

PROCEDURE D'INSTALLATION: WINDOWS – SERVEUR RADIUS



Introduction

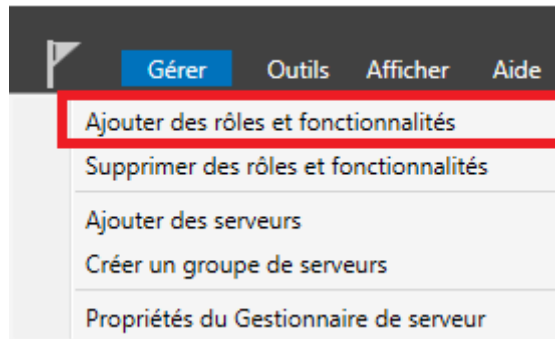
- **Objectif** : L'objectif principal d'un **serveur RADIUS** (*Remote Authentication Dial-In User Service*) est de centraliser l'**authentification**, l'**autorisation** et la **comptabilité** (AAA : *Authentication, Authorization, Accounting*) des accès réseau.

Prérequis

- **Système d'exploitation**
 - **Debian 12 avec les services LAMP**
- **Ressources matérielles (minimum recommandé)**
 - **CPU: 1 vCPU**
 - **RAM: 1 Go**
 - **Disque: 8 Go**

Installation Server Radius

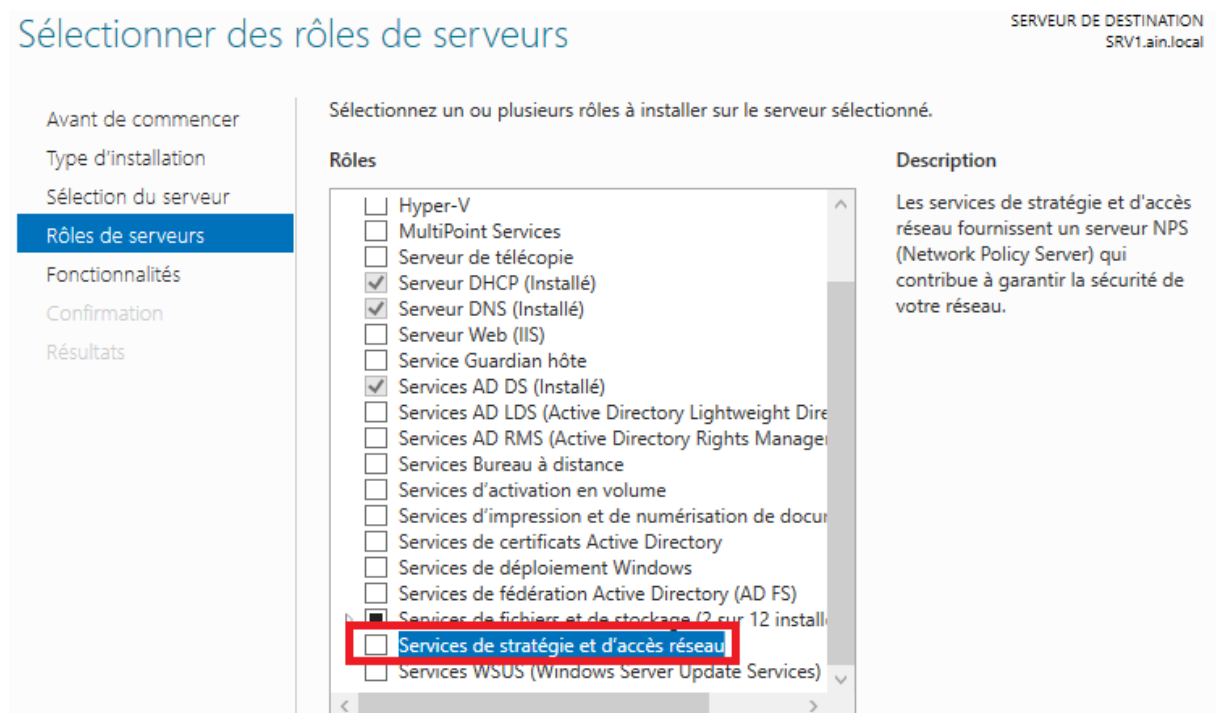
Pour commencer, allez dans le gestionnaire de serveur, cliquez sur « Gérer » puis « Ajouter des rôles et fonctionnalités ».




Sur la première fenêtre, laissez cocher « Installation basée sur un rôle ou une fonctionnalité ».



Sur la fenêtre suivante, « Sélection du serveur » laissez par défaut et cliquez à nouveau sur « Suivant ». Vous arriverez sur la fenêtre de sélection des rôles, cochez « Services de stratégie et d'accès réseau ».



Cliquez sur « Ajouter des fonctionnalités » et cliquez sur « Suivant ».

 Assistant Ajout de rôles et de fonctionnalités ✕

Ajouter les fonctionnalités requises pour Services de stratégie et d'accès réseau ?

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] Outils de la stratégie réseau et des services d'accès

☒ Inclure les outils de gestion (si applicable)

Ajouter des fonctionnalités Annuler

Cliquez sur « Suivant » jusqu'à arriver sur la fenêtre de confirmation d'installation du rôle et cliquez sur « Installer ».

Confirmer les sélections d'installation SERVEUR DE DESTINATION
SRV1.ain.local

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

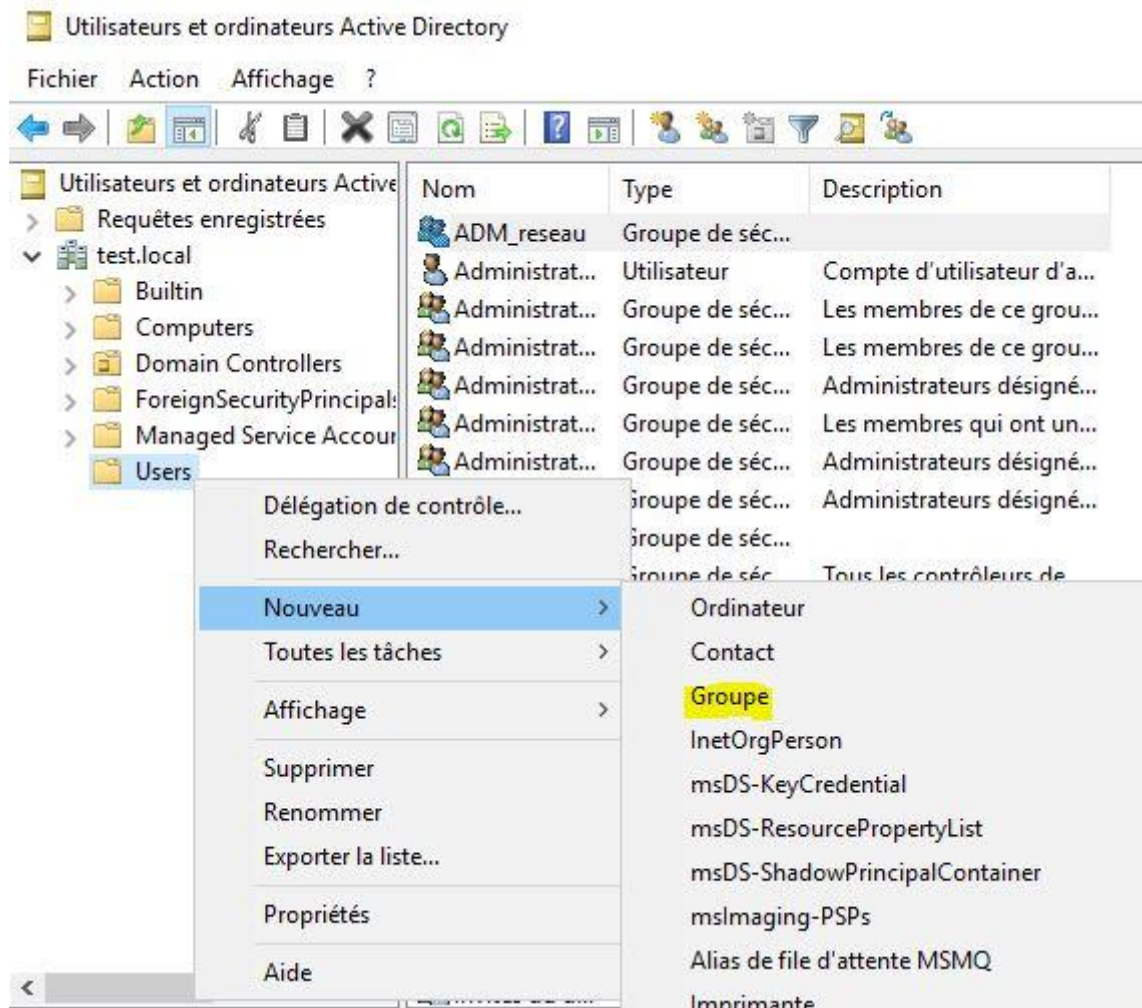
Services de stratégie et d'accès réseau

[Exporter les paramètres de configuration](#)
[Spécifier un autre chemin d'accès source](#)

< Précédent Suivant > Installer Annuler

Configuration Groupe Active Directory

Vous devez créer un groupe ainsi qu'un utilisateur qui fera parti de celui-ci. Nous allons autoriser par la suite tous les utilisateurs présents dans ce groupe à se connecter sur les switchs Cisco. Pour créer le groupe, allez sur votre console d'administration AD DS, dans le menu à gauche faites un clic droit sur Users, sélectionnez « Nouveau » puis « Groupe » :



Nommez votre groupe puis cliquez sur « OK » pour le créer :

Nouvel objet - Groupe

Créer dans : test.local/Users

Nom du groupe :
ADM_reseau

Nom de groupe (antérieur à Windows 2000) :
ADM_reseau

Étendue du groupe

☐ Domaine local

☒ Globale

☐ Universelle

Type de groupe

☒ Sécurité

☐ Distribution

OK Annuler

Le groupe étant à présent créé, nous allons devoir créer les utilisateurs qui feront partie de ce groupe. Faites à nouveau un clic droit sur « Users », sélectionnez « Nouveau » puis « Utilisateur » :

Utilisateurs et ordinateurs Active Directory

Fichier Action Affichage ?

Utilisateurs et ordinateurs Active Directory

- Requêtes enregistrées
- test.local
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipal...
 - Managed Service Account...
 - Users

Nom	Type	Description
ADM_reseau	Groupe de séc...	
Administrat...	Utilisateur	Compte d'utilisateur d'a...
Administrat...	Groupe de séc...	Les membres de ce grou...
Administrat...	Groupe de séc...	Les membres de ce grou...
Administrat...	Groupe de séc...	Administrateurs désigné...
Administrat...	Groupe de séc...	Les membres qui ont un...
Administrat...	Groupe de séc...	Administrateurs désigné...
Administrat...	Groupe de séc...	Administrateurs désigné...
Administrat...	Groupe de séc...	Administrateurs désigné...

Délégation de contrôle...
Rechercher...

Nouveau >
Toutes les tâches >
Affichage >
Actualiser
Exporter la liste...
Propriétés
Aide

Ordinateur
Contact
Groupe
InetOrgPerson
msDS-KeyCredential
msDS-ResourcePropertyList
msDS-ShadowPrincipalContainer
mslmaging-PSPs
Alias de file d'attente MSMQ
Imprimante
Utilisateur

Invité
Invités du d...

Crée un nouvel élément dans ce conteneur.

Remplissez les champs avec les informations de l'administrateur :

Nouvel objet - Utilisateur

Créer dans : test.local/Users

Prénom : Pierre Initiales :

Nom : M

Nom complet : Pierre M

Nom d'ouverture de session de l'utilisateur : pierre.m| @test.local

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) : TEST\ pierre.m

< Précédent Suivant > Annuler

Le groupe et l'utilisateur étant créé, nous allons intégrer l'utilisateur à ce groupe. Faites un clic droit sur le groupe créé puis sélectionnez « Propriétés » :

Utilisateurs et ordinateurs Active Directory

Fichier Action Affichage ?

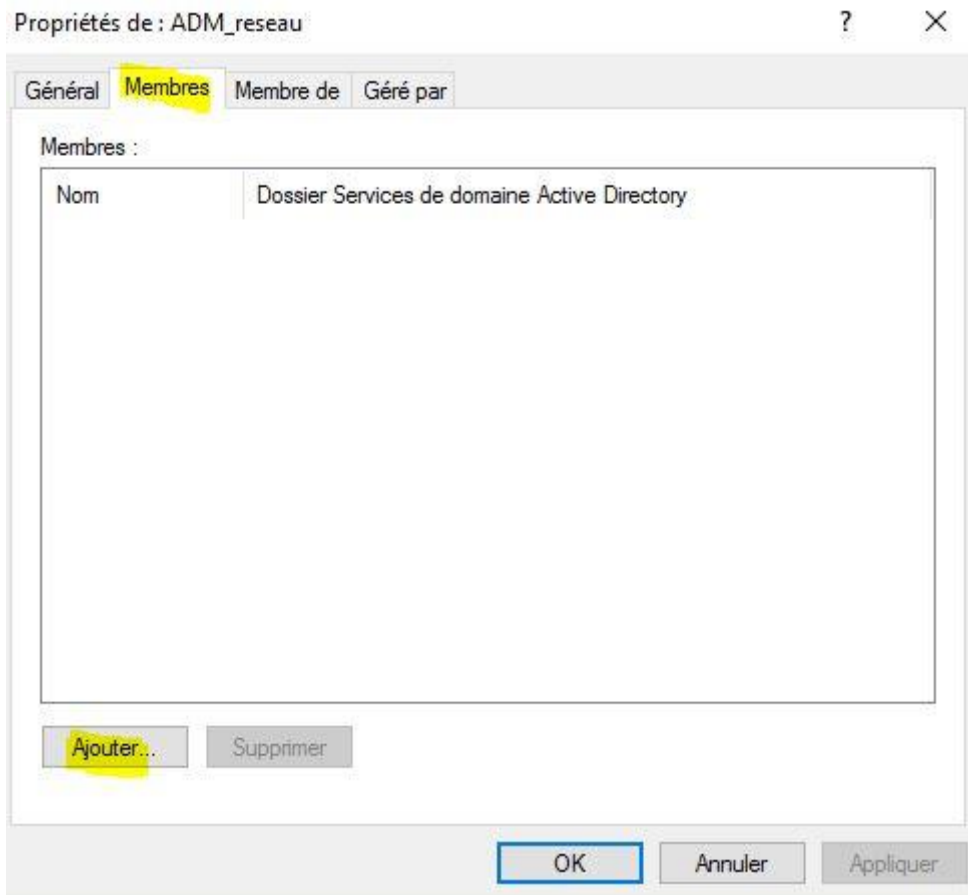
Utilisateurs et ordinateurs Active Directory

- Requêtes enregistrées
- test.local
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - Managed Service Accounts
 - Users

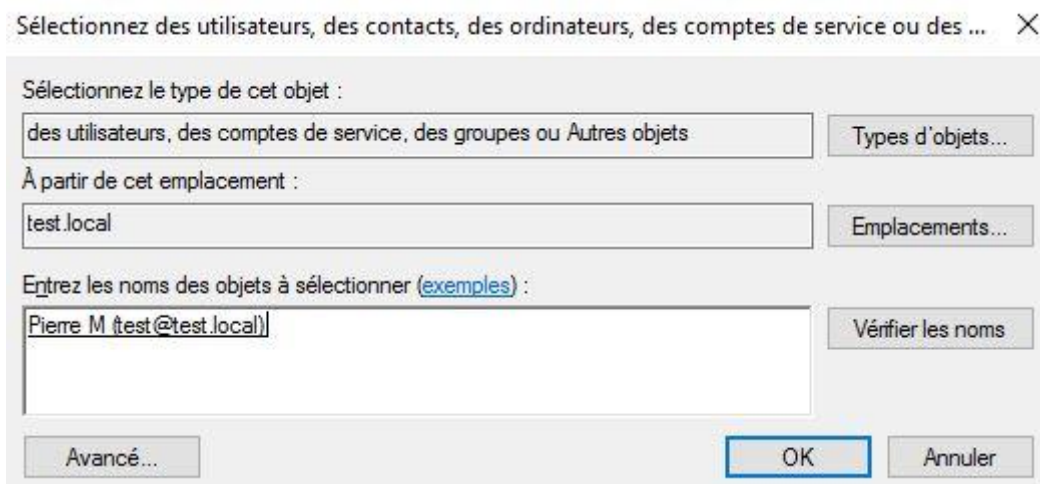
Nom	Type	Description
ADM_reseau	Groupe de sécurité	
Administrateur	Utilisateur	
Administrateur	Groupe de sécurité	
Administrateur	Groupe de sécurité	
Administrateur	Groupe de sécurité	
Administrateur	Groupe de sécurité	
Administrateur	Groupe de sécurité	
Administrateur	Groupe de sécurité	
Admins du réseau	Groupe de sécurité	
Comptabilité	Groupe de sécurité	
Contrôleurs de domaine	Groupe de sécurité	
Contrôleurs de domaine	Groupe de sécurité	
Contrôleurs de domaine	Groupe de sécurité	
Contrôleurs de domaine	Groupe de sécurité	

Ajouter à un groupe...
Déplacer...
Envoyer un message
Toutes les tâches
Couper
Supprimer
Renommer
Propriétés
Aide

Sous l'onglet membre, cliquez sur « Ajouter... » :



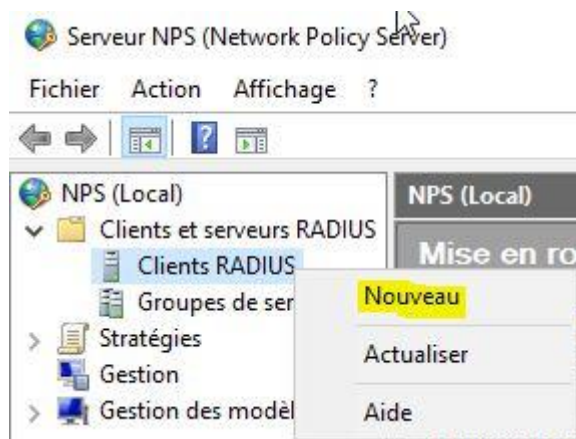
Renseignez le début du nom de l'utilisateur et cliquez sur « Vérifier les noms » :



Validez, votre utilisateur est à présent intégré au groupe.

Configuration Groupe Active Directory

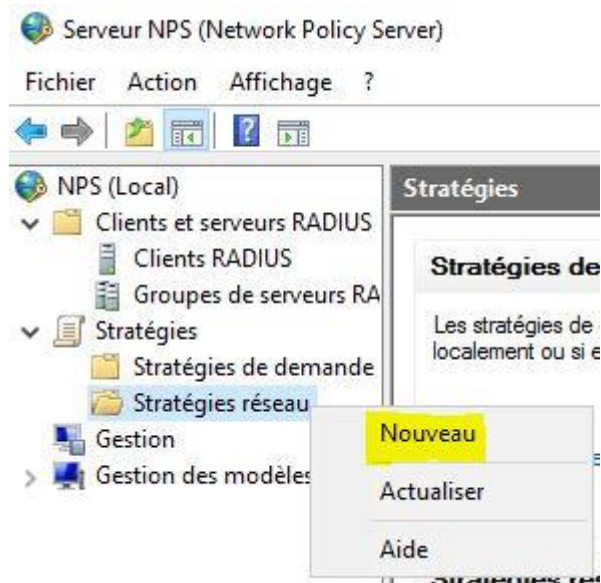
Pour cette étape, vous aurez besoin de l'adresse IP du switch. Allez sur la console NPS sous « Clients et serveurs RADIUS » faites un clic droit sur « Clients RADIUS » puis sélectionnez « Nouveau »



Renseignez l'adresse IP de l'équipement et le secret, gardez le de coté nous allons nous en servir plus tard :


A screenshot of the 'Nouveau client RADIUS' dialog box. The 'Paramètres' tab is selected. The 'Activer ce client RADIUS' checkbox is checked. Below it is a dropdown for 'Sélectionner un modèle existant :'. The 'Nom et adresse' section has 'Nom convivial : S_compta' and 'Adresse (IP ou DNS) : 192.168.1.88' with a 'Vérifier...' button. The 'Secret partagé' section has a dropdown for 'Sélectionnez un modèle de secrets partagés existant :' set to 'Aucun'. Below this is explanatory text: 'Pour taper manuellement un secret partagé, cliquez sur Manuel. Pour générer automatiquement un secret partagé, cliquez sur Générer. Vous devez configurer le client RADIUS avec le même secret partagé entré ici. Les secrets partagés respectent la casse.' There are two radio buttons: 'Manuel' (selected) and 'Générer'. Below them are two text boxes for 'Secret partagé :' and 'Confirmez le secret partagé :', both containing masked characters. At the bottom are 'OK' and 'Annuler' buttons.

Nous allons devoir définir la politique d'accès. Faites un clic droit sur « Stratégies réseau » et sélectionnez « Nouveau » :



Nommez la stratégie et cliquez sur « Suivant » :

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 :

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 :

☐ Spécifique au fournisseur :

Précédent

Suivant

Terminer

Annuler

Sur la fenêtre suivante, nous allons spécifier les conditions d'accès. Nous allons indiquer que seul les utilisateurs faisant partie du groupe créé auparavant pourront s'authentifier. Cliquez sur « Ajouter... » :

Nouvelle stratégie réseau

Spécifier les conditions

Spécifiez les conditions qui déterminent si cette stratégie réseau est évaluée pour une demande de connexion. Au minimum, une condition est nécessaire.

Condition	Valeur
-----------	--------

Description de la condition :

Ajouter... Modifier... Supprimer

Précédent Suivant Terminer Annuler

Sélectionnez « Groupes Windows » :

Nouvelle stratégie réseau

Spécifier les conditions

Spécifiez les conditions qui déterminent si cette stratégie réseau est évaluée pour une demande de connexion. Au minimum, une condition est nécessaire.

Sélectionner une condition

Sélectionnez une condition, puis cliquez sur Ajouter.

Groupes

- Groupes Windows**
La condition Groupes Windows spécifie que l'utilisateur ou l'ordinateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.
- Groupes d'ordinateurs**
La condition Groupes d'ordinateurs spécifie que l'ordinateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.
- Groupes d'utilisateurs**
La condition Groupes d'utilisateurs spécifie que l'utilisateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.

Restrictions relatives aux jours et aux heures

Restrictions relatives aux jours et aux heures
Les restrictions relatives aux jours et aux heures indiquent les jours et les heures auxquels les tentatives de connexion sont autorisées ou non. Ces restrictions sont basées sur le fuseau horaire du serveur NPS (Network Policy Server).

Ajouter... Annuler

Cliquez sur « Ajouter des groupes... » :

Groupes Windows

Spécifiez l'appartenance aux groupes nécessaire pour correspondre à cette stratégie.

Groupes

Ajouter des groupes... Supprimer

OK Annuler

Indiquez le groupe créé au début de l'article :

Sélectionnez un groupe

Sélectionnez le type de cet objet :

un groupe Types d'objets...

À partir de cet emplacement :

test.local Emplacements...

Entrez le nom de l'objet à sélectionner (exemples) :

ADM_reseau Vérifier les noms

Avancé... OK Annuler

Votre groupe étant ajouté, cliquez sur « Suivant » :

Nouvelle stratégie réseau

Spécifier les conditions

Spécifiez les conditions qui déterminent si cette stratégie réseau est évaluée pour une demande de connexion. Au minimum, une condition est nécessaire.

Conditions :

Condition	Valeur
Groupes Windows	TEST\ADM_reseau


Description de la condition :
La condition Groupes Windows spécifie que l'utilisateur ou l'ordinateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.

Ajouter... Modifier... Supprimer

Précédent Suivant Terminer Annuler

Laissez coché « Accès accordé » et cliquez sur « Suivant » :

Nouvelle stratégie réseau ×

 **Spécifier l'autorisation d'accès**

Effectuez la configuration nécessaire pour accorder ou refuser l'accès réseau si la demande de connexion correspond à cette stratégie.

☒ **Accès accordé**
Accordez l'accès si les tentatives de connexion des clients répondent aux conditions de cette stratégie.


☐ **Accès refusé**
Refusez l'accès si les tentatives de connexion des clients répondent aux conditions de cette stratégie.

☐ **L'accès est déterminé par les propriétés de numérotation des utilisateurs (qui remplacent la stratégie NPS)**
Choisissez selon les propriétés de numérotation utilisateur si les tentatives de connexion des clients répondent aux conditions de la stratégie.

Précédent Suivant Terminer Annuler

Cochez uniquement la case « Authentification non chiffrée (PAP, SPAP) », une pop-up apparaîtra, cliquez sur « Non » :

Nouvelle stratégie réseau ×

 **Configurer les méthodes d'authentification**

Configurez une ou plusieurs des méthodes d'authentification nécessaires pour que la demande de connexion corresponde à cette stratégie. Pour l'authentification EAP, vous devez configurer un type EAP.

Les types de protocoles EAP sont négociés entre le serveur NPS et le client dans l'ordre dans lequel ils sont listés.

Types de protocoles EAP :

Monter

Descendre

Ajouter... Modifier... Supprimer

Méthodes d'authentification moins sécurisées :

☐ Authentification chiffrée Microsoft version 2 (MS-CHAP v2)
☐ L'utilisateur peut modifier le mot de passe après son expiration

☐ Authentification chiffrée Microsoft (MS-CHAP)
☐ L'utilisateur peut modifier le mot de passe après son expiration

☐ Authentification chiffrée (CHAP)

☒ **Authentification non chiffrée (PAP, SPAP)**

☐ Autoriser les clients à se connecter sans négocier une méthode d'authentification.

Précédent Suivant Terminer Annuler

Pour les contraintes, elles vous serviront par exemple à forcer la déconnexion des utilisateurs au bout d'un certain délai. Je n'en positionne pas, cliquez sur « Suivant » :

Nouvelle stratégie réseau



Configurer des contraintes

Les contraintes sont des paramètres supplémentaires de la stratégie réseau, auxquels les demandes de connexion doivent se conformer. Si une demande de connexion ne répond pas à une contrainte, le serveur NPS (Network Policy Server) rejette automatiquement cette demande. Les contraintes sont facultatives ; si vous ne souhaitez pas configurer de contraintes, cliquez sur Suivant.

Configurez les contraintes de cette stratégie réseau.

Si la demande de connexion ne répond pas à toutes les contraintes, l'accès réseau est refusé.

Contraintes :

Contraintes

Délai d'inactivité

Délai d'expiration de session

ID de la station appelée

Restrictions relatives aux jours et aux heures

Type de port NAS

Spécifiez le délai maximal d'inactivité du serveur en minutes avant déconnexion

☐ Déconnecter au-delà de la durée d'inactivité maximale

1

Précédent

Suivant

Terminer

Annuler

Dans cette fenêtre, nous allons avoir plusieurs paramètres à positionner. Dans la partie « Standard », supprimez les deux éléments déjà présents puis cliquez sur « Ajouter... » :

Nouvelle stratégie réseau



Configurer les paramètres

Le serveur NPS applique des paramètres à la demande de connexion si toutes les conditions relatives à la stratégie de demande de connexion sont remplies.

Configurez les paramètres de cette stratégie réseau.

Si la demande de connexion répond aux conditions et contraintes, et si la stratégie accorde l'accès, les paramètres sont appliqués.

Paramètres :

Attributs RADIUS

Standard

☒ Spécifiques au fournisseur

Routage et accès à distance

Liaisons multiples et protocole BAP (Bandwidth Allocation Protocol)

Filtres IP

Chiffrement

Paramètres IP

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
Framed-Protocol	PPP
Service-Type	Framed

Ajouter...

Modifier...

Supprimer

Précédent

Suivant

Terminer

Annuler

Dans la liste, sélectionnez « Service-Type » puis cliquez sur « Ajouter... » :

Ajouter un attribut RADIUS standard ✕

Pour ajouter un attribut aux paramètres, sélectionnez-le et cliquez sur Ajouter.

Pour ajouter un attribut personnalisé ou prédéfini spécifique au fournisseur, fermez cette boîte de dialogue et sélectionnez Spécifique au fournisseur, puis cliquez sur Ajouter.

Type d'accès :
Tous ▼

Attributs :

- Nom
- NAS-Port-Id
- Reply-Message
- Service-Type**
- Termination-Action
- Tunnel-Assignment-ID
- Tunnel-Client-Auth-ID

Description :
Spécifie le type de service requis par l'utilisateur.

Ajouter... Fermer

Cochez la case « Autres », sélectionnez « Login » puis validez :

Informations d'attribut ✕

Nom de l'attribut :
Service-Type

Numéro de l'attribut :
6

Format de l'attribut :
Enumerator

Valeur d'attribut :

☐ Communément utilisé pour les connexions d'accès à distance ou VPN
<Aucun> ▼

☐ Communément utilisé pour les connexions 802.1x
<Aucun> ▼

☒ Autres
Login ▼

OK Annuler

Vous devriez avoir ceci :

Nouvelle stratégie réseau



Configurer les paramètres

Le serveur NPS applique des paramètres à la demande de connexion si toutes les conditions relatives à la stratégie de demande de connexion sont remplies.

Configurez les paramètres de cette stratégie réseau.

Si la demande de connexion répond aux conditions et contraintes, et si la stratégie accorde l'accès, les paramètres sont appliqués.

Paramètres :

Attributs RADIUS

Standard

☒ Spécifiques au fournisseur

Routage et accès à distance

Liaisons multiples et protocole BAP (Bandwidth Allocation Protocol)

Filtres IP

Chiffrement

Paramètres IP

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
Service-Type	Login

Ajouter...

Modifier...

Supprimer

Précédent

Suivant

Terminer

Annuler

Ensuite cliquez sur « Spécifiques au fournisseur », puis sur « Ajouter... » :

Nouvelle stratégie réseau



Configurer les paramètres

Le serveur NPS applique des paramètres à la demande de connexion si toutes les conditions relatives à la stratégie de demande de connexion sont remplies.

Configurez les paramètres de cette stratégie réseau.

Si la demande de connexion répond aux conditions et contraintes, et si la stratégie accorde l'accès, les paramètres sont appliqués.

Paramètres :

Attributs RADIUS

Standard

☒ Spécifiques au fournisseur

Routage et accès à distance

Liaisons multiples et protocole BAP (Bandwidth Allocation Protocol)

Filtres IP

Chiffrement

Paramètres IP

Pour envoyer des attributs supplémentaires aux clients RADIUS, sélectionnez un attribut spécifique au fournisseur, 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	Fournisseur	Valeur

Ajouter...

Modifier...

Supprimer

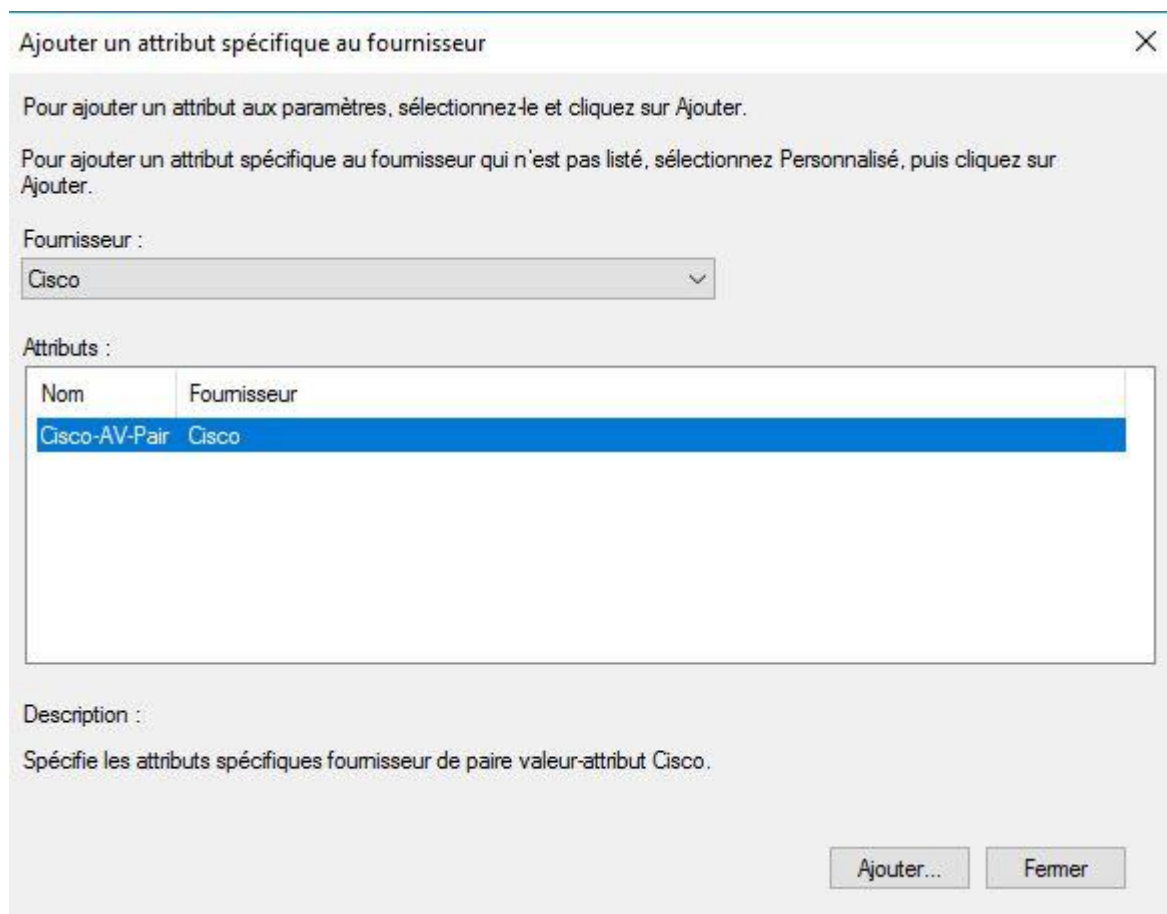
Précédent

Suivant

Terminer

Annuler

Sélectionnez Cisco-AV-Pair » :



Ajouter un attribut spécifique au fournisseur

Pour ajouter un attribut aux paramètres, sélectionnez-le et cliquez sur Ajouter.

Pour ajouter un attribut spécifique au fournisseur qui n'est pas listé, sélectionnez Personnalisé, puis cliquez sur Ajouter.

Fournisseur :

Cisco

Attributs :

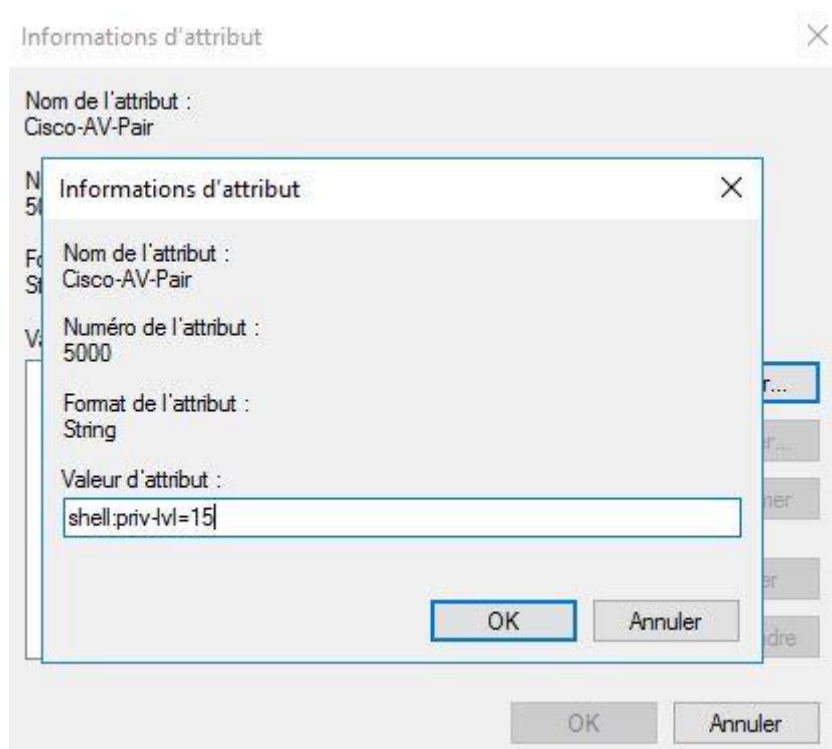
Nom	Fournisseur
Cisco-AV-Pair	Cisco

Description :

Spécifie les attributs spécifiques fournisseur de paire valeur-attribut Cisco.

Ajouter... Fermer

Dans le champ, saisissez la variable « shell:priv-lvl=15 ». Les niveaux d'administration fonctionnent exactement comme sur le switch. Le niveau 15 donne tous les droits.



Informations d'attribut

Nom de l'attribut :
Cisco-AV-Pair

Nom de l'attribut :
Cisco-AV-Pair

Numéro de l'attribut :
5000

Format de l'attribut :
String

Valeur d'attribut :
shell:priv-lvl=15

OK Annuler

Vous devriez avoir comme ci-dessous. Cliquez ensuite sur « Suivant » :

Nouvelle stratégie réseau



Configurer les paramètres

Le serveur NPS applique des paramètres à la demande de connexion si toutes les conditions relatives à la stratégie de demande de connexion sont remplies.

Configurez les paramètres de cette stratégie réseau.

Si la demande de connexion répond aux conditions et contraintes, et si la stratégie accorde l'accès, les paramètres sont appliqués.

Paramètres :

Attributs RADIUS



Standard



Spécifiques au fournisseur

Routage et accès à distance



Liaisons multiples et protocole BAP (Bandwidth Allocation Protocol)



Filtres IP



Chiffrement



Paramètres IP

Pour envoyer des attributs supplémentaires aux clients RADIUS, sélectionnez un attribut spécifique au fournisseur, 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	Fournisseur	Valeur
Cisco-AV-Pair	Cisco	shell:priv-lvl=15

Ajouter...

Modifier...

Supprimer

Précédent


Suivant

Terminer

Annuler

Vous aurez le récapitulatif de la stratégie réseau, cliquez sur « Terminer » :

Nouvelle stratégie réseau X

 **Fin de la configuration de la nouvelle stratégie réseau**

Vous avez correctement créé la stratégie réseau suivante :

acces_sw_cisco

Conditions de la stratégie :

Condition	Valeur
Groupes Windows	TEST\ADM_reseau

Paramètres de la stratégie :

Condition	Valeur
Méthode d'authentification	Authentification non chiffrée (PAP, SPAP)
Autorisation d'accès	Accorder l'accès
Ignorer les propriétés de numérotation des utilisateurs	Faux
Service-Type	Login
Cisco-AV-Pair	shell:priv-lvl=15


Pour fermer cet Assistant, cliquez sur Terminer.

Précédent Suivant Terminer Annuler

Les stratégies sont traitées dans l'ordre de la liste. Faites attention que les stratégies par défaut ou d'autres stratégies de votre réseau ne refusent pas l'accès avant votre stratégie :

Serveur NPS (Network Policy Server) — □ X

Fichier Action Affichage ?






NPS (Local)

- ✓ Clients et serveurs RADIUS
 - Clients RADIUS
 - Groupes de serveurs RA
- ✓ Stratégies
 - Stratégies de demande
 - Stratégies réseau**
 - Gestion
- > Gestion des modèles

Stratégies réseau

Les stratégies réseau vous permettent d'autoriser les connexions au réseau de manière sélective, et d'indiquer les circonstances dans lesquelles ces connexions peuvent s'effectuer ou non.

Nom de la stratégie	État	Ordre de traitement	Type d'accès
 acces_sw_cisco	Activé	1	Accorder l'accès
 Connexions au serveur Microsoft de Routage et Accès distants	Activé	999998	Refuser l'accès
 Connexions à d'autres serveurs d'accès	Activé	999999	Refuser l'accès

< >