

DESCRIPTION D'UNE MISSION BTS SIO			
Prénom – Nom		DELPEIRRE Hugo	N° mission
			6
Option	SISR ☒	SLAM ☐	
Situation	Formation ☒	Entreprise ☐	

Lieu de réalisation	Coordonnées entreprise ou centre de formation <i>selon le lieu de réalisation</i>	Logo entreprise ou du centre <i>selon le lieu de réalisation</i>
Période de réalisation	Du : 05/02/2024	Au : 12/02/2024
Modalité de réalisation	VÉCUE ☒	OBSERVÉE ☐

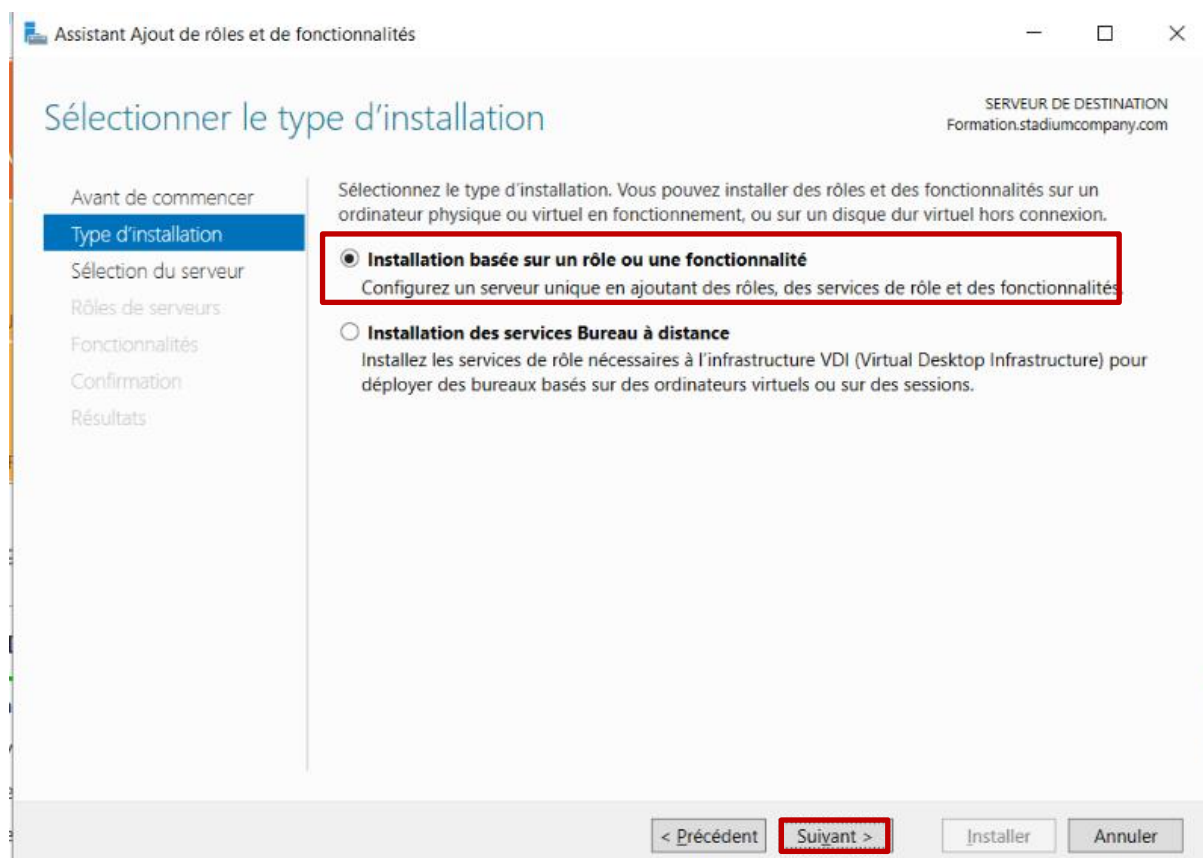
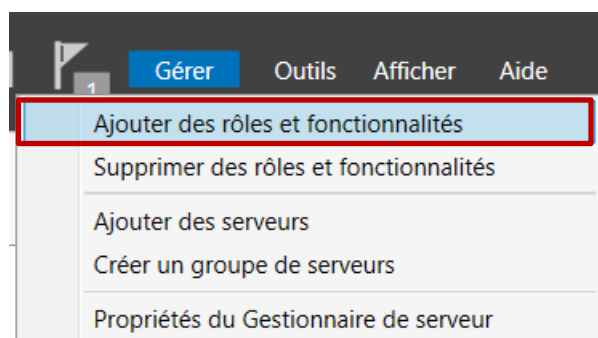
Intitulé de la mission	Titre de la mission	
	Implémentation d'un Réseau Wi-Fi pour les Employés et les Visiteurs au Stade	
Description du contexte de la mission	Description en 2 à 3 lignes maxi	
	La mission consiste à mettre en place une solution d'accès Wi-Fi pour les employés du stade de StadiumCompany, ainsi que pour les visiteurs. Les visiteurs auront un accès limité à Internet, conformément aux obligations légales. Voici les éléments du cahier des charges concernant les accès Wi-Fi : 1. Point d'accès par Service : Chaque service dispose d'un point d'accès 802.11 b/g/n compatible PoE (Power over Ethernet). Un SSID non diffusé est attribué à chaque service, sauf pour le VLAN visiteur. 2. Sécurité par WPA2, WPA3 Enterprise : La sécurité des réseaux Wi-Fi sera assurée par la norme WPA2 Enterprise. Cela garantit une authentification robuste pour les employés	

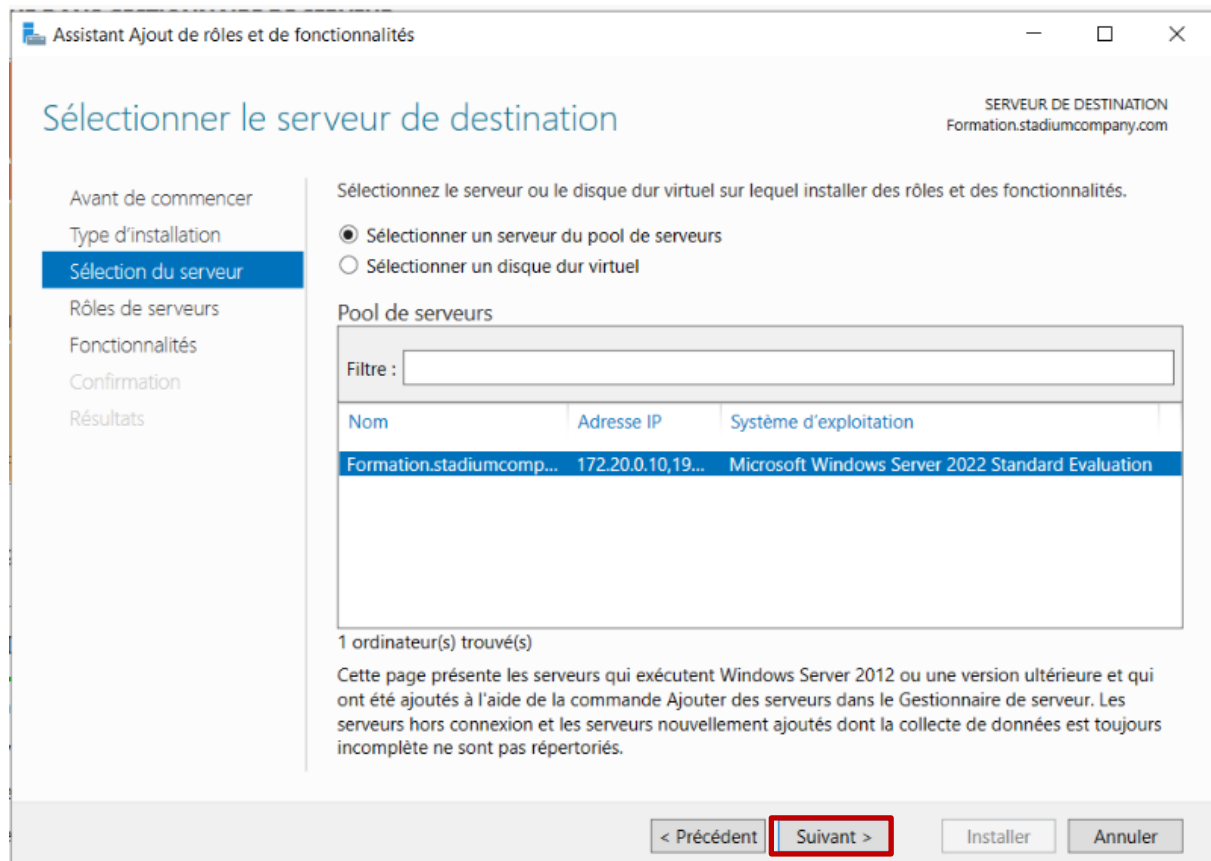
Ressources et outils utilisés	Liste des ressources disponibles et outils utilisés (Documentations, Matériels et Logiciels)	
	Windows Server avec services (Service de Certificats AD, Service Serveur NPS) Borne WI-Fi Cisco	
Résultat attendu	Résultat attendu avec la réalisation de cette mission	
	Avoir une solution d'accès Wi-Fi avec Authentification RADIUS.	
Contraintes	Contraintes : techniques budgétaires temps O.S. ou outils imposés...	

Compétences associées <i>(voir tableau)</i>	Liste des intitulés du tableau de compétences (avec les références)
	Maîtrise de l'utilisation des services « Certificats AD » et « Serveur NPS ».

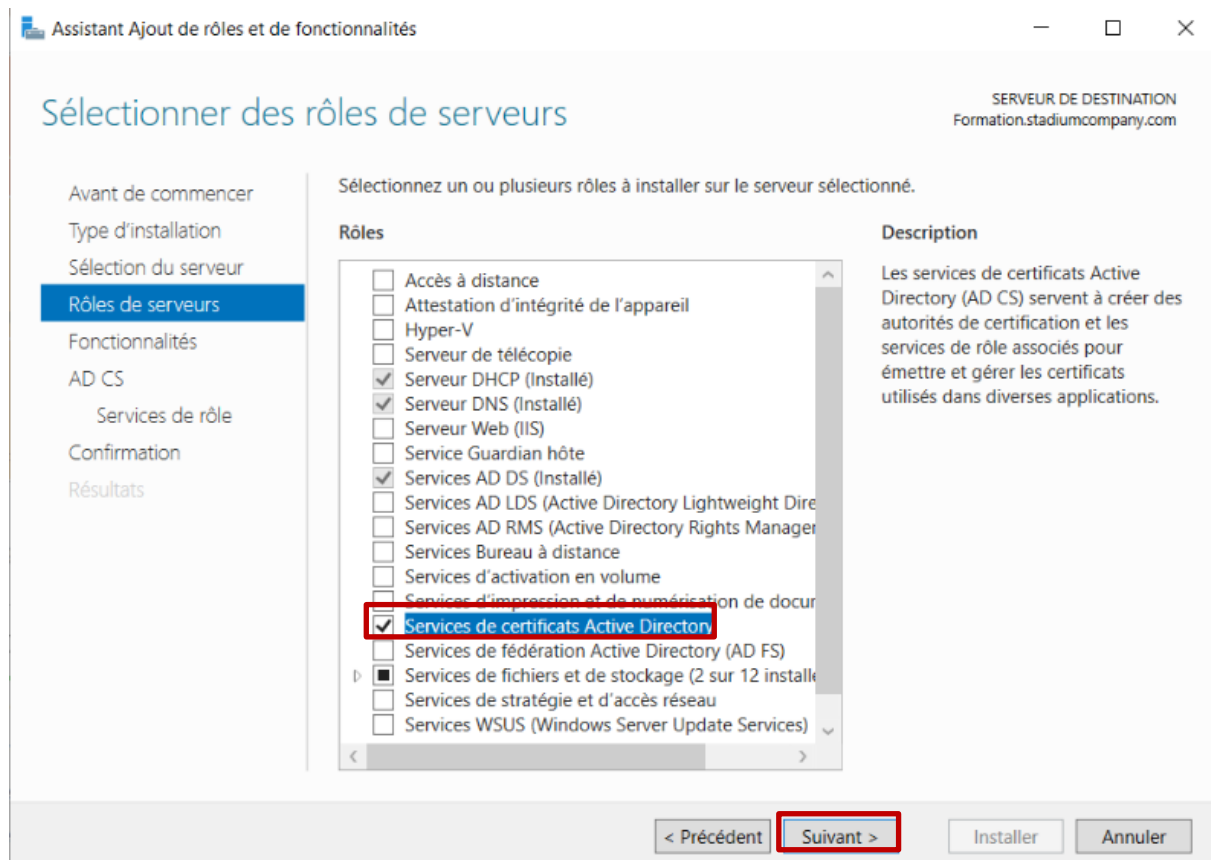
Description simplifiée des différentes étapes de réalisation de la mission en mettant en évidence la démarche suivie, les méthodes et les techniques utilisées

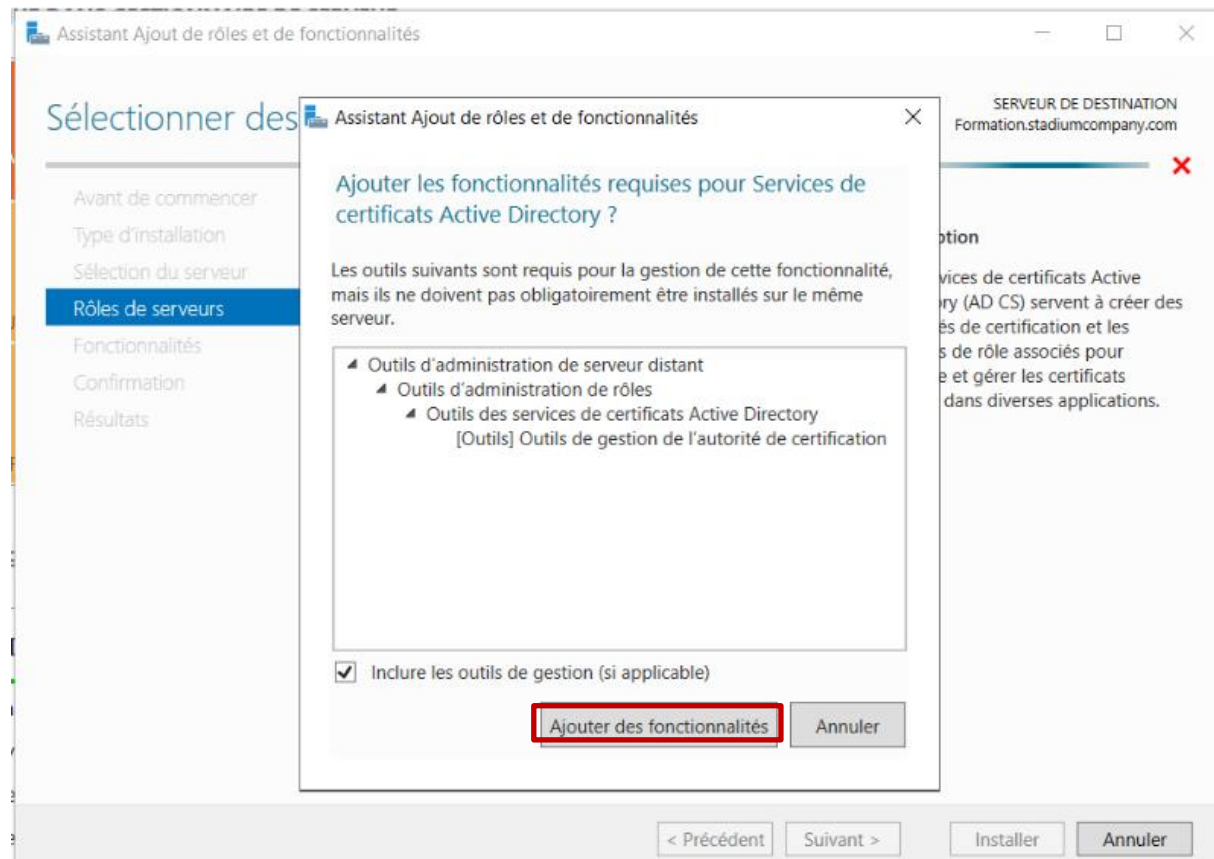
Rendez-vous sur votre contrôleur de domaine Active Directory pour ajouter le rôle « Service de certificats Active Directory » :



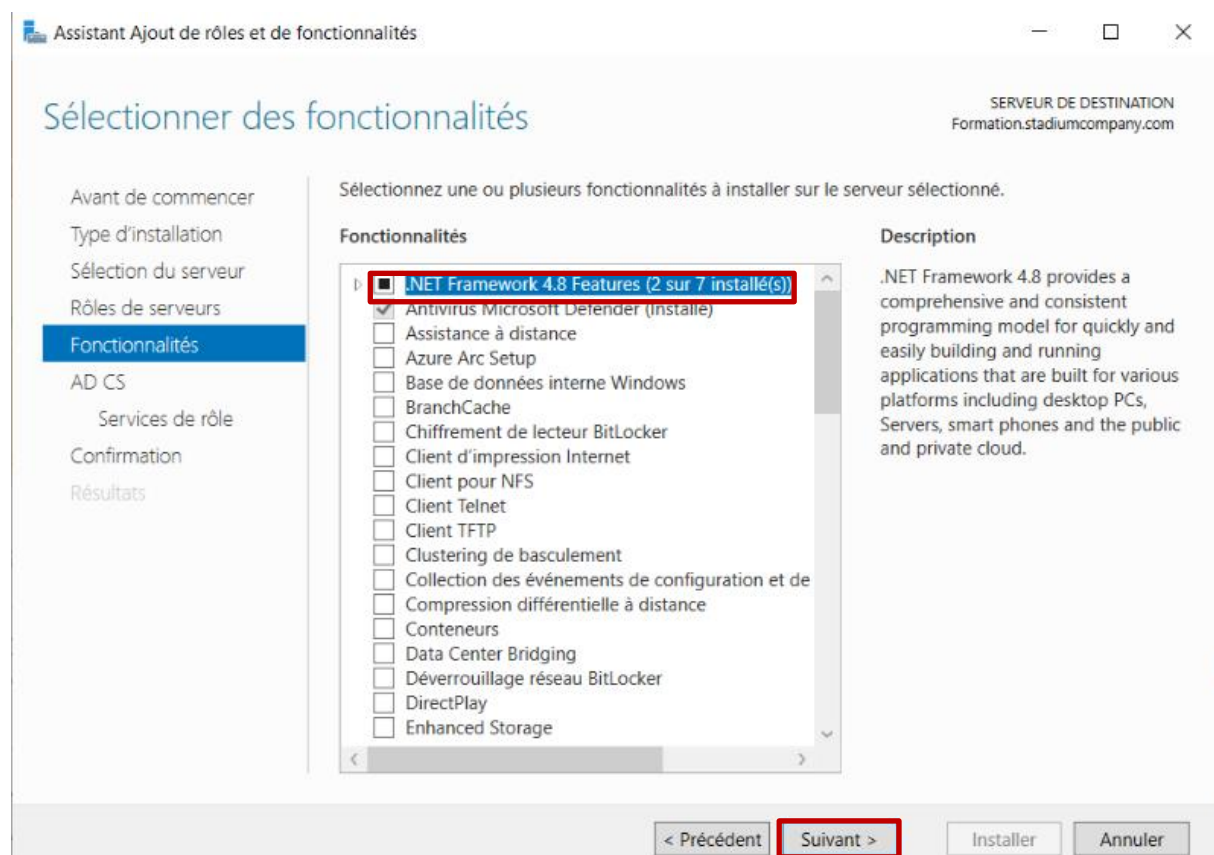


Sélectionner le rôle « Service de certificats Active Directory ».

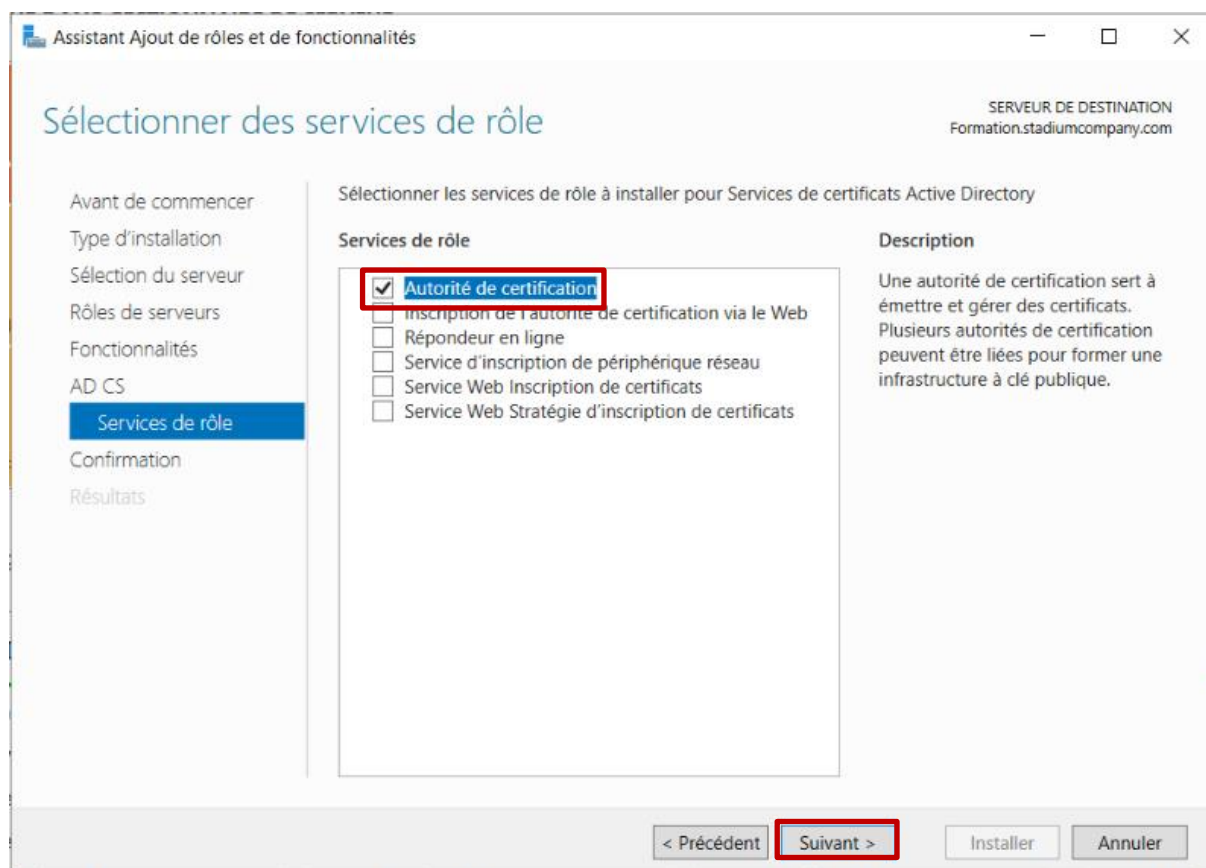




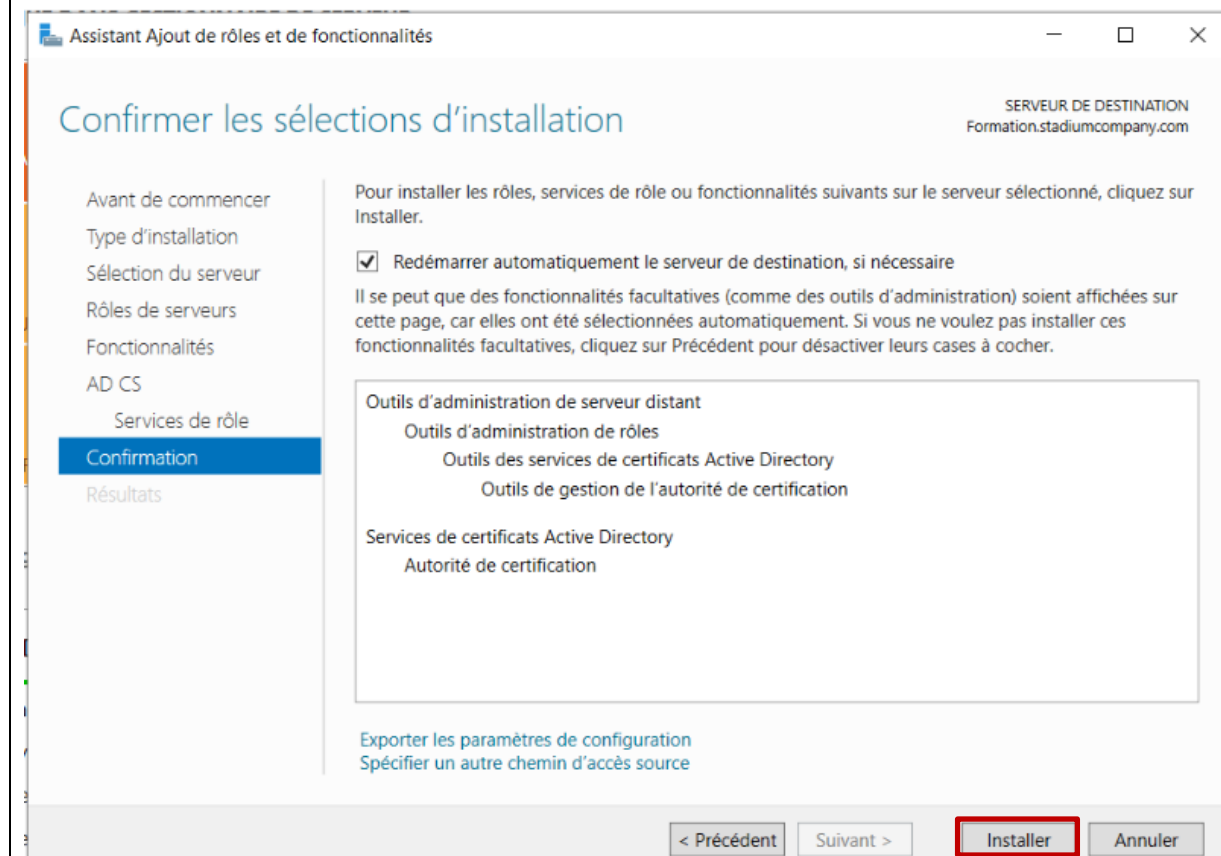
Ajouter la fonctionnalité « .NET Framework 4.8 Features ».

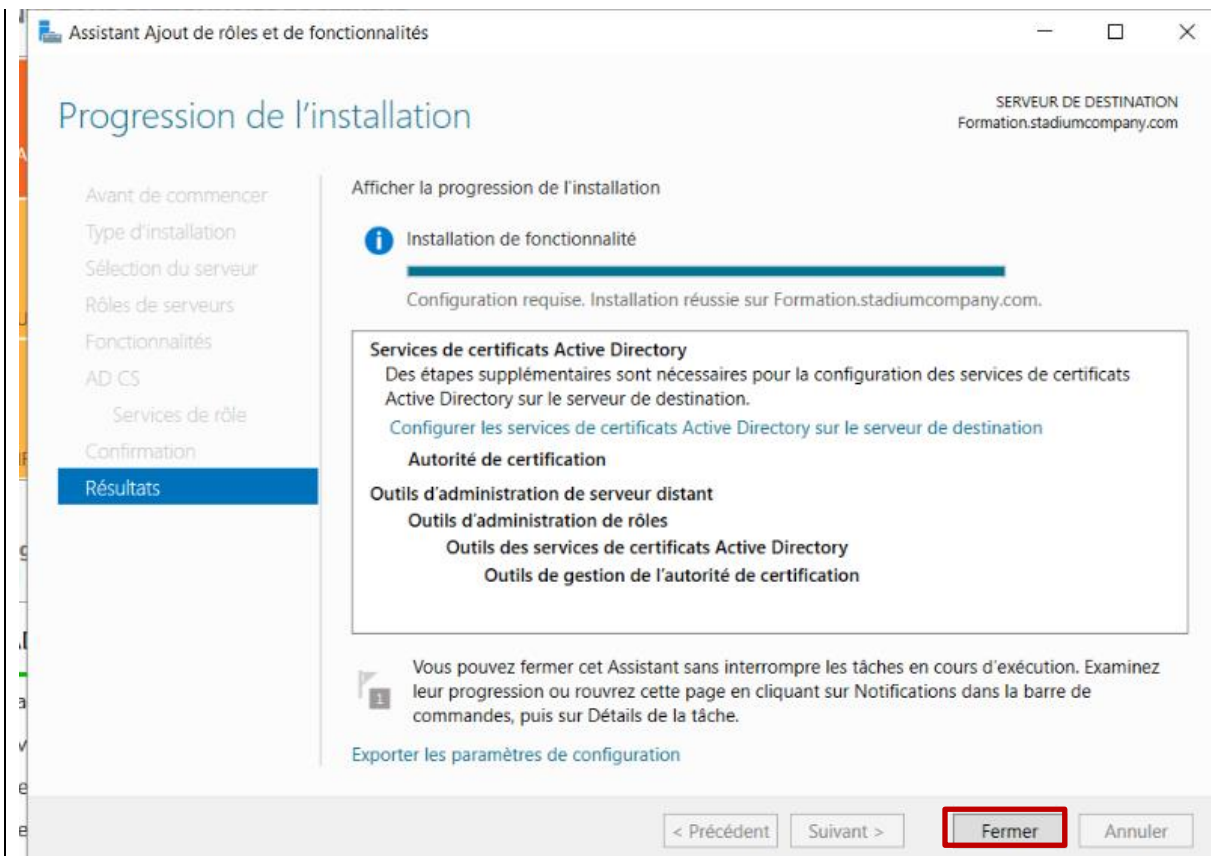


Pour le rôle, sélectionner « Autorité de certification ».

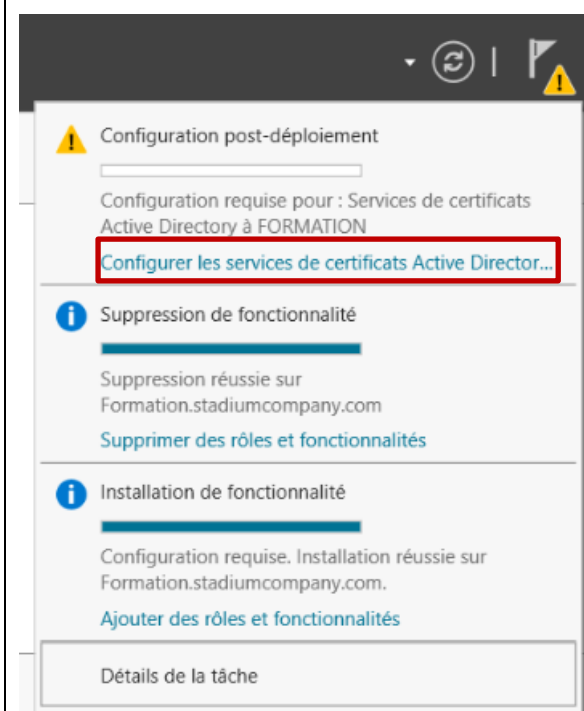


Cliquer sur « Installer »





Une fois cela fait, il faut configurer le service installé.



Configuration des services de certificats Active Directory

Informations d'identification

SERVEUR DE DESTINATION
Formation.stadiumcompany.com

Informations d'identification...

Services de rôle

Confirmation

Progression

Résultats

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 : STADIUMCOMPANY\Administrati Modifier...

En savoir plus sur les rôles de serveur AD CS

< Précédent Suivant > Configurer Annuler

Cocher « Autorité de certification ».

Configuration des services de certificats Active Directory

Services de rôle

SERVEUR DE DESTINATION
Formation.stadiumcompany.com

Informations d'identification...

Services de rôle

Type d'installation

Type d'AC

Clé privée

Chiffrement

Nom de l'AC

Période de validité

Base de données de certi...

Confirmation

Progression

Résultats

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

Cocher « Autorité de certification d'entreprise ».

The screenshot shows the 'Configuration des services de certificats Active Directory' window. The title bar includes the window name and standard Windows controls. The main heading is 'Type d'installation'. On the right, it says 'SERVEUR DE DESTINATION: Formation.stadiumcompany.com'. A left-hand navigation pane lists steps: Informations d'identificati..., Services de rôle, Type d'installation (highlighted), Type d'AC, Clé privée, Chiffrement, Nom de l'AC, Période de validité, Base de données de certi..., Confirmation, Progression, and Résultats. The main area is titled 'Spécifier le type d'installation de l'AC'. It contains two radio button options. The first option, 'Autorité de certification d'entreprise', is selected and highlighted with a red rectangle. Below it, text explains that enterprise certification authorities must be domain members and typically online. The second option, 'Autorité de certification autonome', is unselected. Below it, text explains that autonomous authorities can be group members or offline. At the bottom, there are four buttons: '< Précédent', 'Suivant >' (highlighted with a red rectangle), 'Configurer', and 'Annuler'. A link 'En savoir plus sur le type d'installation' is at the bottom left.

Configuration des services de certificats Active Directory

SERVEUR DE DESTINATION
Formation.stadiumcompany.com

Type d'installation

Informations d'identificati...
Services de rôle
Type d'installation
Type d'AC
Clé privée
Chiffrement
Nom de l'AC
Période de validité
Base de données de certi...
Confirmation
Progression
Résultats

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

Cocher « Autorité de certification racine ».

The screenshot shows the 'Configuration des services de certificats Active Directory' window at the 'Type d'autorité de certification' step. The title bar and destination server information are the same. The left-hand navigation pane highlights 'Type d'AC'. The main area is titled 'Spécifier le type de l'AC'. It contains two radio button options. The first option, 'Autorité de certification racine', is selected and highlighted with a red rectangle. Below it, text explains that root authorities are the first or only in a PKI hierarchy. The second option, 'Autorité de certification secondaire', is unselected. Below it, text explains that secondary authorities need an established PKI hierarchy. At the bottom, there are four buttons: '< Précédent', 'Suivant >' (highlighted with a red rectangle), 'Configurer', and 'Annuler'. A link 'En savoir plus sur le type d'autorité de certification' is at the bottom left.

Configuration des services de certificats Active Directory

SERVEUR DE DESTINATION
Formation.stadiumcompany.com

Type d'autorité de certification

Informations d'identificati...
Services de rôle
Type d'installation
Type d'AC
Clé privée
Chiffrement
Nom de l'AC
Période de validité
Base de données de certi...
Confirmation
Progression
Résultats

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

Il faut créer une clé privée, on coche donc « Créer une clé privée ».

Configuration des services de certificats Active Directory

SERVEUR DE DESTINATION
Formation.stadiumcompany.com

Clé privée

Informations d'identification...
Services de rôle
Type d'installation
Type d'AC
Clé privée
Chiffrement
Nom de l'AC
Période de validité
Base de données de certi...
Confirmation
Progression
Résultats

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

On configure l'option de chiffrement en algorithme de hachage « SHA1 ».

Configuration des services de certificats Active Directory

SERVEUR DE DESTINATION
Formation.stadiumcompany.com

Chiffrement pour l'autorité de certification

Informations d'identificati...
Services de rôle
Type d'installation
Type d'AC
Clé privée
Chiffrement
Nom de l'AC
Période de validité
Base de données de certi...
Confirmation
Progression
Résultats

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

SERVEUR DE DESTINATION
Formation.stadiumcompany.com

Nom de l'autorité de certification

Informations d'identificati...
Services de rôle
Type d'installation
Type d'AC
Clé privée
Chiffrement
Nom de l'AC
Période de validité
Base de données de certi...
Confirmation
Progression
Résultats

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 :
stadiumcompany-FORMATION-CA

Suffixe du nom unique :
DC=stadiumcompany,DC=com

Aperçu du nom unique :
CN=stadiumcompany-FORMATION-CA,DC=stadiumcompany,DC=com

[En savoir plus sur le nom de l'autorité de certification](#)

< Précédent **Suivant >** Configurer Annuler

On spécifie la date de validité du certificat à 5 ans pour cette autorité de certification AD.

Configuration des services de certificats Active Directory

SERVEUR DE DESTINATION
Formation.stadiumcompany.com

Période de validité

Informations d'identificati...
Services de rôle
Type d'installation
Type d'AC
Clé privée
Chiffrement
Nom de l'AC
Période de validité
Base de données de certi...
Confirmation
Progression
Résultats

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 : 05/02/2029 14:03:00

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

SERVEUR DE DESTINATION
Formation.stadiumcompany.com

Base de données de l'autorité de certification

Informations d'identificati...
Services de rôle
Type d'installation
Type d'AC
Clé privée
Chiffrement
Nom de l'AC
Période de validité
Base de données de certi...
Confirmation
Progression
Résultats

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

Configuration des services de certificats Active Directory

Confirmation

SERVEUR DE DESTINATION
Formation.stadiumcompany.com

Informations d'identificati...
Services de rôle
Type d'installation
Type d'AC
Clé privée
Chiffrement
Nom de l'AC
Période de validité
Base de données de certi...
Confirmation
Progression
Résultats

Pour configurer les rôles, services de rôle ou fonctionnalités ci-après, cliquez sur Configurer.

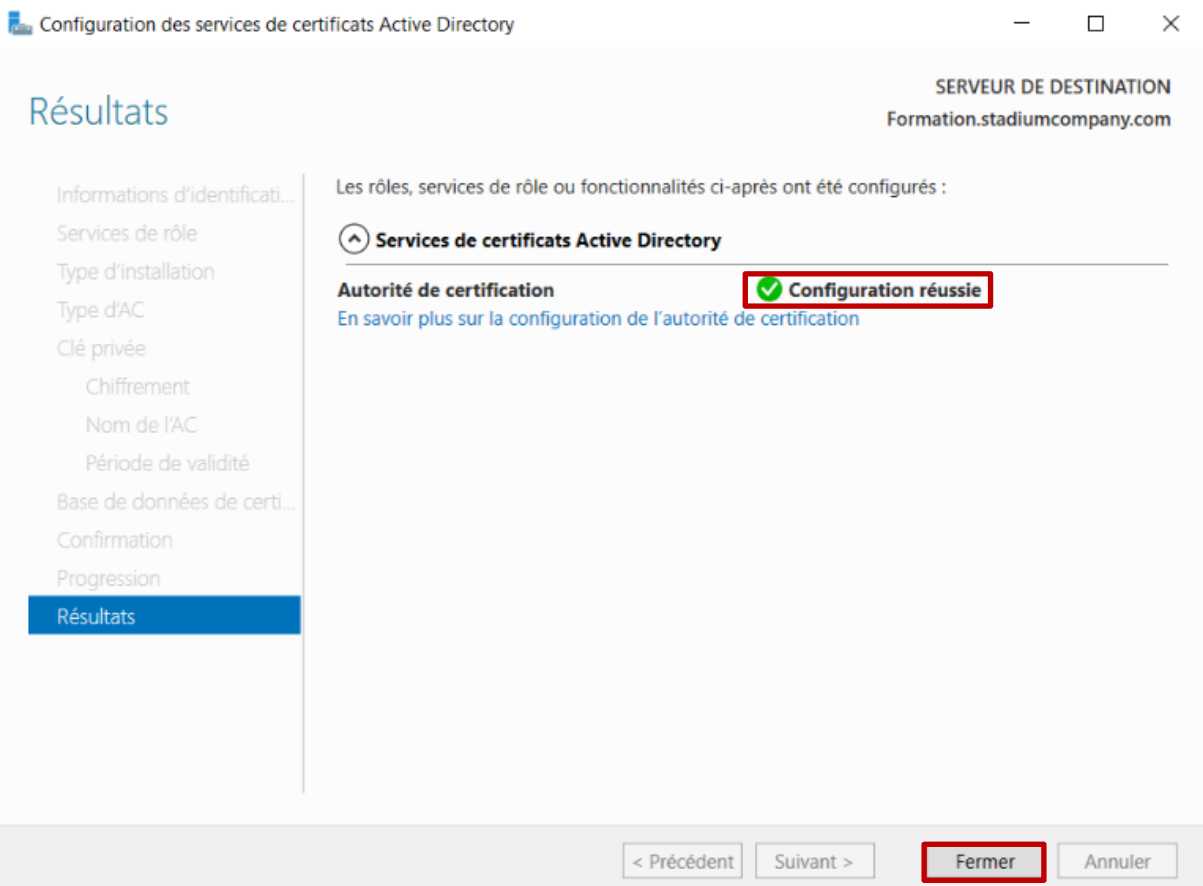
Services de certificats Active Directory

Autorité de certification

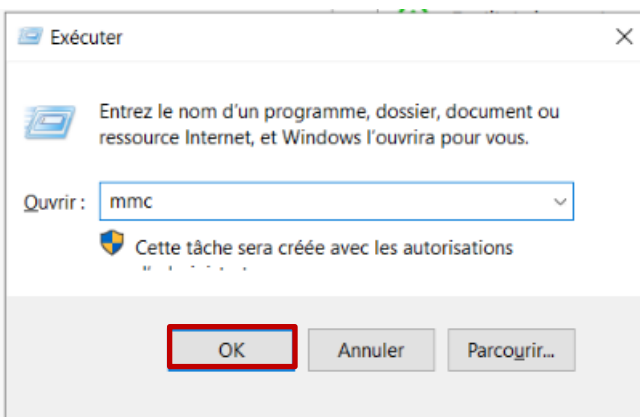
Type d'AC :	Racine d'entreprise
Fournisseur de services de chiffrement :	RSA#Microsoft Software Key Storage Provider
Algorithme de hachage :	SHA1
Longueur de la clé :	2048
Autoriser l'interaction de l'administrateur :	Activé
Période de validité du certificat :	05/02/2029 14:03:00
Nom unique :	CN=stadiumcompany-FORMATION-CA,DC=stadiumcompany,DC=com
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

< Précédent Suivant > **Configurer** Annuler

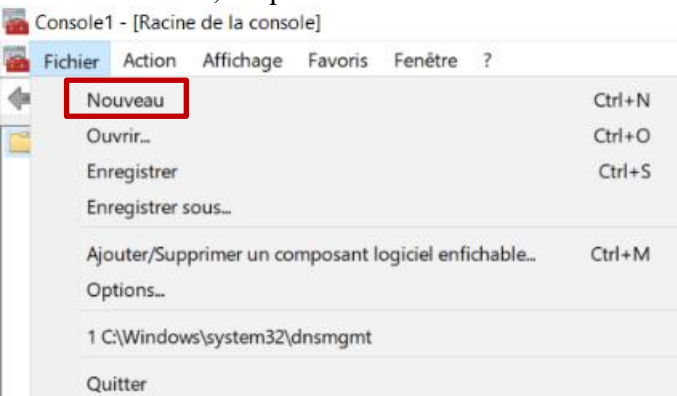
Windows nous confirme que la configuration du service est réussie. Cliquer sur « Fermer ».



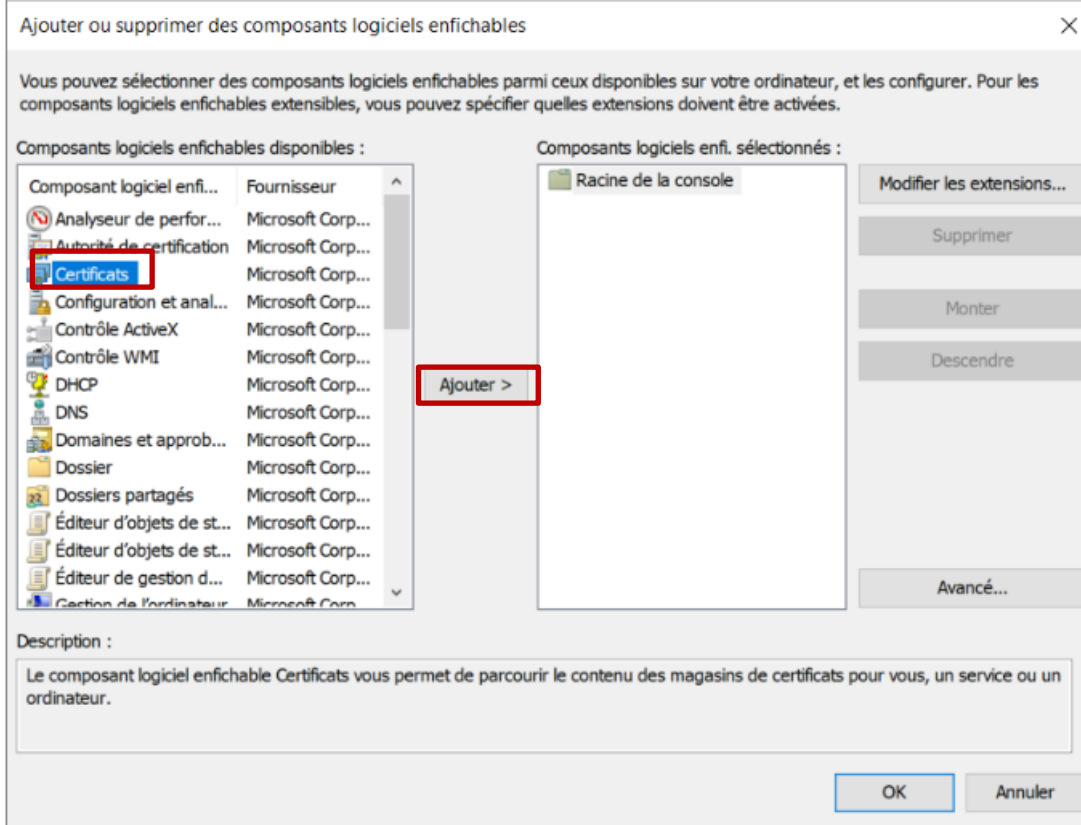
Avec la commande « Win + R », taper « mmc » pour ouvrir le service de certificat AD.



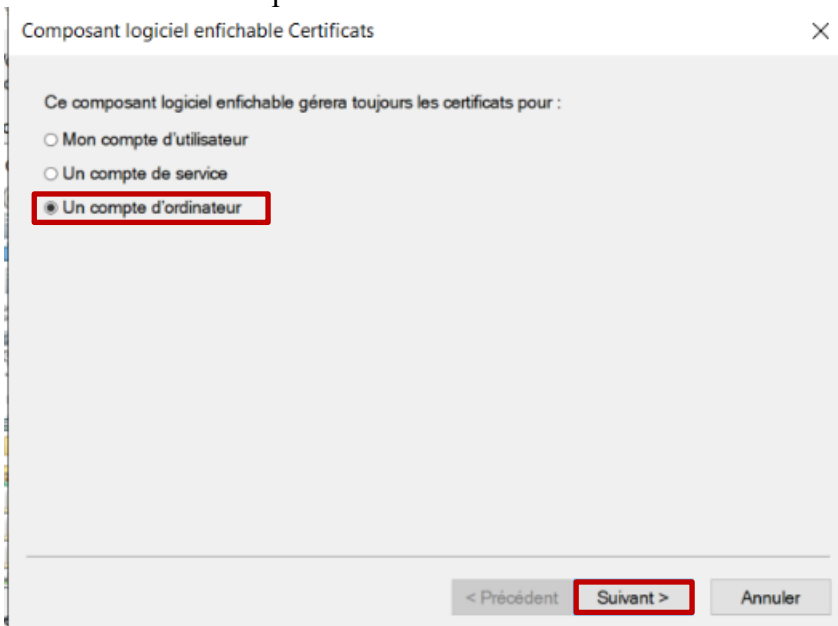
Dans « Fichier », cliquer sur « Nouveau ».



On va ajouter et configurer un certificat. Cliquer sur « Certificats » puis sur « Ajouter ».



Choisir « Un compte d'ordinateur ».



Sélectionner « Ordinateur local », puis « Terminer ».

Sélectionner un ordinateur

Sélectionnez l'ordinateur devant être géré par ce composant logiciel enfichable.

Ce composant logiciel enfichable gèrera 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

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 enfichables extensibles, vous pouvez spécifier quelles extensions doivent être activées.

Composants logiciels enfichables disponibles :

Composant logiciel enfi...	Fournisseur
Analyseur de perfor...	Microsoft Corp...
Autorité de certification	Microsoft Corp...
Certificats	Microsoft Corp...
Configuration et anal...	Microsoft Corp...
Contrôle ActiveX	Microsoft Corp...
Contrôle WMI	Microsoft Corp...
DHCP	Microsoft Corp...
DNS	Microsoft Corp...
Domaines et approb...	Microsoft Corp...
Dossier	Microsoft Corp...
Dossiers partagés	Microsoft Corp...
Éditeur d'objets de st...	Microsoft Corp...
Éditeur d'objets de st...	Microsoft Corp...
Éditeur de gestion d...	Microsoft Corp...
Gestion de l'ordinateur	Microsoft Corp...

Ajouter >

Composants logiciels enfi. sélectionnés :

- Racine de la console
- Certificats (ordinateur local)

Modifier les extensions...

Supprimer

Monter

Descendre

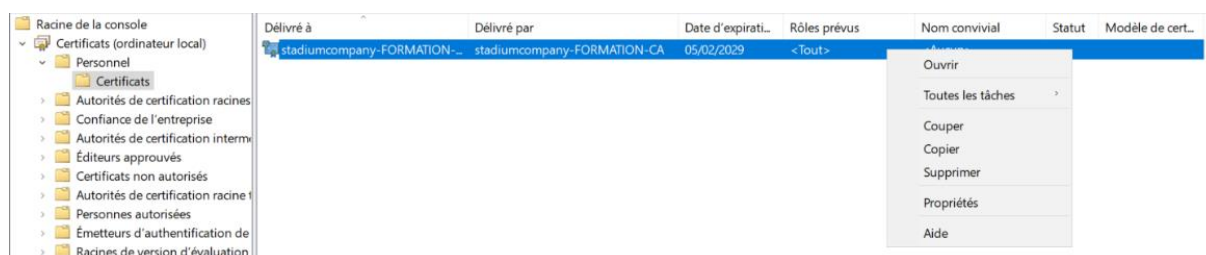
Avancé...

Description :

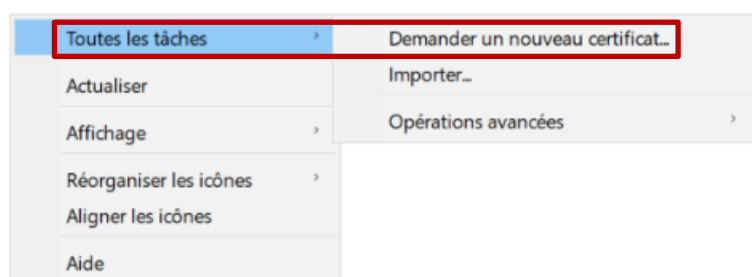
Le composant logiciel enfichable Certificats vous permet de parcourir le contenu des magasins de certificats pour vous, un service ou un ordinateur.

OK Annuler

Dans la racine du service « Certificats AD », sélectionner « Certificats » et supprimer le certificat affiché, et supprimer le.



Dans fichier -> Toutes les tâches, sélectionner « Demander un nouveau certificat ».



Inscription de certificats

Sélectionner la stratégie d'inscription de certificat

La stratégie d'inscription de certificat permet l'inscription de certificats en fonction de modèles de certificats prédéfinis. Il est possible qu'elle soit déjà configurée.

Configurés par votre administrateur

Stratégie d'inscription à Active Directory

Configurés par vous [Ajouter une nouvelle URL](#)

Suivant

Annuler

Cliquer sur « Contrôleur de domaine », puis sur « Inscription ».

Inscription de certificats

Demander des certificats

Vous pouvez demander les types de certificats suivants. Sélectionnez les certificats que vous voulez demander, puis cliquez sur Inscription.

Stratégie d'inscription à Active Directory		
☐ Authentification du contrôleur de domaine	 Statut : Disponible	Détails ▾
☐ Authentification Kerberos	 Statut : Disponible	Détails ▾
☒ Contrôleur de domaine	 Statut : Disponible	Détails ▾
☐ Réplication de la messagerie de l'annuaire	 Statut : Disponible	Détails ▾

☐ Afficher tous les modèles

Inscription

Annuler

L'inscription du nouveau certificat est réussie, cliquer sur « Terminer ».

Inscription de certificats

Résultats de l'installation des certificats

Les certificats suivants ont été inscrits et installés sur cet ordinateur.

Stratégie d'inscription à Active Directory		
☒ Contrôleur de domaine	 Statut : Opération réussie	Détails ▾

Terminer

Vous devriez voir apparaître deux certificats avec les rôles « Authentification du client / du serveur ».

Delivré à	Delivré par	Date d'expiration	Rôles prévus	Non
Formation.stadiumcompany.com	stadiumcompany-FORMATION-CA	04/02/2025	Authentification du client, Authentification du serveur	< Au
Formation.stadiumcompany.com	stadiumcompany-FORMATION-CA	04/02/2025	Authentification du client, Authentification du serveur	< Au

Voici la configuration de la carte réseau du contrôleur de domaine :

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 : 10 . 0 . 228 . 83

Masque de sous-réseau : 255 . 255 . 254 . 0

Passerelle par défaut : 10 . 0 . 228 . 1

☐ Obtenir les adresses des serveurs DNS automatiquement

☒ Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré : 127 . 0 . 0 . 1

Serveur DNS auxiliaire : 1 . 1 . 1 . 1

☐ Valider les paramètres en quittant

Avancé...

OK Annuler

On vient ajouter des rôles de serveurs une nouvelle fois, on sélectionne le rôle « Services de stratégie et d'accès réseau ».

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

Confirmation

Résultats

Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné

Rôles

- ☐ 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 Directory Services)
- ☐ Services AD RMS (Active Directory Rights Management Services)
- ☐ Services Bureau à distance
- ☐ Services d'activation en volume
- ☐ Services d'impression et de numérisation de documents
- ☒ Services de certificats Active Directory (1 sur 6 installés)
- ☐ Services de fédération Active Directory (AD FS)
- ☒ Services de fichiers et de stockage (2 sur 12 installés)
- ☒ Services de stratégie et d'accès réseau
- ☐ Services WSUS (Windows Server Update Services)
- ☐ Windows Deployment Services

SERVER DE DESTINATION

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

< Précédent Suivant > Installer Annuler

Services de stratégie et d'accès réseau

SERVEUR DE DESTINATION
Formation.stadiumcompany.com

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Services de stratégie et d'

Confirmation

Résultats

Les services de stratégie et d'accès réseau vous permettent de définir et d'appliquer des stratégies d'accès réseau, d'authentification et d'autorisation à l'aide du serveur NPS (Network Policy Server).

À noter :

- Vous pouvez déployer NPS comme un serveur et un proxy RADIUS (Remote Authentication Dial-In User Service). Après l'installation du serveur NPS au moyen de cet Assistant, vous pouvez configurer NPS à partir de la page d'accueil NPAS en utilisant la console NPS.

< Précédent

Suivant >

Installer

Annuler

Cliquer sur « Installer ».

Assistant Ajout de rôles et de fonctionnalités

SERVEUR DE DESTINATION
Formation.stadiumcompany.com

Confirmer les sélections d'installation

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

Assistant Ajout de rôles et de fonctionnalités

SERVEUR DE DESTINATION
Formation.stadiumcompany.com

Progression de l'installation

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Services de stratégie et d'...
Confirmation
Résultats

Afficher la progression de l'installation

i Installation de fonctionnalité

Installation réussie sur Formation.stadiumcompany.com.

Outils d'administration de serveur distant

Outils d'administration de rôles

Outils de la stratégie réseau et des services d'accès

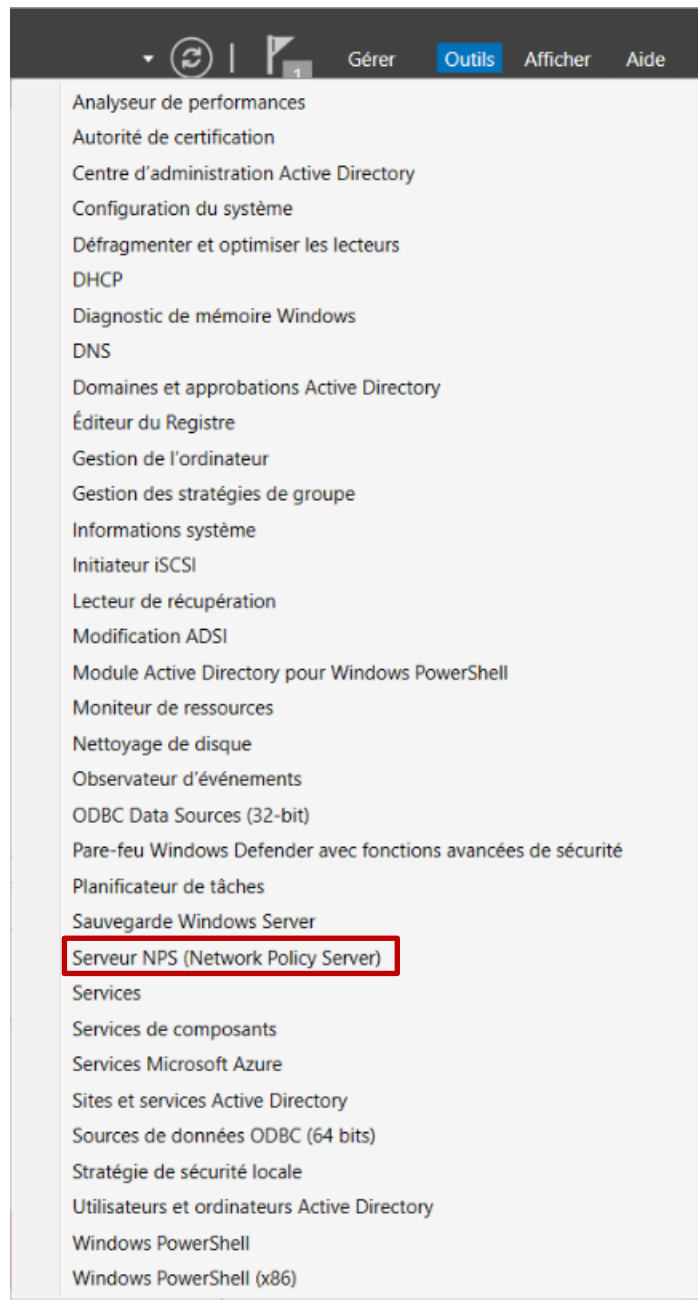
Services de stratégie et d'accès réseau

1 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.

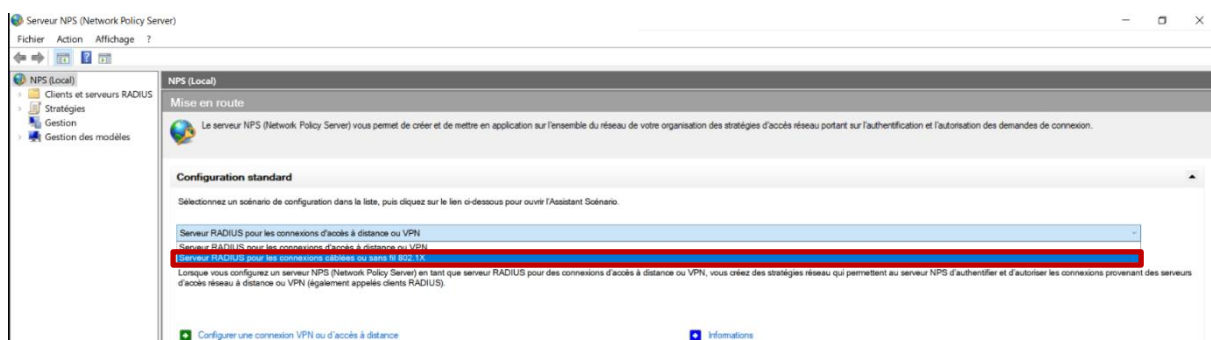
[Exporter les paramètres de configuration](#)

< Précédent Suivant > **Fermer** Annuler

Dans le gestionnaire de serveur, Ouvrir le service « Serveur NPS » récemment installé.



Sélectionner « Serveur RADIUS pour les connexions 802.1X ».



Cliquer sur « Configurer 802.1X »



Cette fenêtre apparaît. Sélectionner « Connexions sans fil sécurisées », puis « Suivant ».

The screenshot shows the 'Configurer 802.1X' window with the title 'Sélectionner le type de connexions 802.1X'. It features a red box around the 'Type de connexions 802.1X' section, which contains two radio buttons. The first, 'Connexions sans fil sécurisées', is selected. Below it, a text box contains the text: '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.' The second option is 'Connexions câblées (Ethernet) sécurisées'. Below this, there is a 'Nom' field with the text 'Connexions sans fil sécurisées' and a 'Suivant' button highlighted with a red box.

Configurer 802.1X

Sélectionner le type de connexions 802.1X

Type de connexions 802.1X :

☒ Connexions sans fil sécurisées

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

Précédent Suivant Terminer Annuler

Cliquer sur « Ajouter ». Ici, nommer le client Radius (Wi-Fi Radius », et insérer son adresse IP. Dans la section « Secret partagé », il faut renseigner le mot de passe utilisé pour se connecter au futur client Radius. Le nôtre est « BTS2024\$ ».

The screenshot shows the 'Configurer 802.1X' window with the title 'Spécifier les commutateurs 802.1X'. It features a red box around the 'Ajouter...' button in the 'Clients RADIUS' section. A 'Nouveau client RADIUS' dialog box is open, showing the 'Paramètres' tab. The dialog box has a red box around the 'Nom et adresse' section, which contains the text 'Wi-Fi-Radius' and '10.0.228.63'. The 'Secret partagé' section contains the text 'Aucun' and 'Manuel'. The 'OK' button is highlighted with a red box.

Configurer 802.1X

Spécifier les commutateurs 802.1X

Spécifiez les commutateurs ou points d'accès sans fil 802.1X (clients RADIUS)

Les clients RADIUS sont des serveurs d'accès réseau, à l'image des commutateurs d'authentification et des points d'accès sans fil. Les clients RADIUS ne sont pas des ordinateurs clients.

Pour spécifier un client RADIUS, cliquez sur Ajouter.

Clients RADIUS :

Ajouter...

Modifier...

Supprimer

Nouveau client RADIUS

Paramètres

☐ Sélectionner un modèle existant :

Nom et adresse

Nom convivial :

Wi-Fi-Radius

Adresse (IP ou DNS) :

10.0.228.63

Vérifier...

Secret partagé

Sélectionnez un modèle de secrets partagés existant :

Aucun

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.

☒ Manuel ☐ Générer

Secret partagé :

Confirmez le secret partagé :

OK Annuler

Le client récemment configuré apparaît désormais dans la liste. Cliquer sur « Suivant ».

Configurer 802.1X

Spécifier les commutateurs 802.1X

Spécifiez les commutateurs ou points d'accès sans fil 802.1X (clients RADIUS)

Les clients RADIUS sont des serveurs d'accès réseau, à l'image des commutateurs d'authentification et des points d'accès sans fil. Les clients RADIUS ne sont pas des ordinateurs clients.

Pour spécifier un client RADIUS, cliquez sur Ajouter.

Clients RADIUS :

WiFi-Radius

Ajouter...

Modifier...

Supprimer

Précédent **Suivant** Terminer Annuler

Choisissez « Microsoft PEAP », puis « Suivant ».

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)
Microsoft: Carte à puce ou autre certificat
Microsoft: PEAP (Protected EAP)
Microsoft: Mot de passe sécurisé (EAP-MSCHAP version 2)

Configurer...

Précédent **Suivant** Terminer Annuler

Ajouter les utilisateurs souhaités dans « Ajouter », puis cliquer sur « Suivant ». (Nous avons sélectionné tous les utilisateurs du domaine).

Configurer 802.1X

Spécifier des groupes d'utilisateurs

L'accès des utilisateurs membres du ou des groupes sélectionnés sera autorisé ou non en fonction du paramètre d'autorisation d'accès de la stratégie réseau.

Pour sélectionner des groupes d'utilisateurs, cliquez sur Ajouter. Si aucun groupe n'est sélectionné, cette stratégie s'applique à tous les utilisateurs.

Groupes

STADIUMCOMPANY\Utilisateurs du domaine

Ajouter...

Supprimer

Précédent

Suivant

Terminer

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

Cliquer sur « Terminer ».

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 :
Wi-Fi-Radius (10.0.228.63)

Stratégie de demande de connexion :
Connexions sans fil sécurisées

Stratégies réseau :
Connexions sans fil sécurisées

[Détails de la configuration](#)

Précédent Suivant Terminer Annuler

Rendez-vous sur la page de votre borne Wi-Fi, dans la section « Express Security » et choisissez un SSID pour la borne. Dans la partie « Security », entrez l'adresse IP de votre Serveur Radius, ainsi que le « Server Secret » défini précédemment (Rappel : BTS2024\$ pour notre part).

HOME

EXPRESS SET-UP

EXPRESS SECURITY

NETWORK MAP

ASSOCIATION

NETWORK INTERFACES

SECURITY

SERVICES

WIRELESS SERVICES

SYSTEM SOFTWARE

EVENT LOG

LOGOUT

Hostname ap

Express Security Set-Up

SSID Configuration

1. SSID ☒ [Broadcast SSID in Beacon](#)

2. VLAN

☒ No VLAN

☐ Enable VLAN ID: (1-4094) ☐ Native VLAN

3. Security

☐ [No Security](#)

☐ [Static WEP Key](#)

Key 1 (128 bit)

☐ [EAP Authentication](#)

☒ [WPA](#)

RADIUS Server: (Hostname or IP Address)

RADIUS Server Secret:

RADIUS Server: (Hostname or IP Address)

RADIUS Server Secret:

Ref : SIO-THM-2017-MISSION

IRIS

BTS-SIO

Dans vos interfaces réseaux, il faut activer le mode « Radio » et définir son rôle afin que la borne soit active.

Cliquer sur « Enable » pour « Enable Radio », et son rôle en « Access Point » pour l’interface « Radio 2.4 GHz ».

HOME

EXPRESS SET-UP

EXPRESS SECURITY

NETWORK MAP

ASSOCIATION

NETWORK INTERFACES

IP Address

GigabitEthernet

Radio0-802.11N^{2.4GHz}

Radio1-802.11N^{5GHz}

SECURITY

SERVICES

WIRELESS SERVICES

SYSTEM SOFTWARE

RADIO0-802.11N^{2.4GHz}

STATUS

DETAILED STATUS

SETTINGS

Hostname ap

Network Interfaces: Radio0-802.11N^{2.4GHz} Settings

Operating Mode:

Mixed

Enable Radio:

☒ Enable

☐ Disable

Current Status (Software/Hardware):

Enabled

Up

Role in Radio Network:

☒ Access Point

☐ Access Point (Fallback to Radio Shutdown)

☐ Access Point (Fallback to Repeater)

☐ Repeater

Vérifier depuis la page d’accueil de l’interface graphique de votre borne que l’interface précédemment configurée soit bien active.

HOME

EXPRESS SET-UP

EXPRESS SECURITY

NETWORK MAP

ASSOCIATION

NETWORK INTERFACES

SECURITY

SERVICES

WIRELESS SERVICES

SYSTEM SOFTWARE

EVENT LOG

LOGOUT

Hostname ap

Home: Summary Status

Association

Clients: 0

Infrastructure clients: 0

Network Identity

IP Address

10.0.228.63

MAC Address

a44c.11d3.305f

Network Interfaces

Interface	MAC Address	Transmission Rate
↑ GigabitEthernet	a44c.11d3.305f	1000Mb/s
↑ Radio0-802.11N^{2.4GHz}	f47f.355e.5720	Mcs Index 15
↓ Radio1-802.11N^{5GHz}	f47f.3558.a000	Mcs Index 15

Conclusion	Que pouvez-vous dire de cette mission : apport personnel, expérience, etc
	Cette mission m’a appris à me servir des services « Certificats Active Directory » et « Serveur NPS » ; J’ai appris également ce qu’était le protocole RADIUS et à m’en servir pour obtenir un moyen d’authentification via borne WI-FI sécurisé.

Evolution possible <i>(facultatif)</i>	Evolution du service concerné par cette mission qui pourrait être envisagée

Productions associées	Liste des documents produits et description