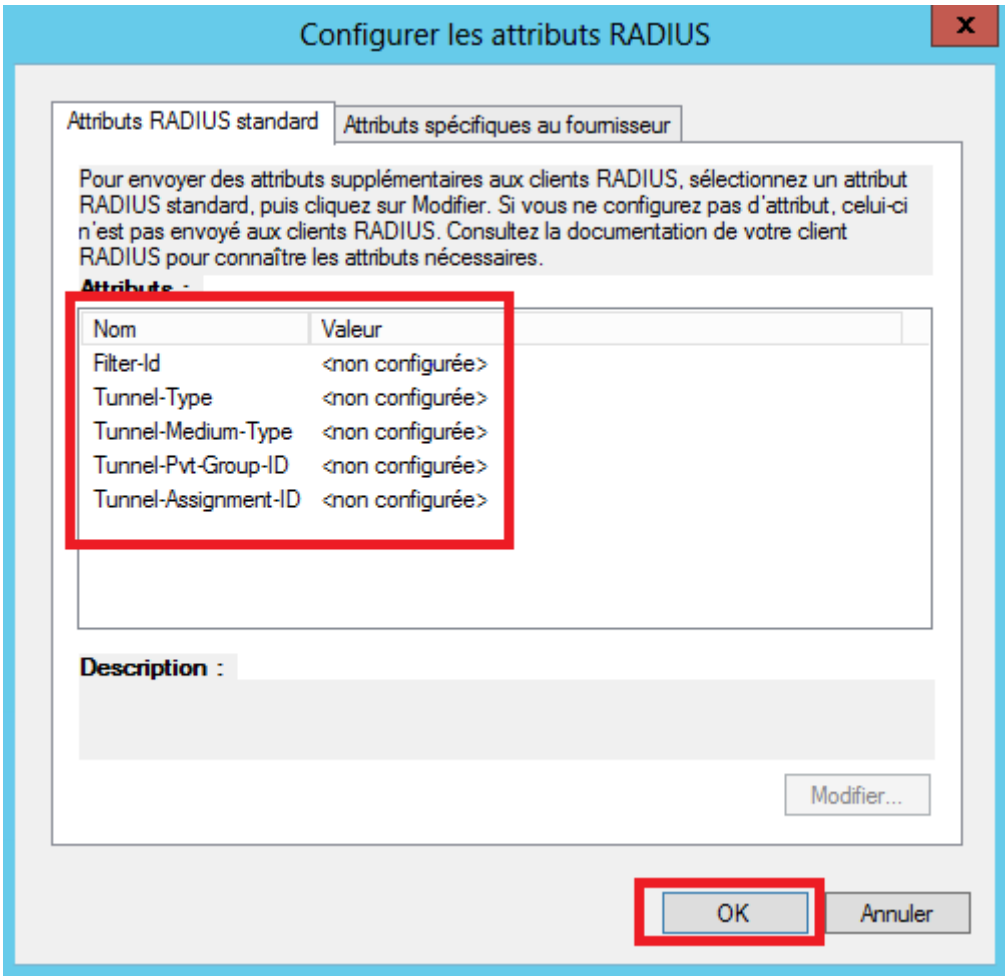


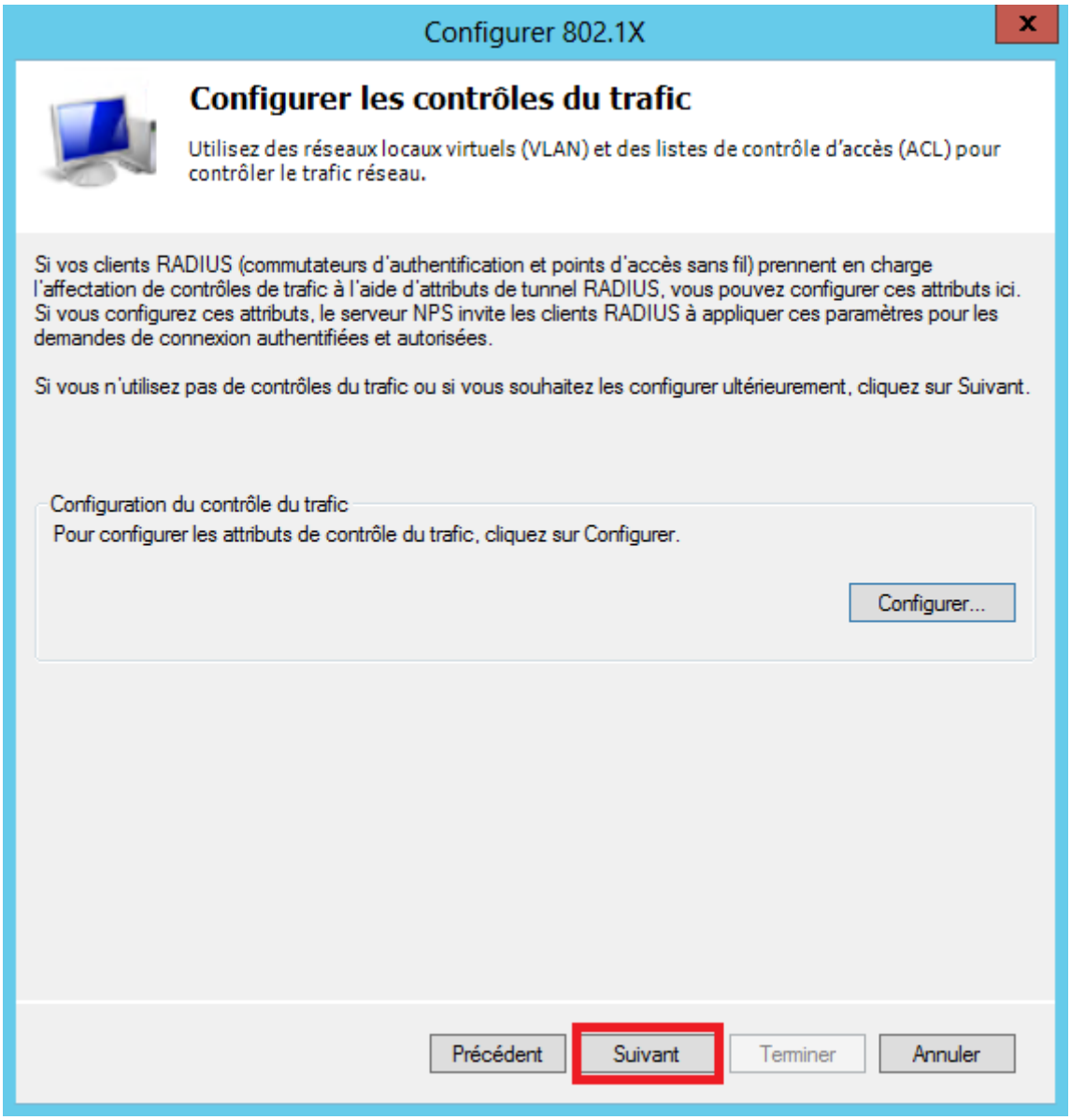

Configurer 802.1X
Configurer une méthode d'authentification
Sélectionnez le type de protocole EAP pour cette stratégie.
Type (basé sur la méthode d'accès et la configuration réseau) :
Microsoft: PEAP (Protected EAP)
1)
2)
Configurer...
en application sur l'ensemble du réseau de
clients, ainsi que sur l'authentification et
Modifier les propriétés EAP Protégé
Sélectionnez le certificat que le serveur doit utiliser comme preuve de son identité auprès du client. Un certificat configuré pour EAP Protégé dans la stratégie de demande de connexion remplacera ce certificat.
Certificat délivré à :
fr
3)
Nom convivial :
.fr
Émetteur :
Date d'expiration :
19/01/2016 07:13:34
Activer la reconnexion rapide
Déconnecter les clients sans chiffrement forcé
Types EAP
Mot de passe sécurisé (EAP-MSCHAP version 2)
Monter
Descendre
4)
5)
Précédent
Suivant
Ajouter
Modifier
Supprimer
OK
Annuler

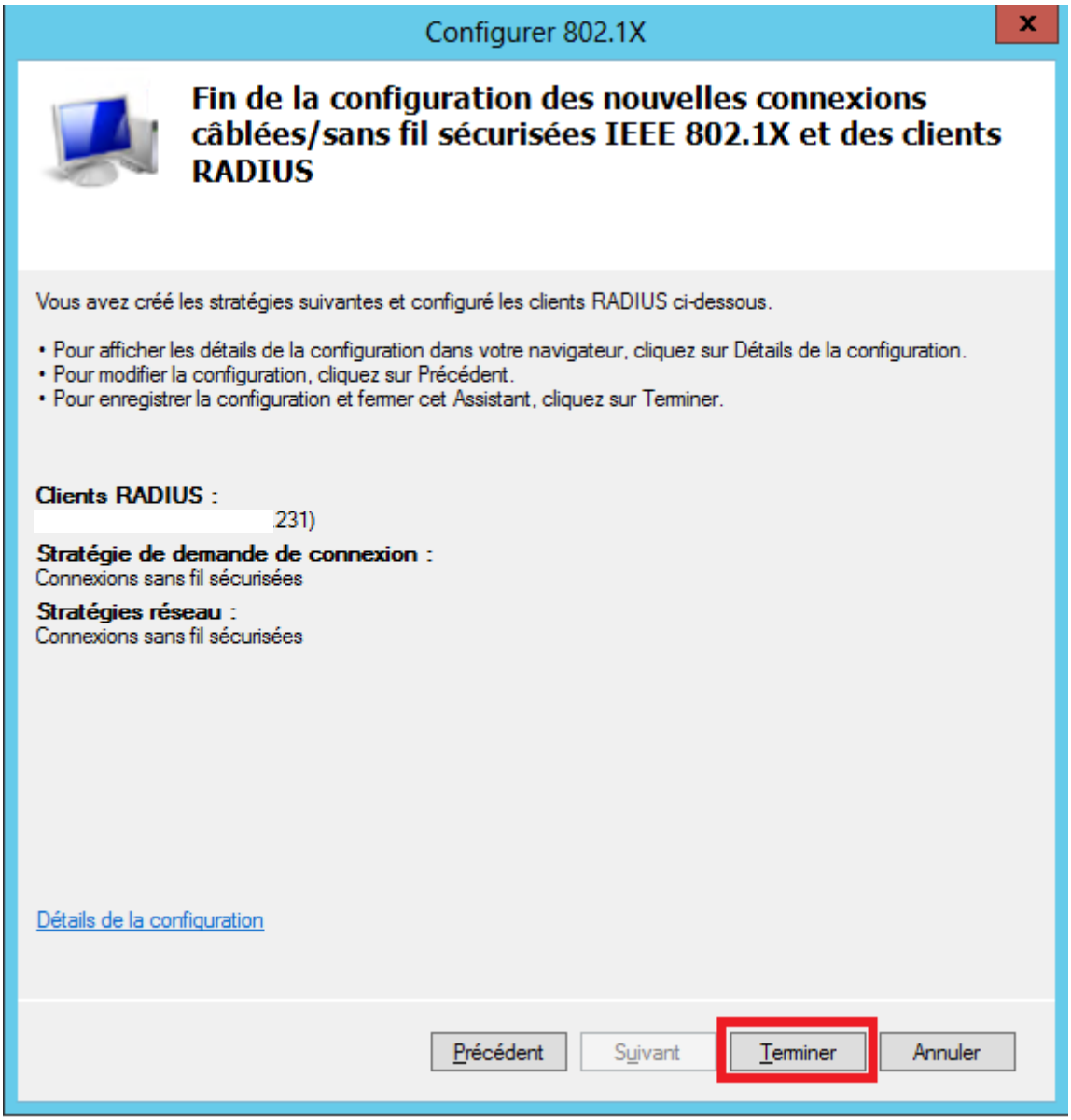
Il faut ensuite ajouter le ou les groupes d'utilisateurs autorisés à s'authentifier :




Configurer 802.1X
Configurer les contrôles du trafic
Utilisez des réseaux locaux virtuels (VLAN) et des listes de contrôle d'accès (ACL) pour contrôler le trafic réseau.
Si vos clients RADIUS (commutateurs d'authentification et points d'accès sans fil) prennent en charge l'affectation de contrôles de trafic à l'aide d'attributs de tunnel RADIUS, vous pouvez configurer ces attributs ici. Si vous configurez ces attributs, le serveur NPS invite les clients RADIUS à appliquer ces paramètres pour les demandes de connexion authentifiées et autorisées.
Si vous n'utilisez pas de contrôles du trafic ou si vous souhaitez les configurer ultérieurement, cliquez sur Suivant.
Configuration du contrôle du trafic
Pour configurer les attributs de contrôle du trafic, cliquez sur Configurer.
1)
Configurer...
Précédent
Suivant
Terminer
Annuler


Configurer les attributs RADIUS
Attributs RADIUS standard
Attributs spécifiques au fournisseur
Pour envoyer des attributs supplémentaires aux clients RADIUS, sélectionnez un attribut RADIUS standard, puis cliquez sur Modifier. Si vous ne configurez pas d'attribut, celui-ci n'est pas envoyé aux clients RADIUS. Consultez la documentation de votre client RADIUS pour connaître les attributs nécessaires.
Attributs :
Nom
Valeur
Filter-Id
<non configurée>
Tunnel-Type
<non configurée>
Tunnel-Medium-Type
<non configurée>
Tunnel-Pvt-Group-ID
<non configurée>
Tunnel-Assignment-ID
<non configurée>
Description :
Modifier...
OK
Annuler


Configurer 802.1X
Configurer les contrôles du trafic
Utilisez des réseaux locaux virtuels (VLAN) et des listes de contrôle d'accès (ACL) pour contrôler le trafic réseau.
Si vos clients RADIUS (commutateurs d'authentification et points d'accès sans fil) prennent en charge l'affectation de contrôles de trafic à l'aide d'attributs de tunnel RADIUS, vous pouvez configurer ces attributs ici. Si vous configurez ces attributs, le serveur NPS invite les clients RADIUS à appliquer ces paramètres pour les demandes de connexion authentifiées et autorisées.
Si vous n'utilisez pas de contrôles du trafic ou si vous souhaitez les configurer ultérieurement, cliquez sur Suivant.
Configuration du contrôle du trafic
Pour configurer les attributs de contrôle du trafic, cliquez sur Configurer.
Configurer...
Précédent
Suivant
Terminer
Annuler


Configurer 802.1X
Fin de la configuration des nouvelles connexions câblées/sans fil sécurisées IEEE 802.1X et des clients RADIUS
Vous avez créé les stratégies suivantes et configuré les clients RADIUS ci-dessous.
• Pour afficher les détails de la configuration dans votre navigateur, cliquez sur Détails de la configuration.
• Pour modifier la configuration, cliquez sur Précédent.
• Pour enregistrer la configuration et fermer cet Assistant, cliquez sur Terminer.
Clients RADIUS :
231)
Stratégie de demande de connexion :
Connexions sans fil sécurisées
Stratégies réseau :
Connexions sans fil sécurisées
Détails de la configuration
Précédent
Suivant
Terminer
Annuler

Les clients RADIUS Peuvent aussi être ajoutés en utilisant Powershell. Pour cela, il faut créer un fichier CSV dans lequel on indique :

- Le nom convivial du point d'accès : il permet d'identifier le point d'accès dans la liste des clients
- Son adresse IP
- La clé secrète liée au point d'accès (si celle-ci est la même partout, inutile de la préciser dans ce fichier, elle peut être renseignée directement dans le script, voir exemple ci-dessous)

```
# New-NpsRadiusClient -Address "ADRESSE_IP_DU_POINT_D_ACCES" -Name "NOM_CONVIVIAL"
#                     -NapCompatible $True -SharedSecret "CLE_SECRETE"
# On renseigne le chemin d'accès au fichier CSV
$filepath = "c:\liste_pa.csv"

# On utilise la fonction d'import de CSV
Import-CSV $filepath -delimiter ";" -Header NAME,IP | Foreach-Object{
    # Pour chaque ligne du fichier, on ajoute un nouveau client RADIUR
    New-NpsRadiusClient -Address $_.IP -Name $_.NAME -SharedSecret Clés3crèt3
}
```