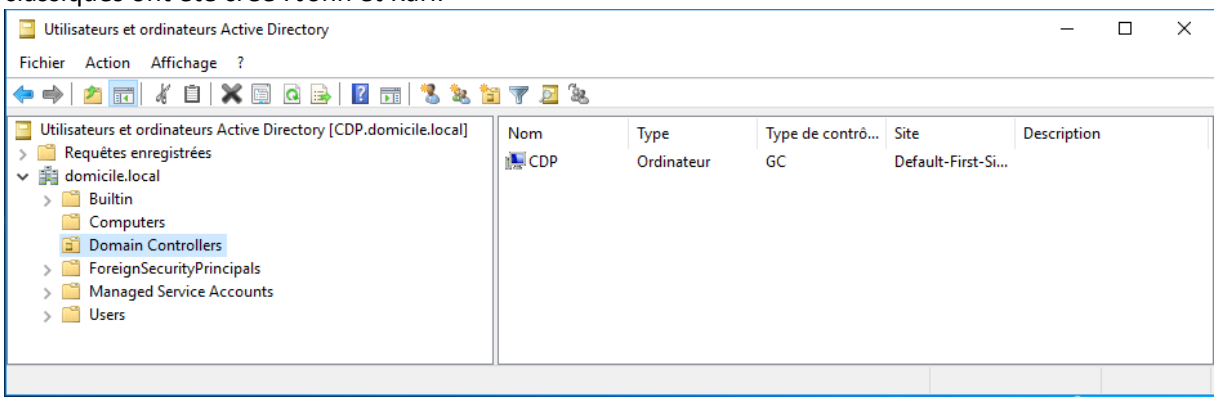
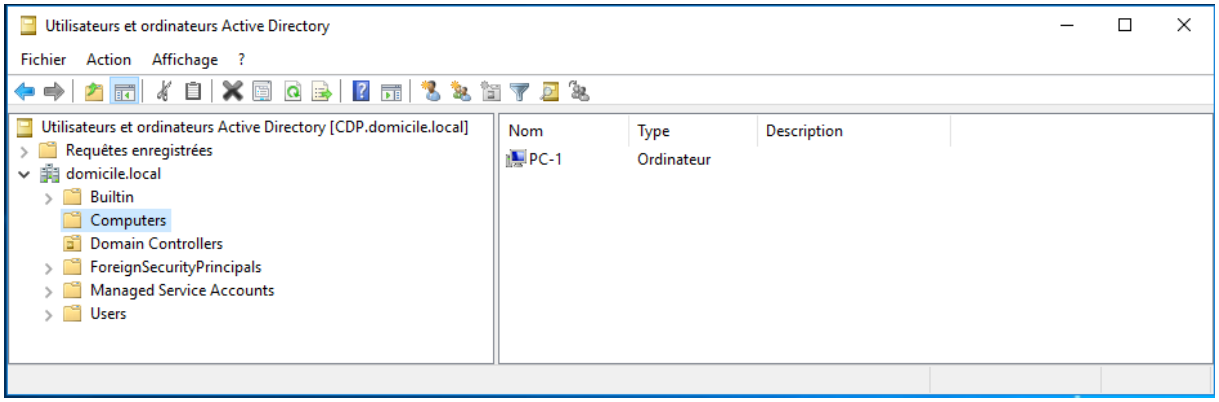
Logiciel : Yubico	**MISE EN ŒUVRE DE LA PKI WINDOWS/AD & YUBICO**	Version : 2016
Service : Informatique **! Doc en cours !**		Document initié le 01/09/2022 **! Doc en cours !**
Auteur : Claude SANTERO		Config. : Windows.

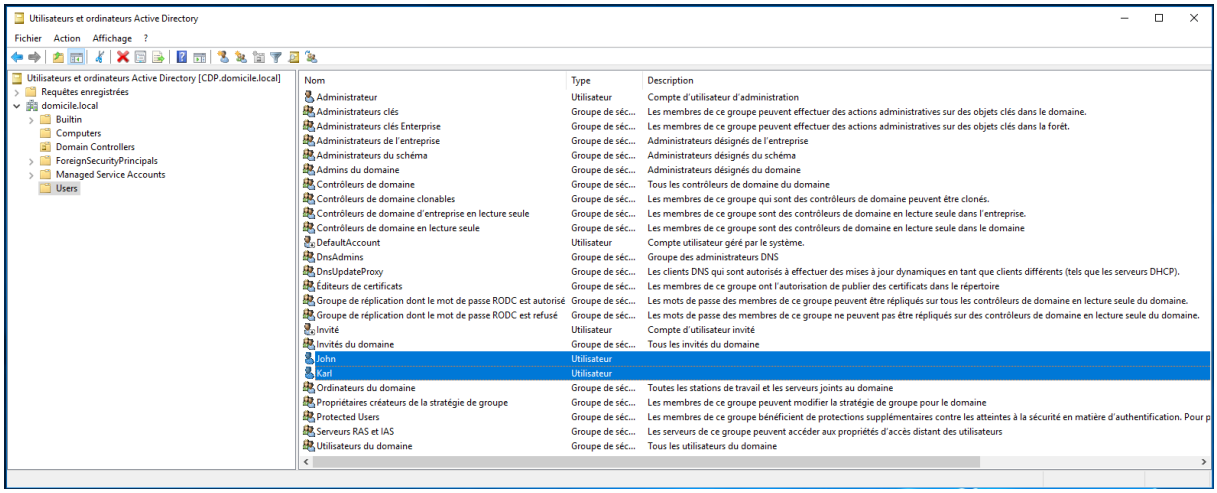
Configuration AD / Authentification Yubico :

1. Prérequis :

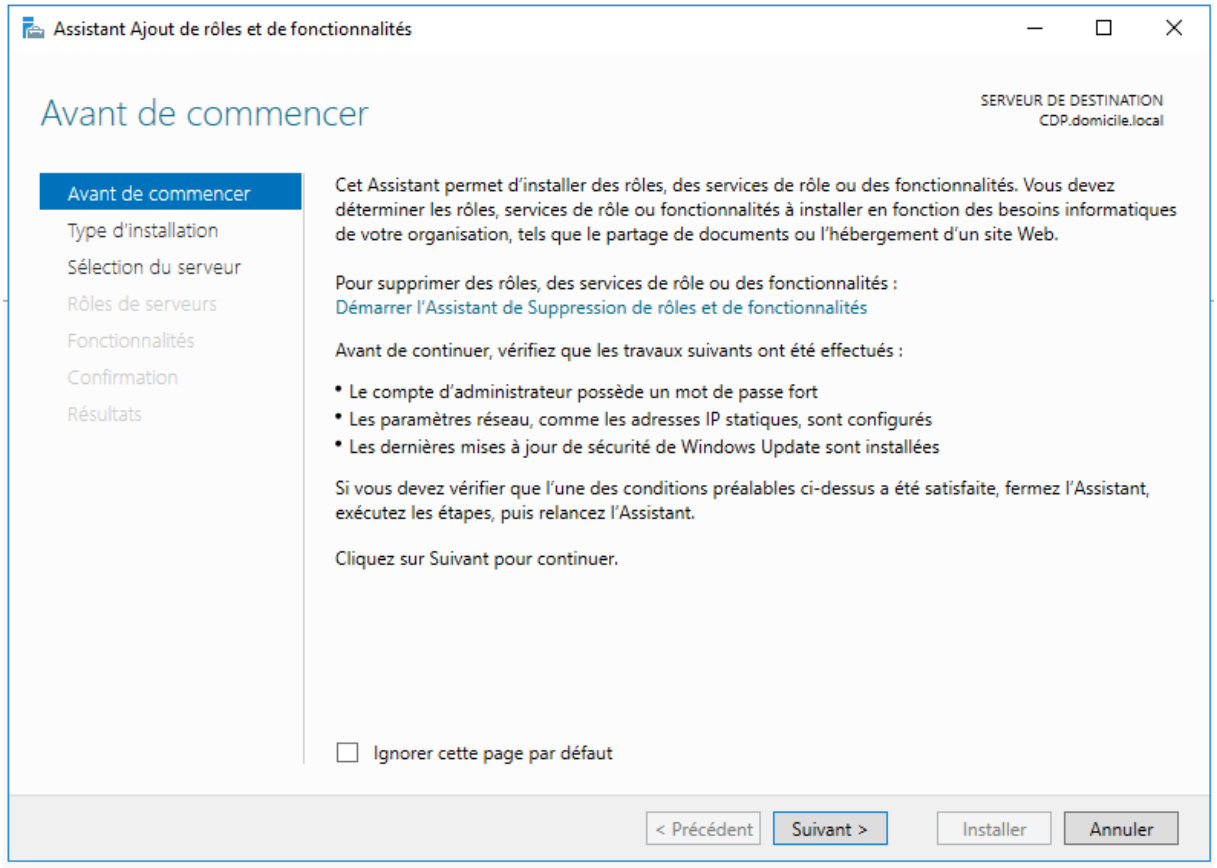
   Vous devez avoir installé un serveur Windows 2016 minimum avec les services Active Directory et DNS correctement configurés.
   Dans notre exemple nous avons créé un domaine baptisé domicile.local porté par un seul serveur nommé CDP. Un poste de travail est membre de ce serveur (PC-1) et deux utilisateurs classiques ont été créé : John et Karl.

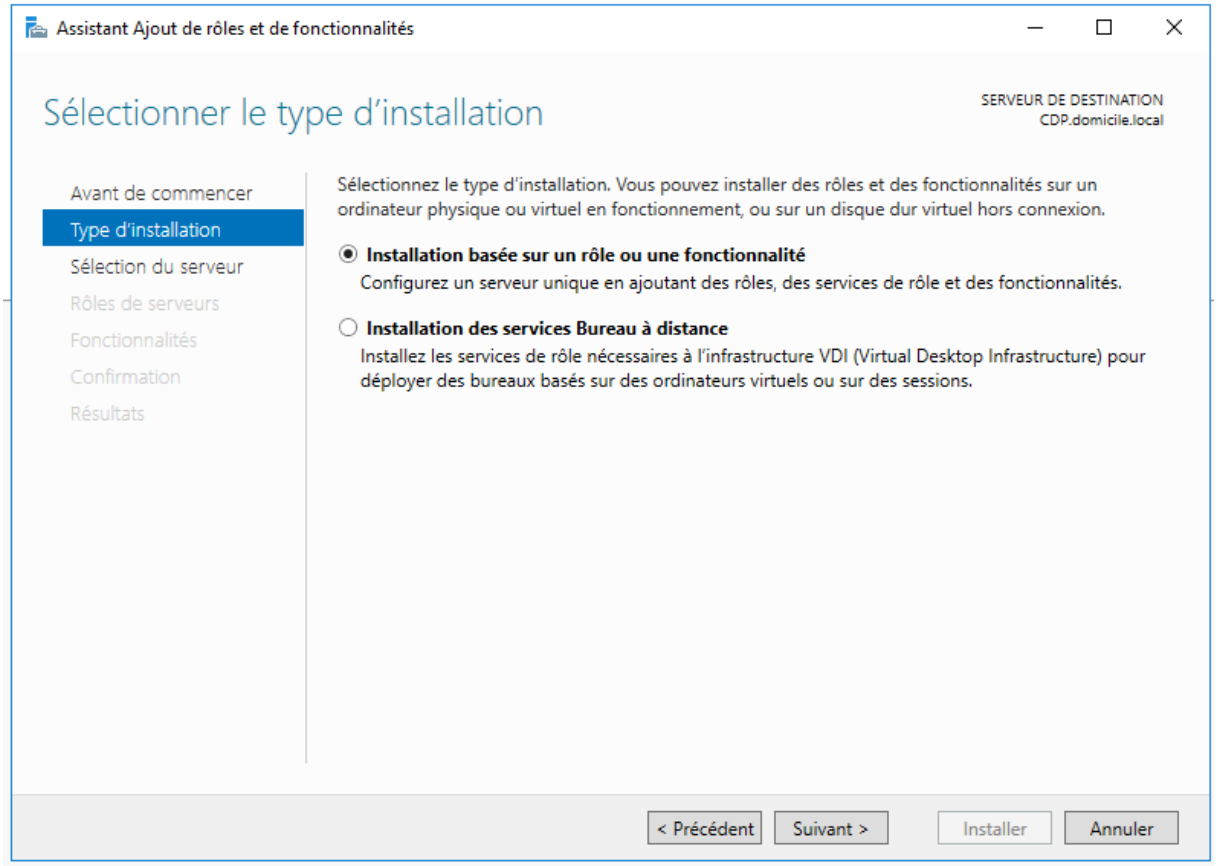


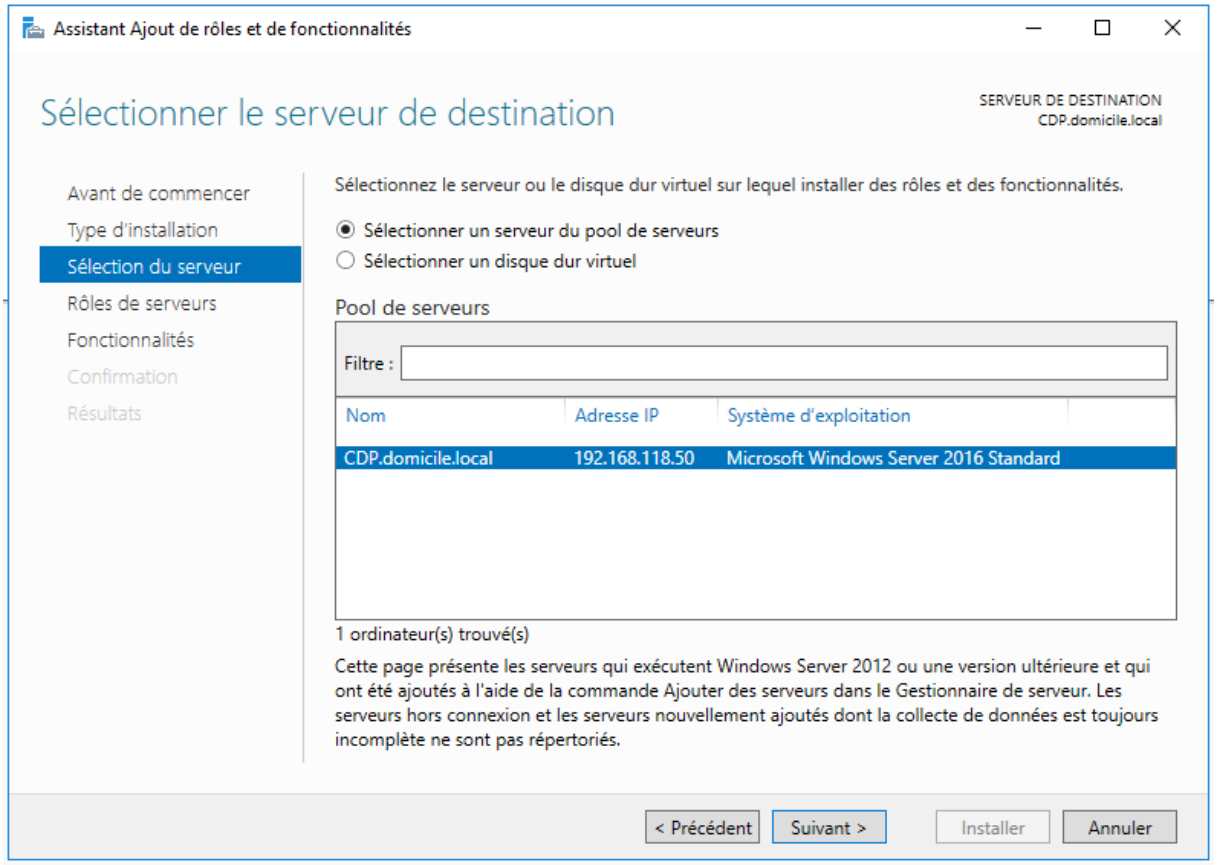


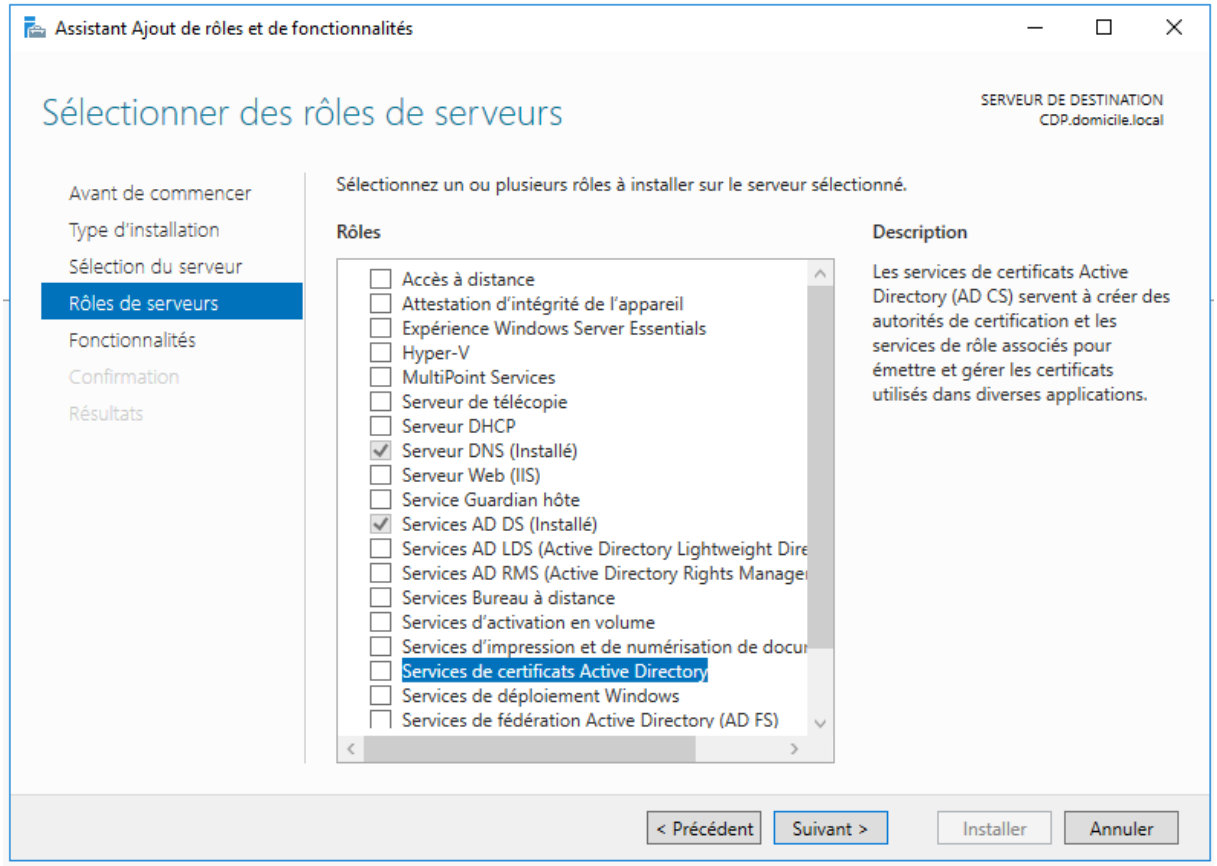


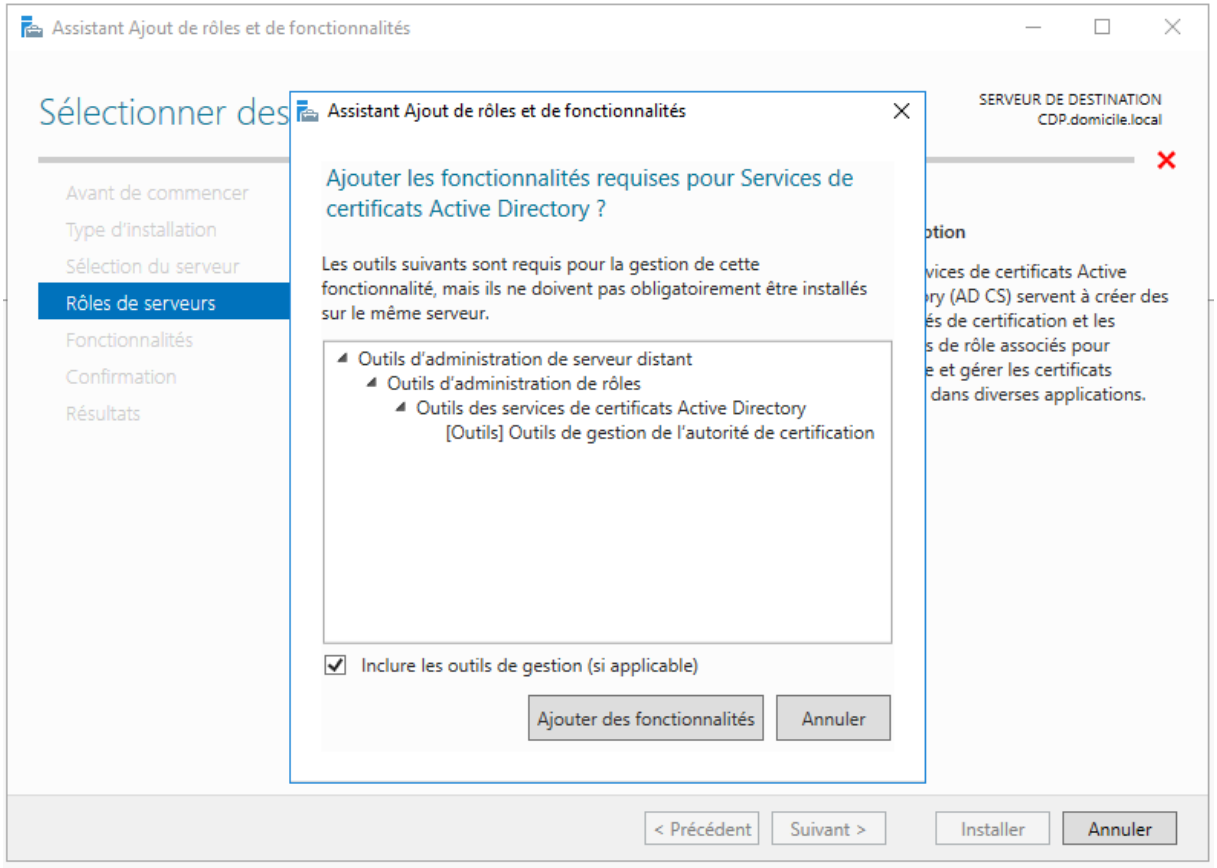
2. Installer le rôle de certificat AD :

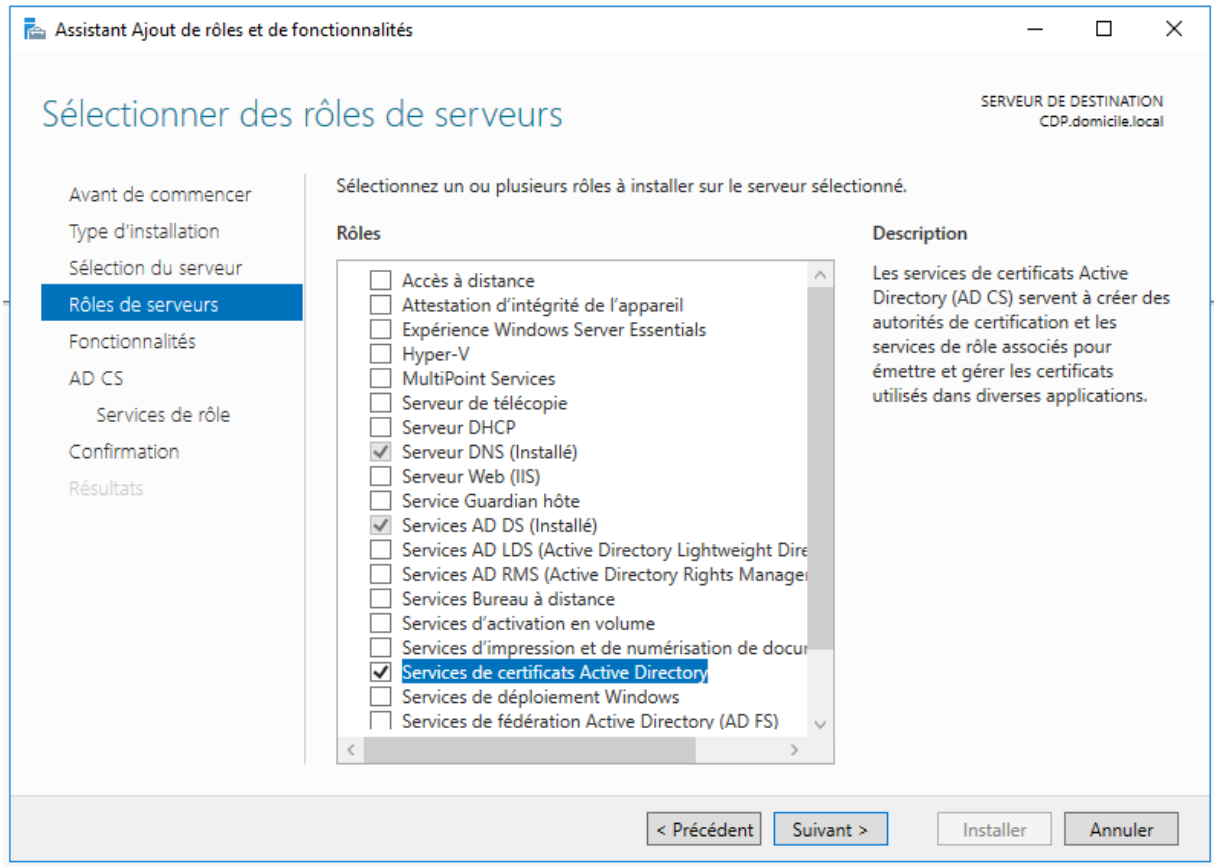


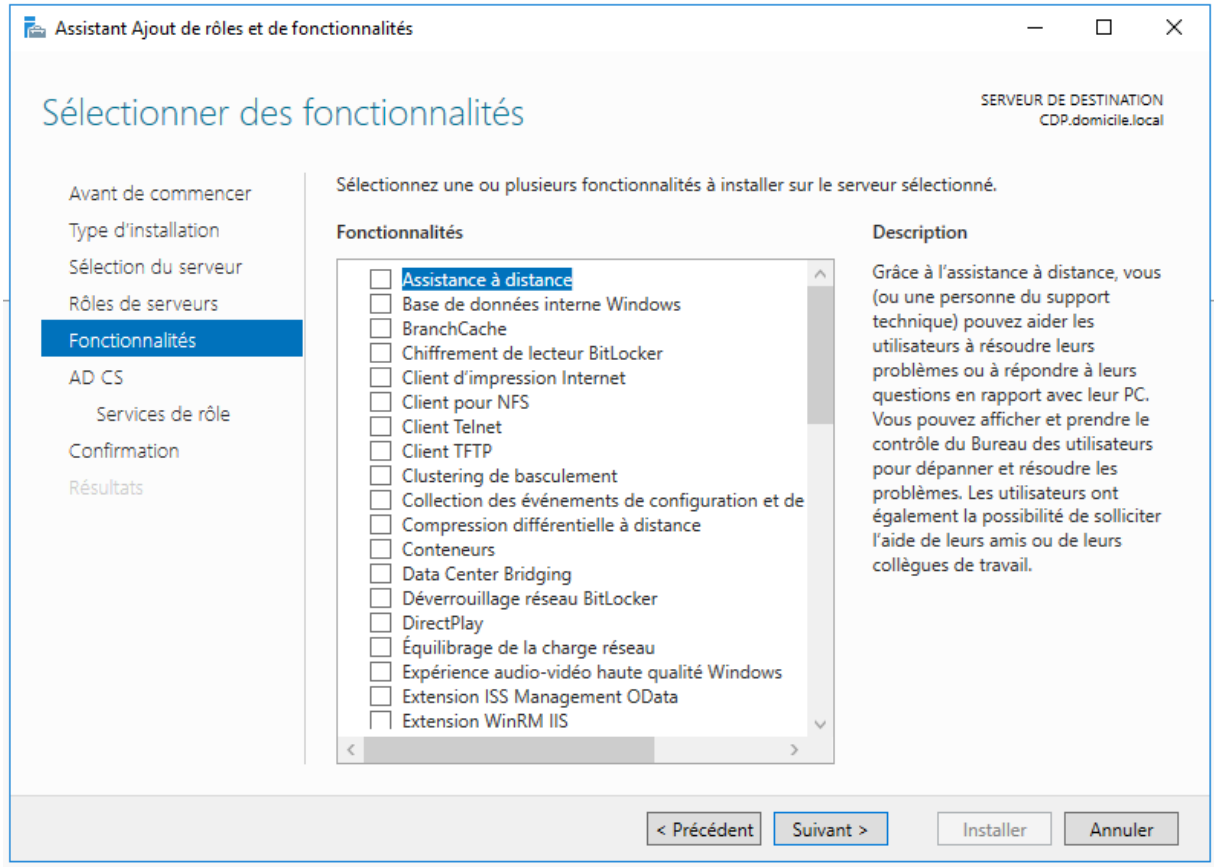


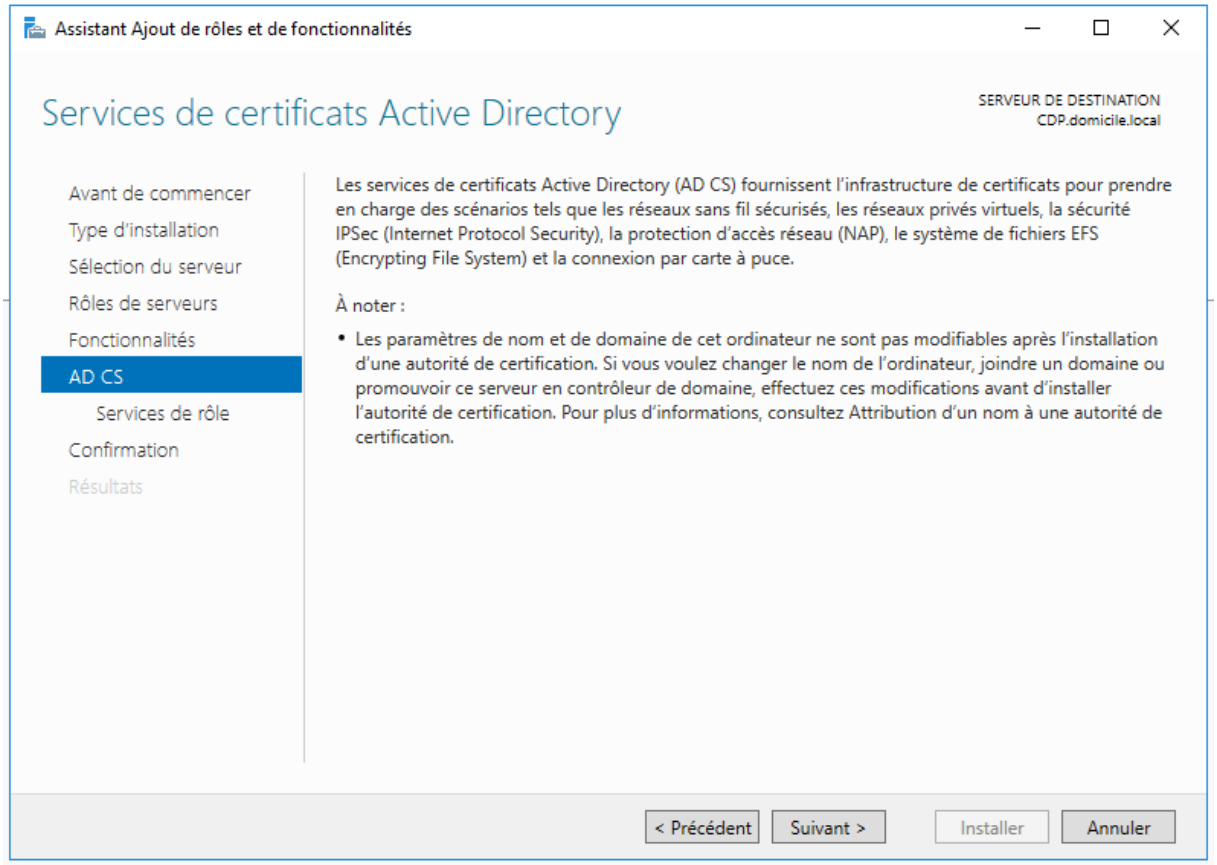

Assistant Ajout de rôles et de fonctionnalités
Sélectionner le serveur de destination
SERVEUR DE DESTINATION
CDP.domicile.local
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats
Sélectionnez le serveur ou le disque dur virtuel sur lequel 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
CDP.domicile.local
192.168.118.50
Microsoft Windows Server 2016 Standard
1 ordinateur(s) trouvé(s)
Cette page présente les serveurs qui exécutent Windows Server 2012 ou une version ultérieure et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors connexion et les serveurs nouvellement ajoutés dont la collecte de données est toujours incomplète ne sont pas répertoriés.
< Précédent
Suivant >
Installer
Annuler

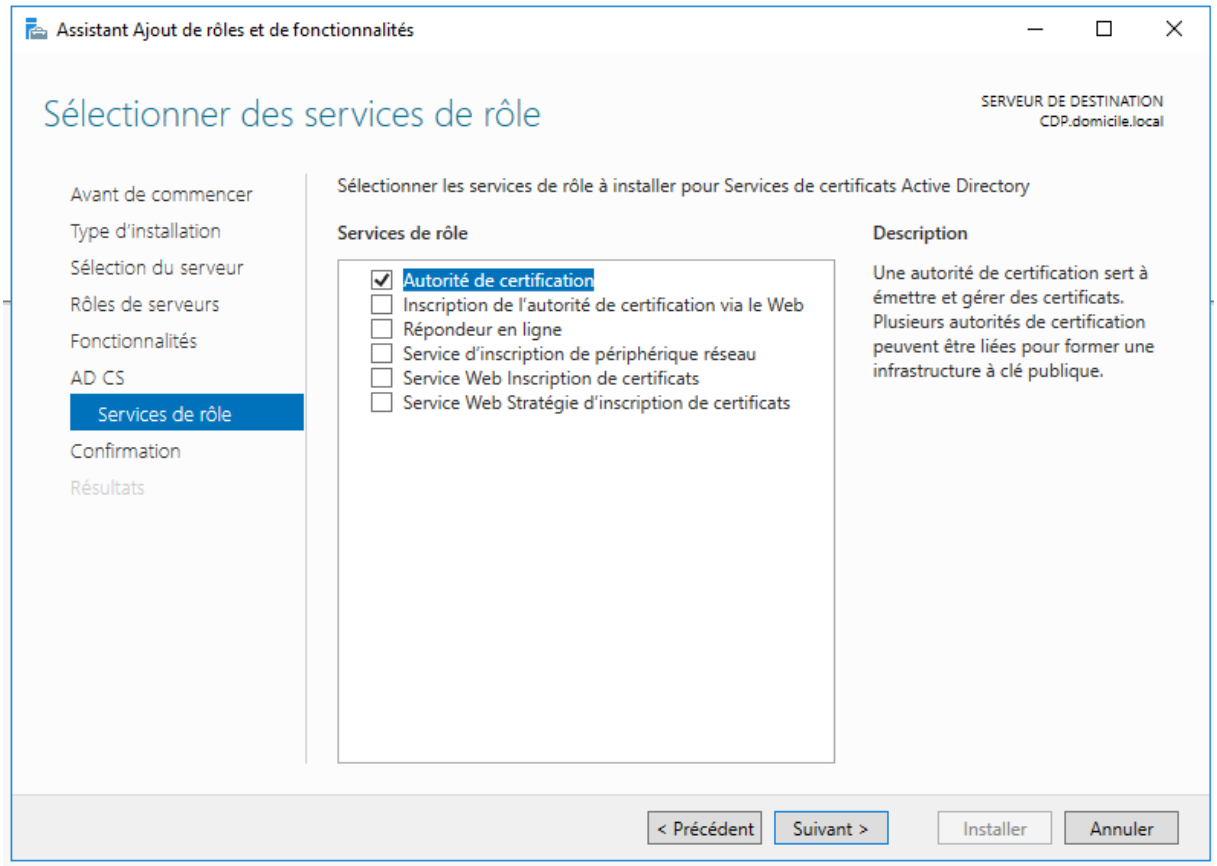

Assistant Ajout de rôles et de fonctionnalités
Sélectionner des rôles de serveurs
SERVEUR DE DESTINATION
CDP.domicile.local
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats
Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.
Rôles
Description
Accès à distance
Attestation d'intégrité de l'appareil
Expérience Windows Server Essentials
Hyper-V
MultiPoint Services
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 déploiement Windows
Services de fédération Active Directory (AD FS)
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

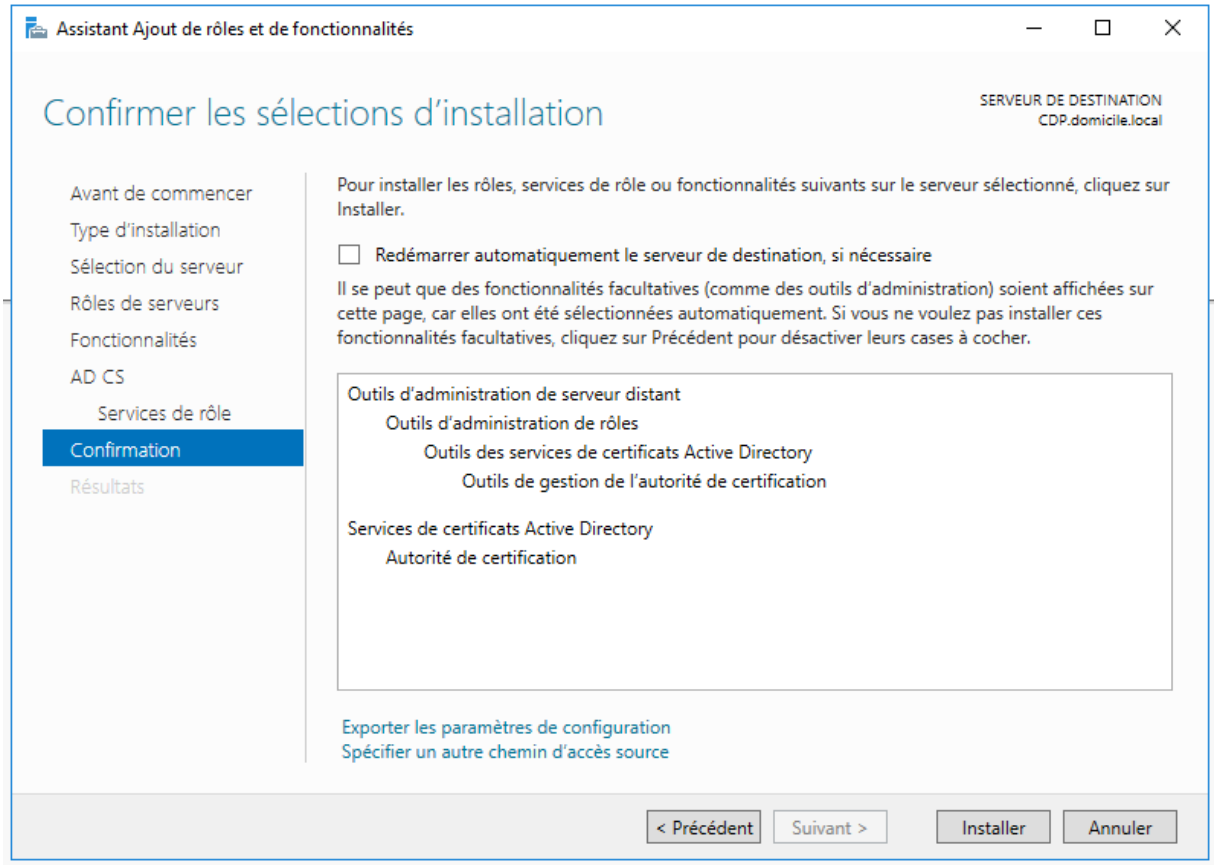

Assistant Ajout de rôles et de fonctionnalités
Sélectionner des
SERVEUR DE DESTINATION
CDP.domicile.local
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats
Assistant Ajout de rôles et de fonctionnalités
Ajouter les fonctionnalités requises pour Services 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
< Précédent
Suivant >
Installer
Annuler

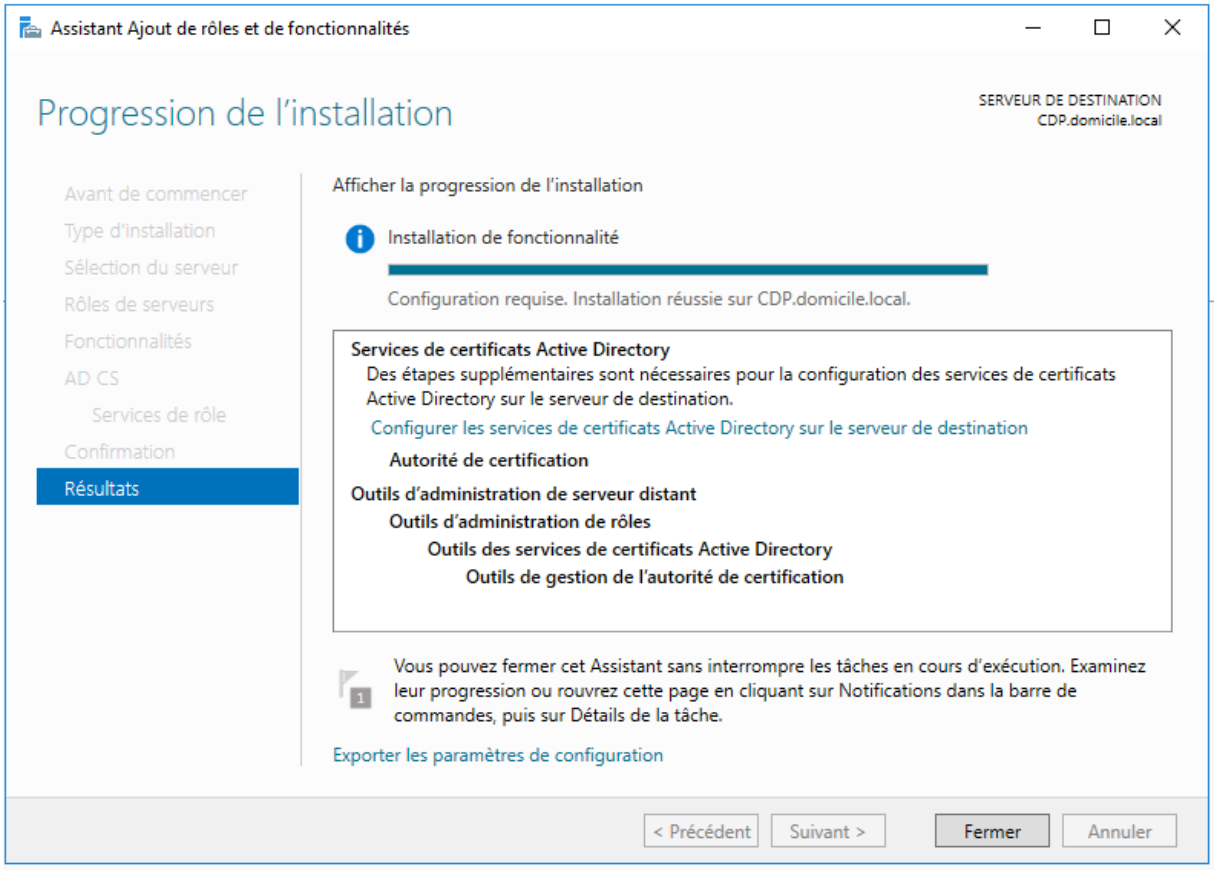

Assistant Ajout de rôles et de fonctionnalités
Sélectionner des rôles de serveurs
SERVEUR DE DESTINATION
CDP.domicile.local
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
AD CS
Services de rôle
Confirmation
Résultats
Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.
Rôles
Accès à distance
Attestation d'intégrité de l'appareil
Expérience Windows Server Essentials
Hyper-V
MultiPoint Services
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 déploiement Windows
Services de fédération Active Directory (AD FS)
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
Sélectionner des fonctionnalités
SERVEUR DE DESTINATION
CDP.domicile.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
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
Équilibrage de la charge réseau
Expérience audio-vidéo haute qualité Windows
Extension ISS Management OData
Extension WinRM IIS
Description
Grâce à l'assistance à distance, vous (ou une personne du support technique) pouvez aider les utilisateurs à résoudre leurs problèmes ou à répondre à leurs questions en rapport avec leur PC. Vous pouvez afficher et prendre le contrôle du Bureau des utilisateurs pour dépanner et résoudre les problèmes. Les utilisateurs ont également la possibilité de solliciter l'aide de leurs amis ou de leurs collègues de travail.
< Précédent
Suivant >
Installer
Annuler


Assistant Ajout de rôles et de fonctionnalités
Services de certificats Active Directory
SERVEUR DE DESTINATION
CDP.domicile.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.
< Précédent
Suivant >
Installer
Annuler

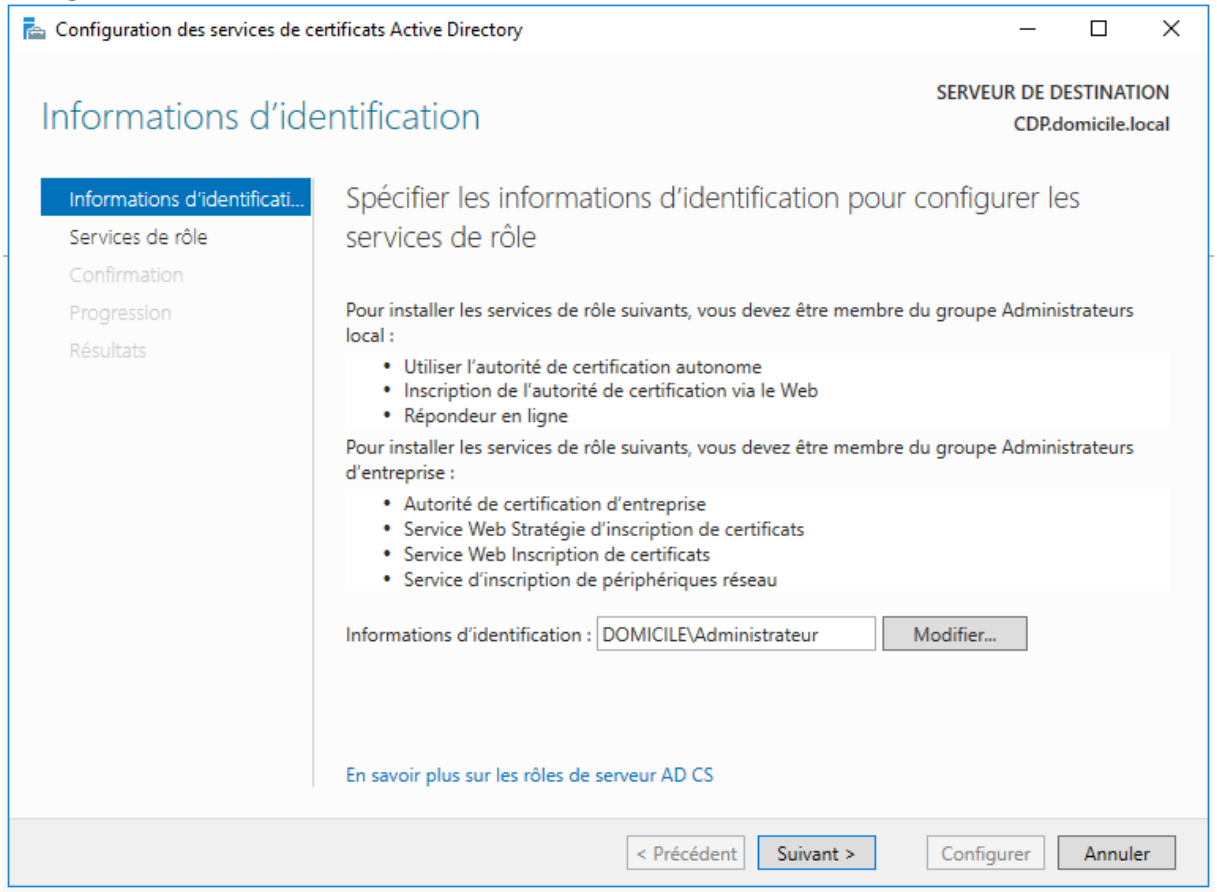

Assistant Ajout de rôles et de fonctionnalités
Sélectionner des services de rôle
SERVEUR DE DESTINATION
CDP.domicile.local
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
AD CS
Services de rôle
Confirmation
Résultats
Sélectionner les services de rôle à installer 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.
< Précédent
Suivant >
Installer
Annuler

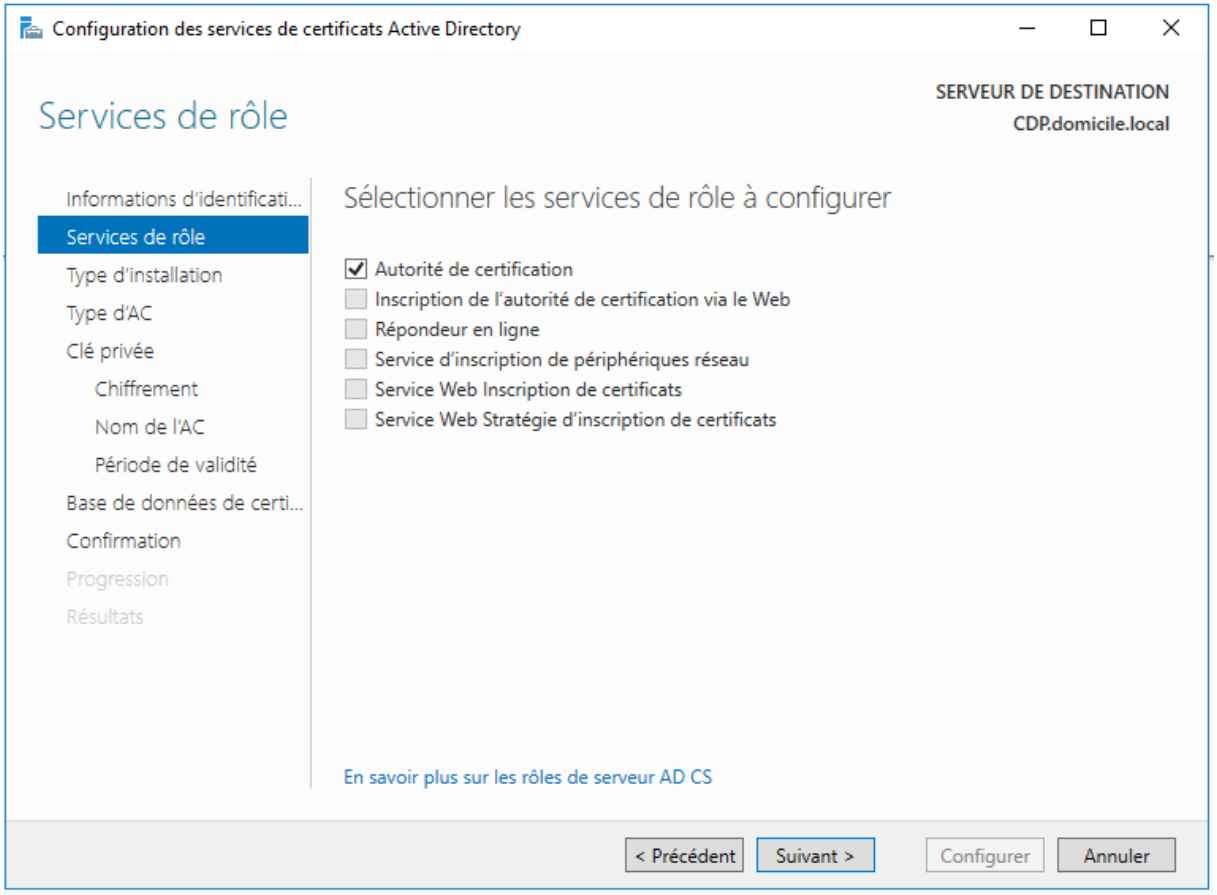

Assistant Ajout de rôles et de fonctionnalités
Confirmer les sélections d'installation
SERVEUR DE DESTINATION
CDP.domicile.local
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
AD CS
Services de rôle
Confirmation
Résultats
Pour installer les rôles, services 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.
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
Services de certificats Active Directory
Autorité de certification
Exporter les paramètres de configuration
Spécifier un autre chemin d'accès source
< Précédent
Suivant >
Installer
Annuler

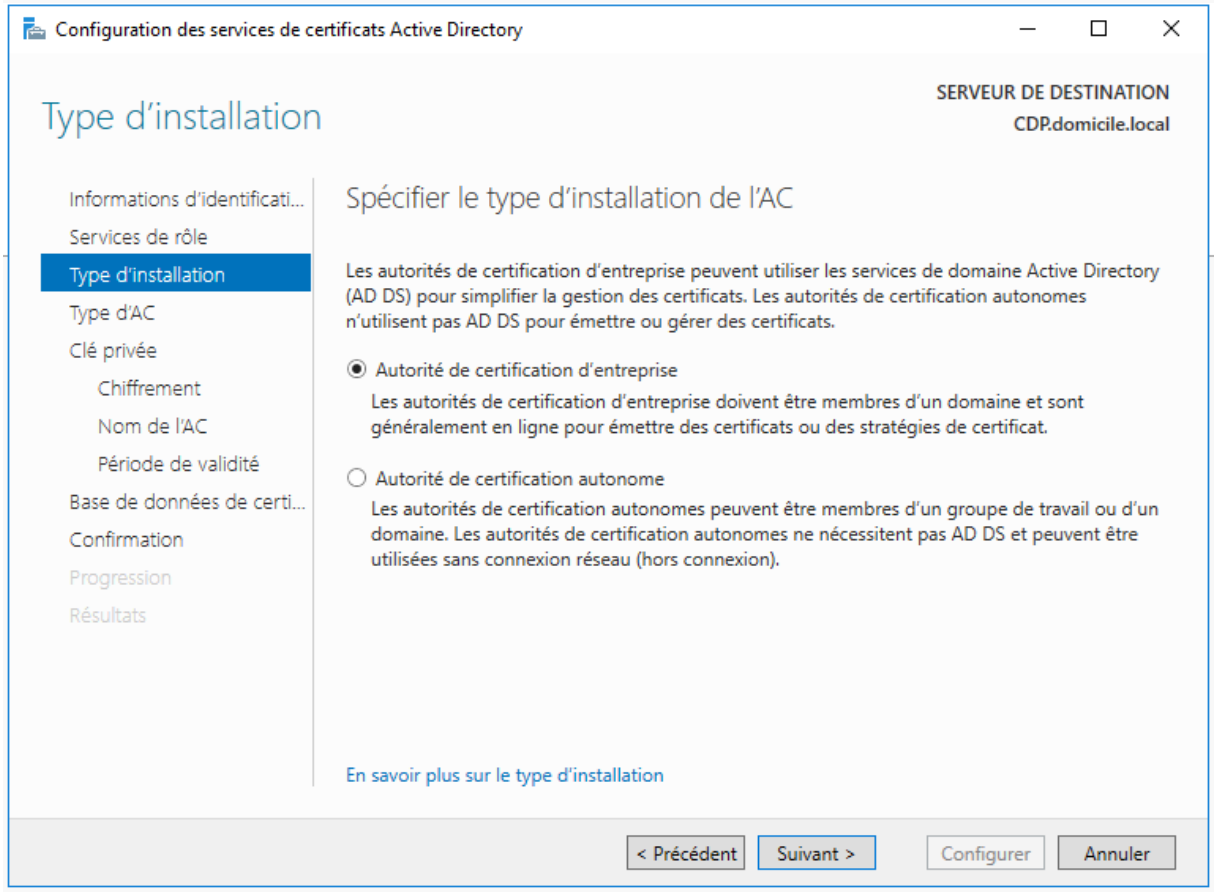


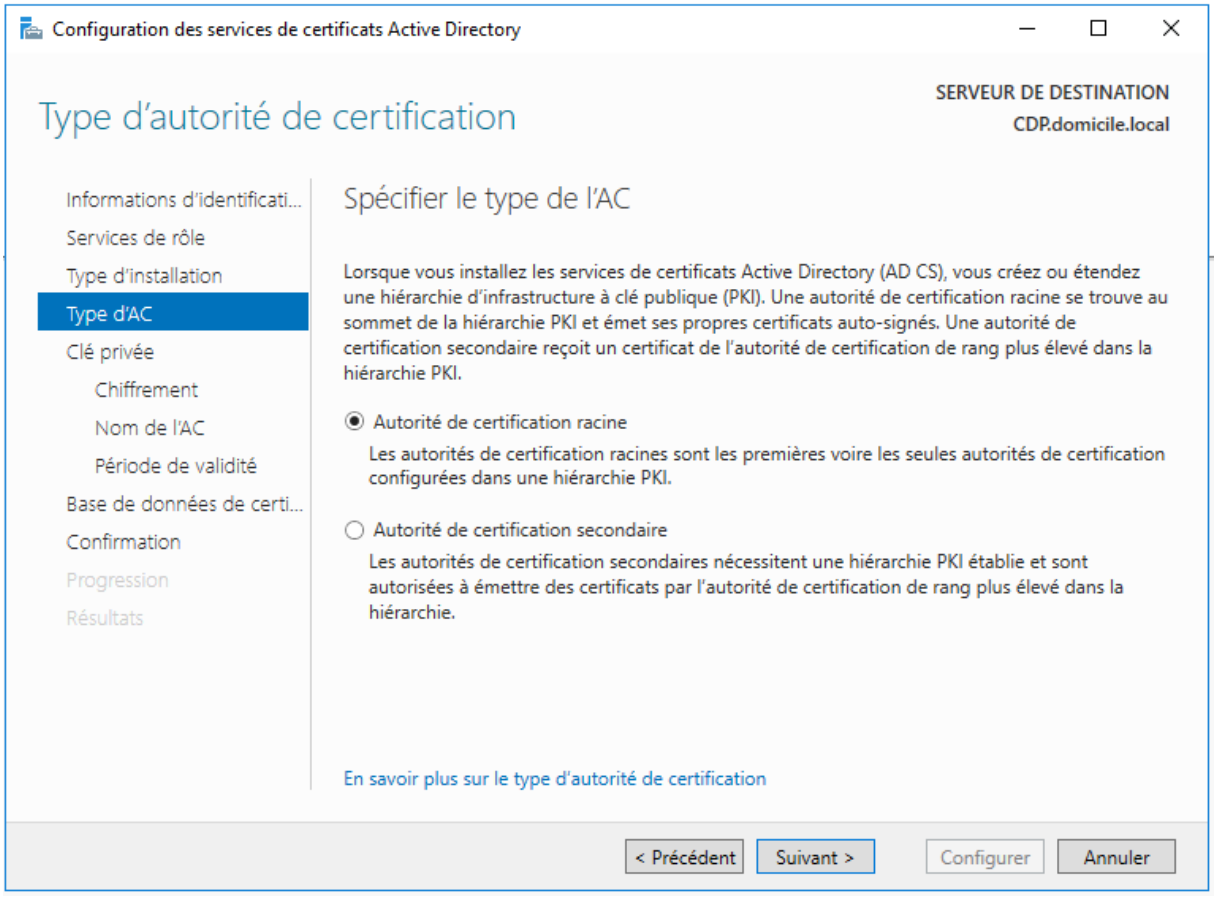
Cliquer sur « Configurer les services de certificats Active Directory sur le serveur de destination ».

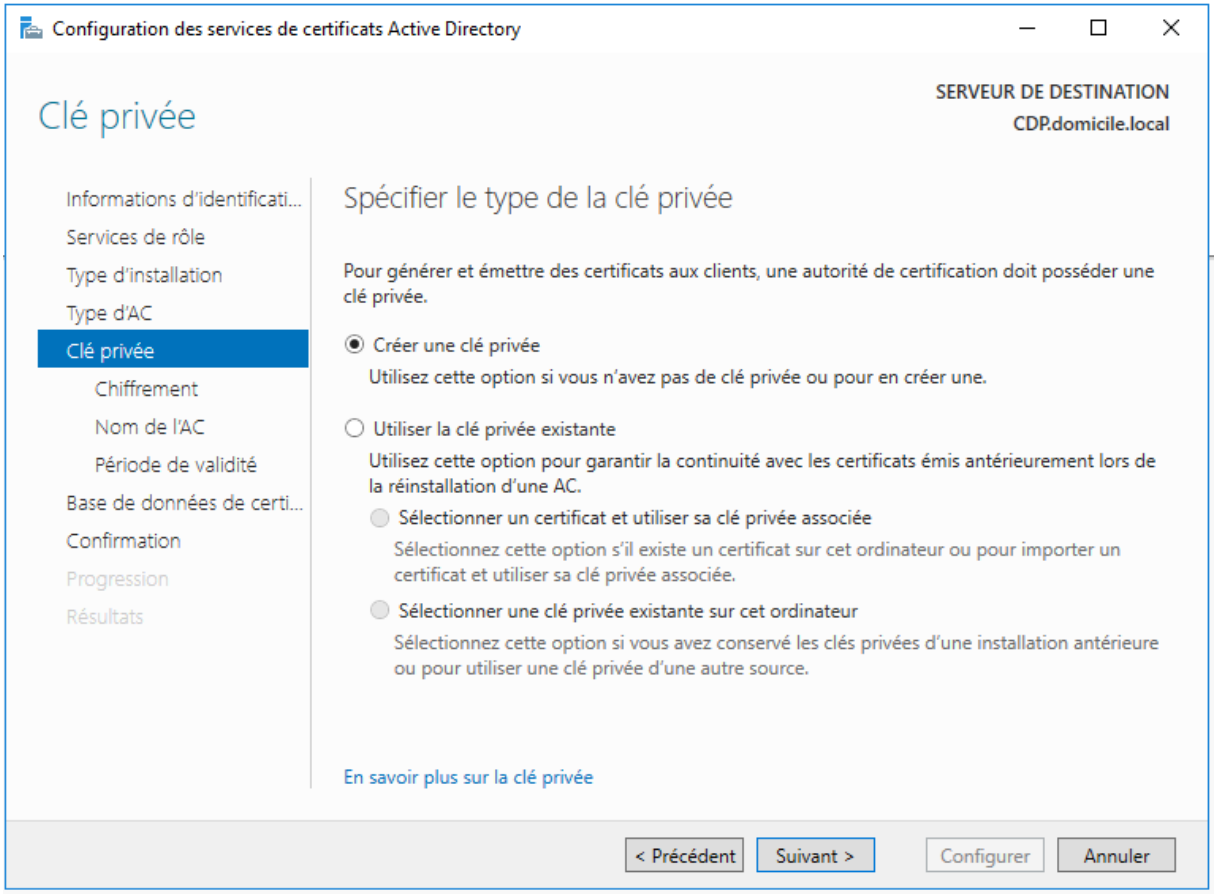
3. Configurer le service de Certificats :

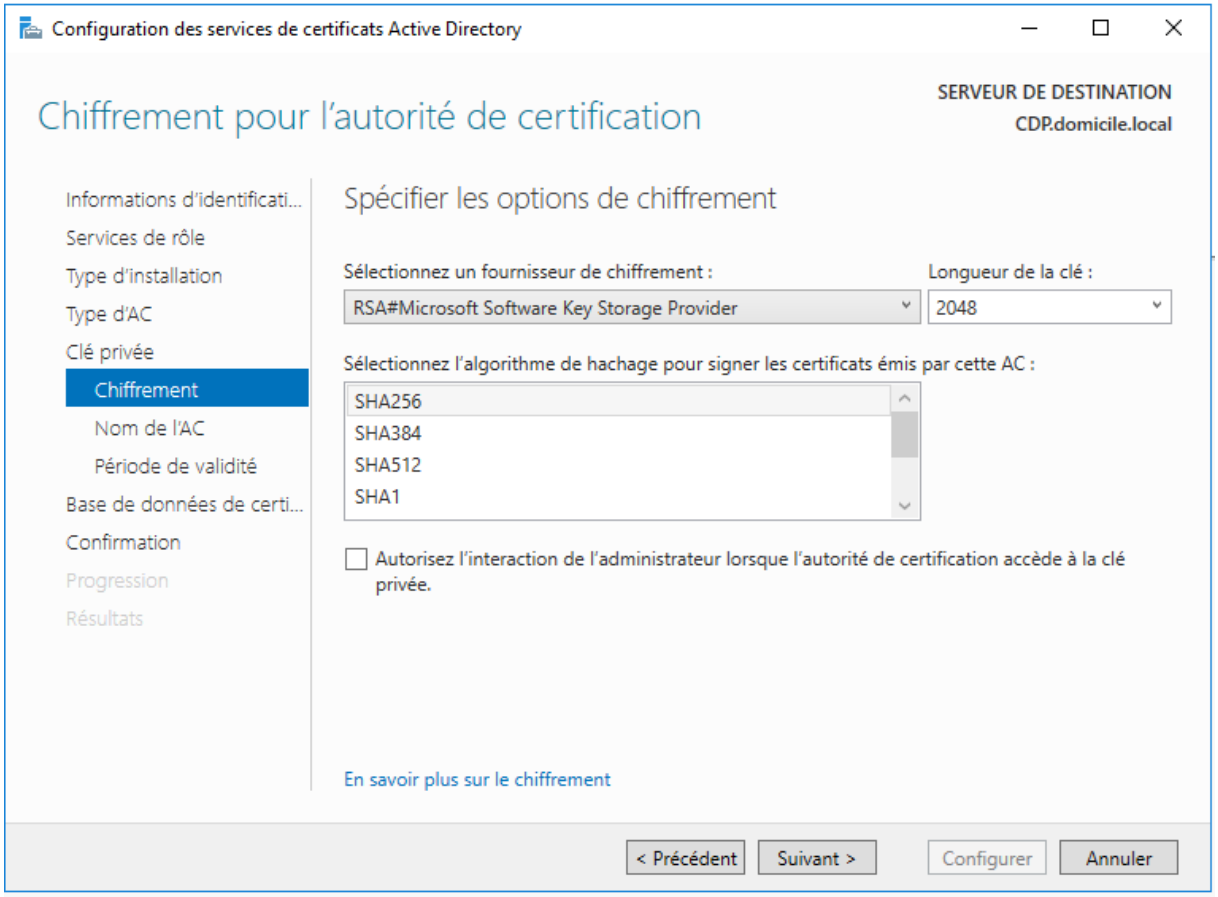


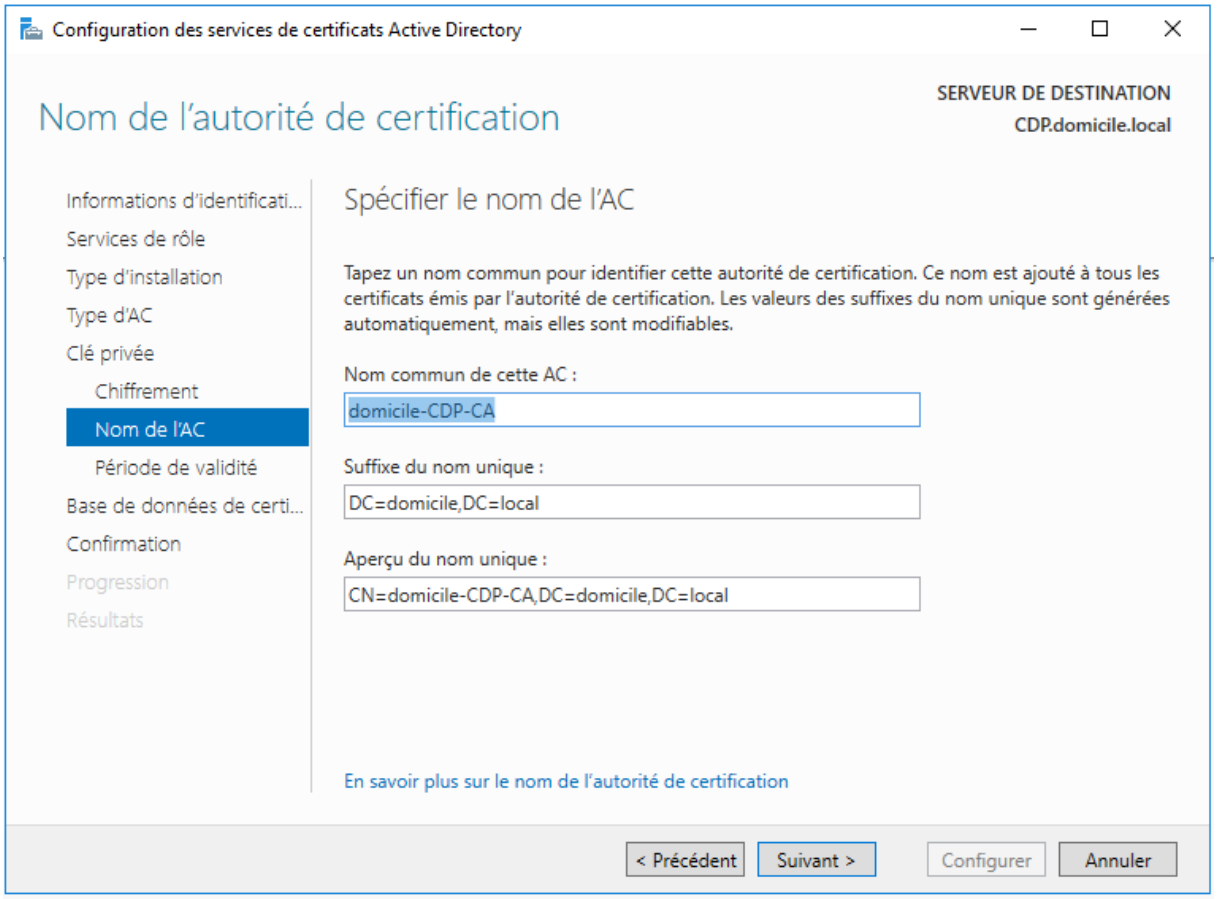

Configuration des services de certificats Active Directory
Services de rôle
SERVEUR DE DESTINATION
CDP.domicile.local
Informations d'identificati...
Services de rôle
Type d'installation
Type d'AC
Clé privée
Chiffrement
Nom de l'AC
Période de validité
Base de données de certi...
Confirmation
Progression
Résultats
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
CDP.domicile.local
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

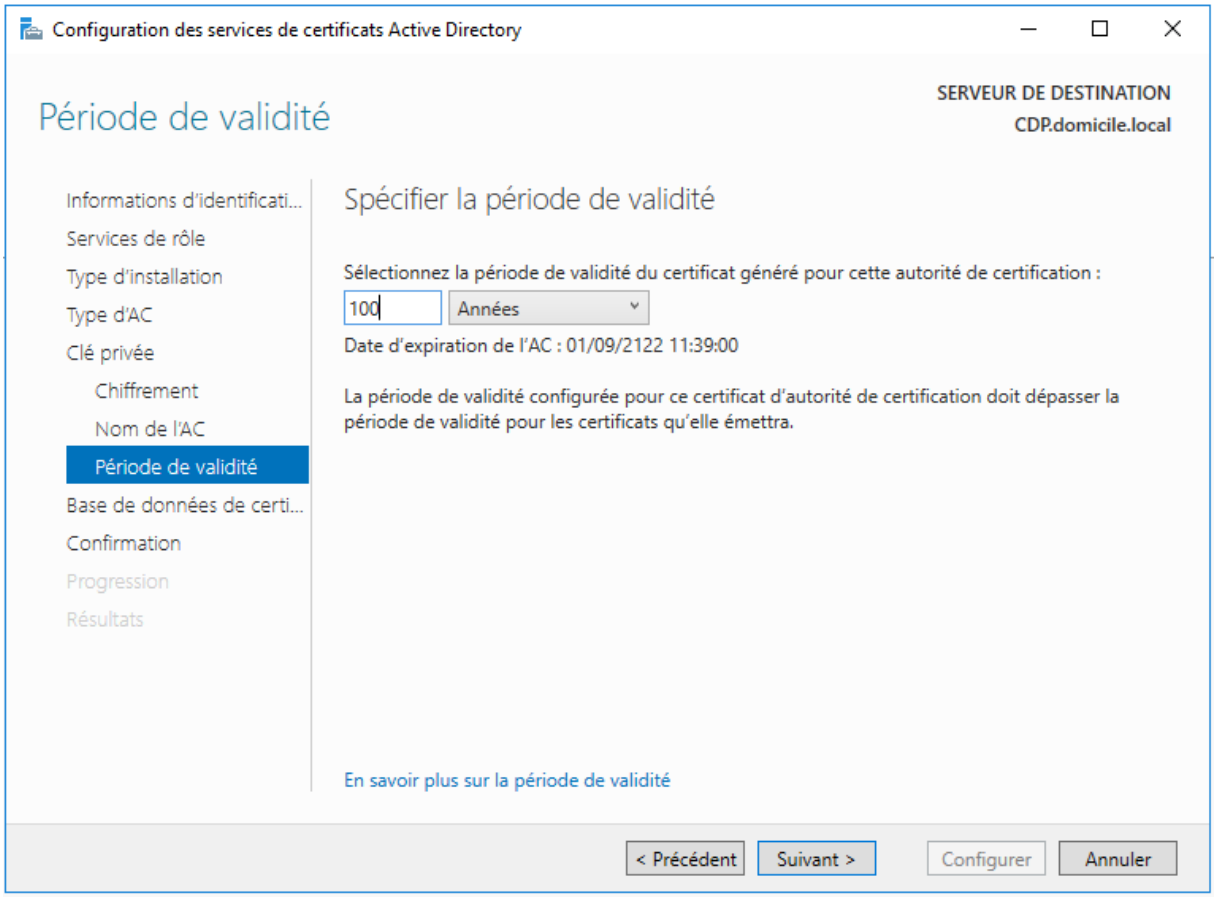

Configuration des services de certificats Active Directory
Type d'autorité de certification
SERVEUR DE DESTINATION
CDP.domicile.local
Informations d'identificati...
Services de rôle
Type d'installation
Type d'AC
Clé privée
Chiffrement
Nom de l'AC
Période de validité
Base de données de certi...
Confirmation
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

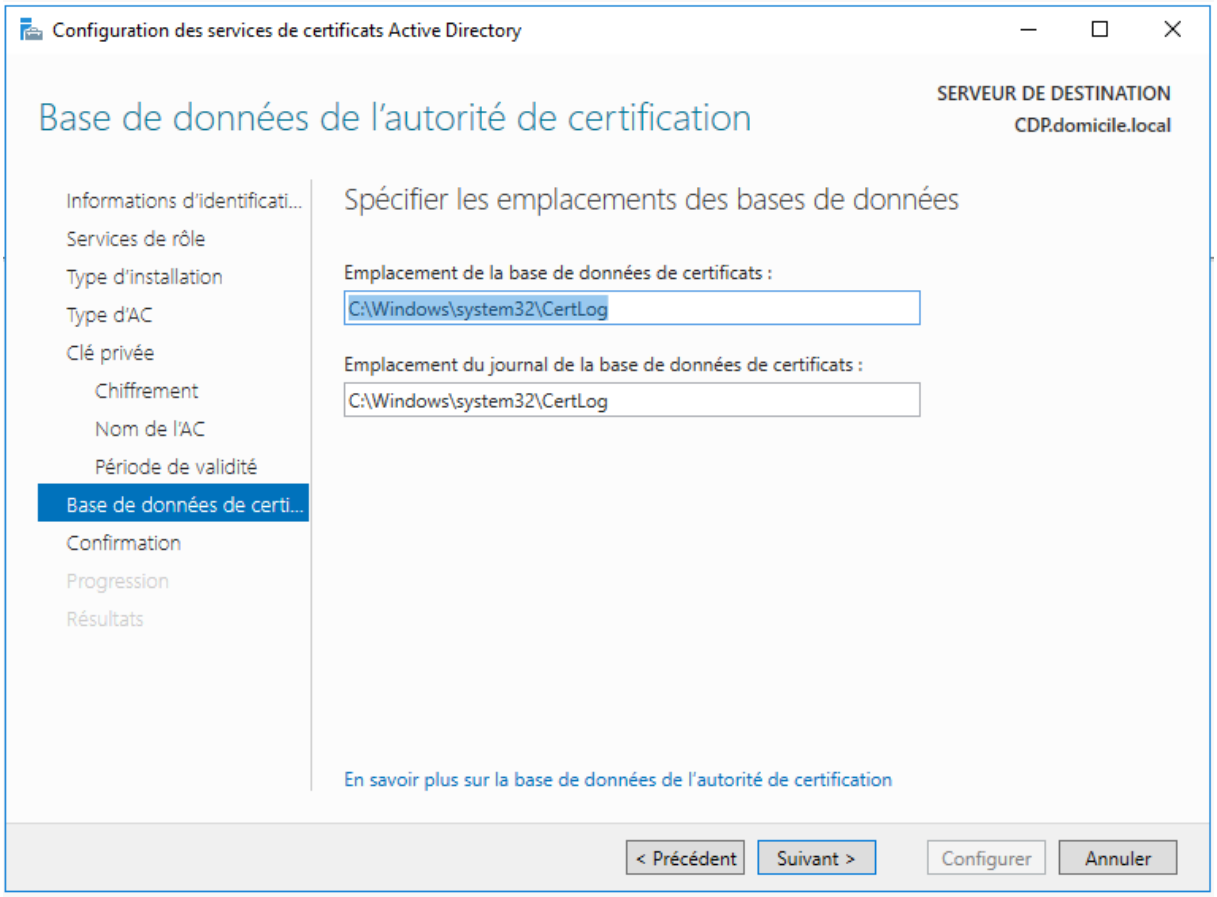

Configuration des services de certificats Active Directory
Clé privée
SERVEUR DE DESTINATION
CDP.domicile.local
Informations d'identificati...
Services de rôle
Type d'installation
Type d'AC
Clé privée
Chiffrement
Nom de l'AC
Période de validité
Base de données de certi...
Confirmation
Progression
Résultats
Spécifier le type de 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

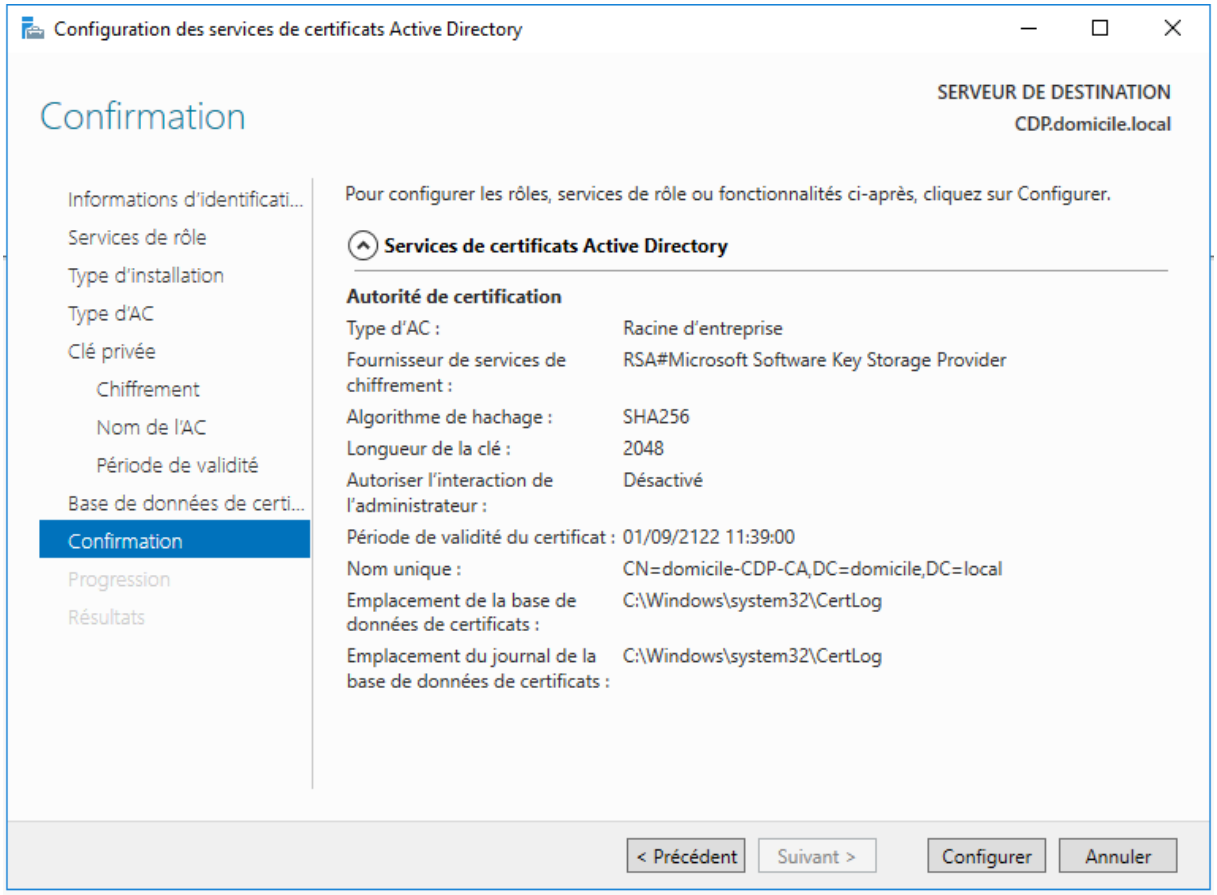

Configuration des services de certificats Active Directory
Chiffrement pour l'autorité de certification
SERVEUR DE DESTINATION
CDP.domicile.local
Informations d'identificati...
Services de rôle
Type d'installation
Type d'AC
Clé privée
Chiffrement
Nom de l'AC
Période de validité
Base de données de certi...
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

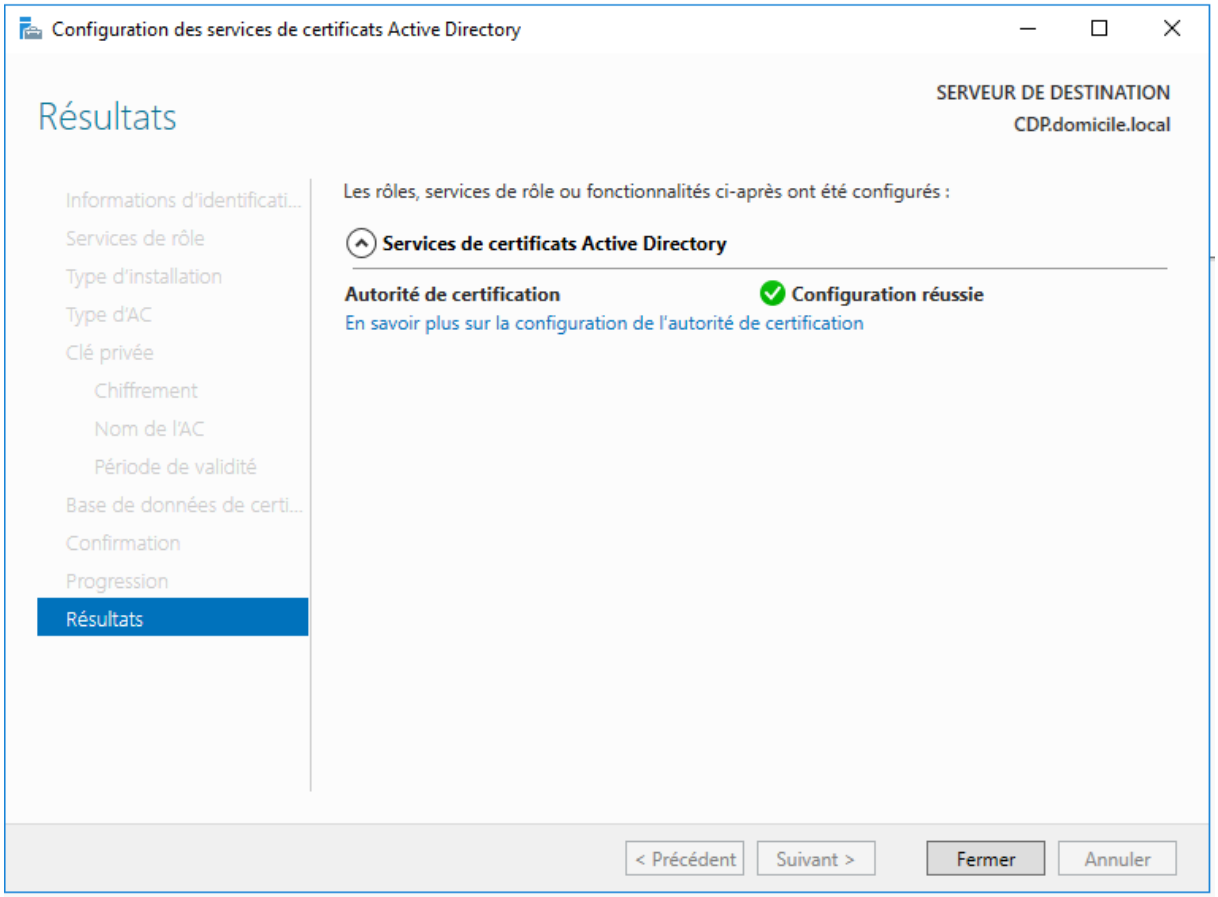


Défaut 5 Ans, pour ne pas avoir à le renouveler choisir 100 Ans :

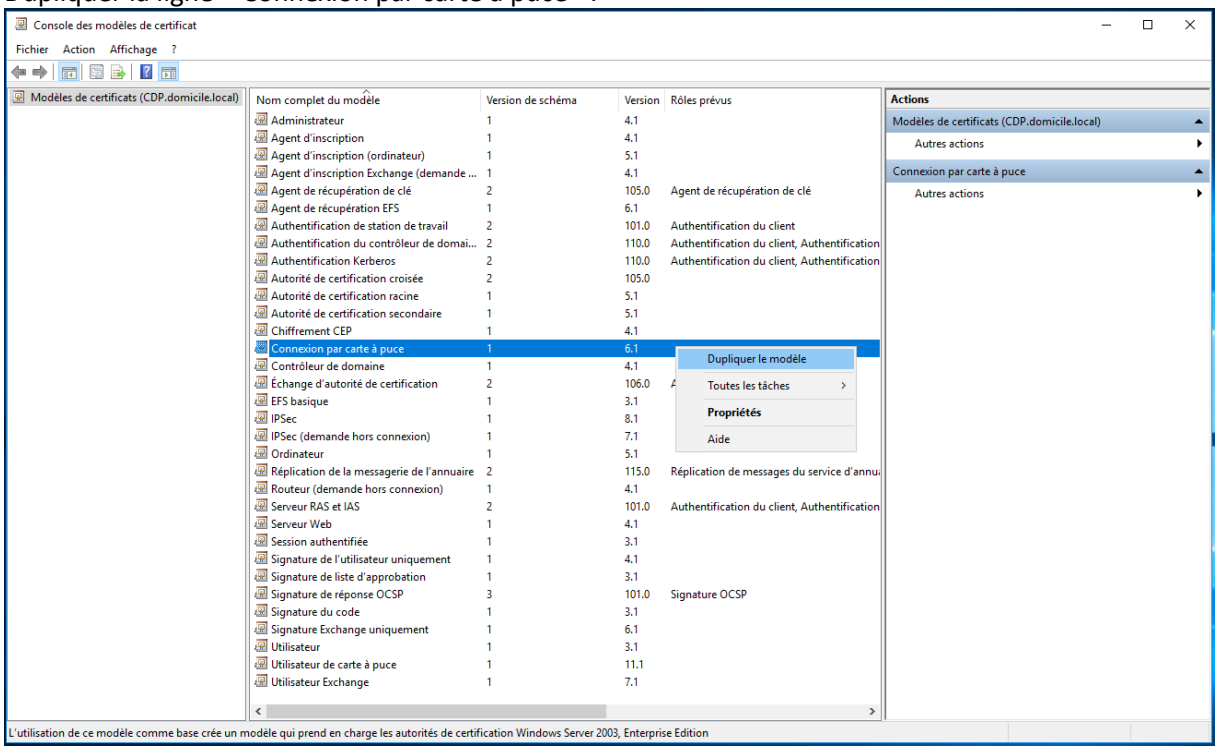

Configuration des services de certificats Active Directory
Période de validité
SERVEUR DE DESTINATION
CDP.domicile.local
Informations d'identificati...
Services de rôle
Type d'installation
Type d'AC
Clé privée
Chiffrement
Nom de l'AC
Période de validité
Base de données de certi...
Confirmation
Progression
Résultats
Spécifier la période de validité
Sélectionnez la période de validité du certificat généré pour cette autorité de certification :
100
Années
Date d'expiration de l'AC : 01/09/2122 11:39:00
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
CDP.domicile.local
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

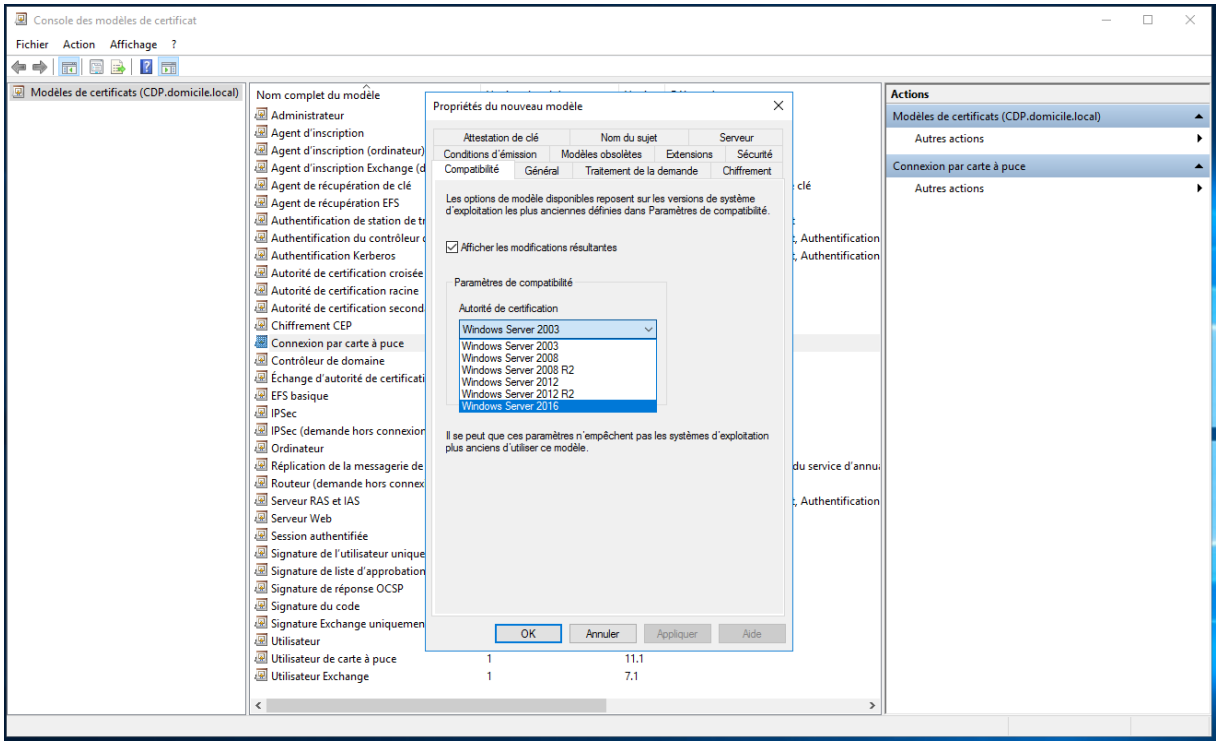

Configuration des services de certificats Active Directory
Confirmation
SERVEUR DE DESTINATION
CDP.domicile.local
Informations d'identificati...
Services de rôle
Type d'installation
Type d'AC
Clé privée
Chiffrement
Nom de l'AC
Période de validité
Base de données de certi...
Confirmation
Progression
Résultats
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 : SHA256
Longueur de la clé : 2048
Autoriser l'interaction de l'administrateur : Désactivé
Période de validité du certificat : 01/09/2122 11:39:00
Nom unique : CN=domicile-CDP-CA,DC=domicile,DC=local
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

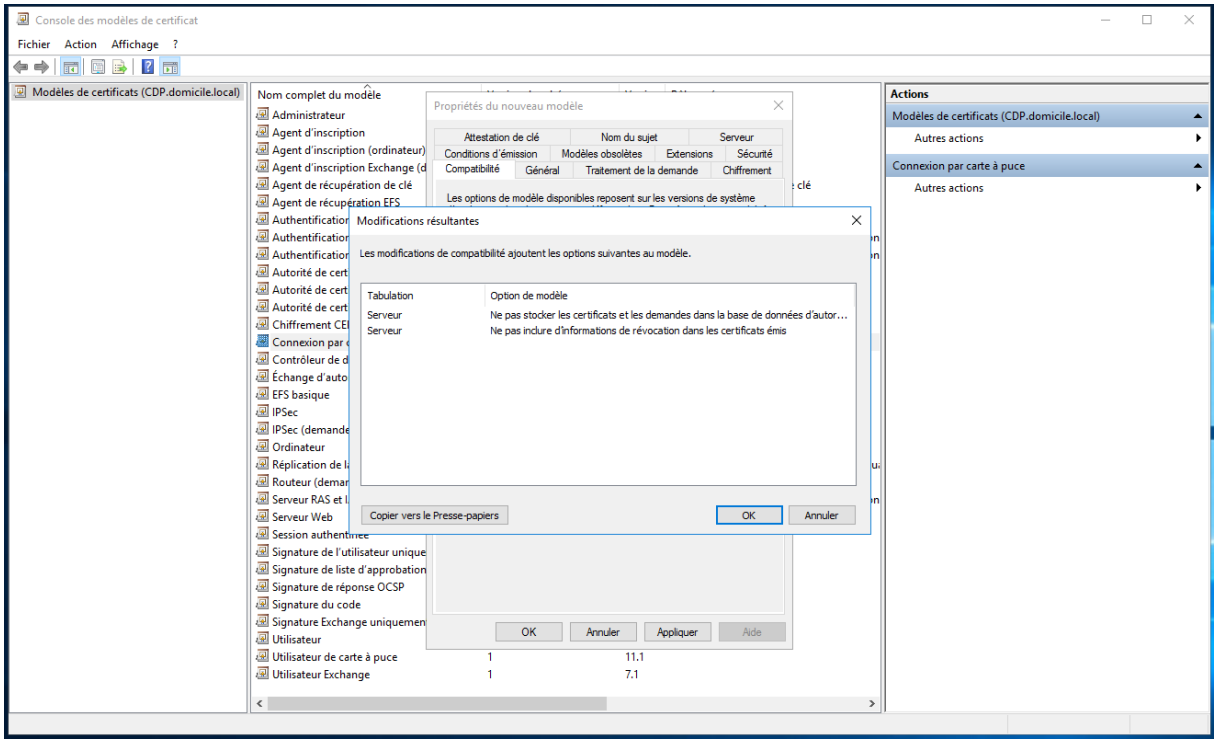

Configuration des services de certificats Active Directory
Résultats
SERVEUR DE DESTINATION
CDP.domicile.local
Informations d'identificati...
Services de rôle
Type d'installation
Type d'AC
Clé privée
Chiffrement
Nom de l'AC
Période de validité
Base de données de certi...
Confirmation
Progression
Résultats
Les rôles, services de rôle ou fonctionnalités ci-après ont été configurés :
Services de certificats Active Directory
Autorité de certification
Configuration réussie
En savoir plus sur la configuration de l'autorité de certification
< Précédent
Suivant >
Fermer
Annuler

4. Ajouter un nouveau modèle de certificat pour notre clef :
   Cliquer sur « Démarrer / Exécuter » et saisir le commande « certtmpl.msc ».
   Dupliquer la ligne « Connexion par carte à puce ».

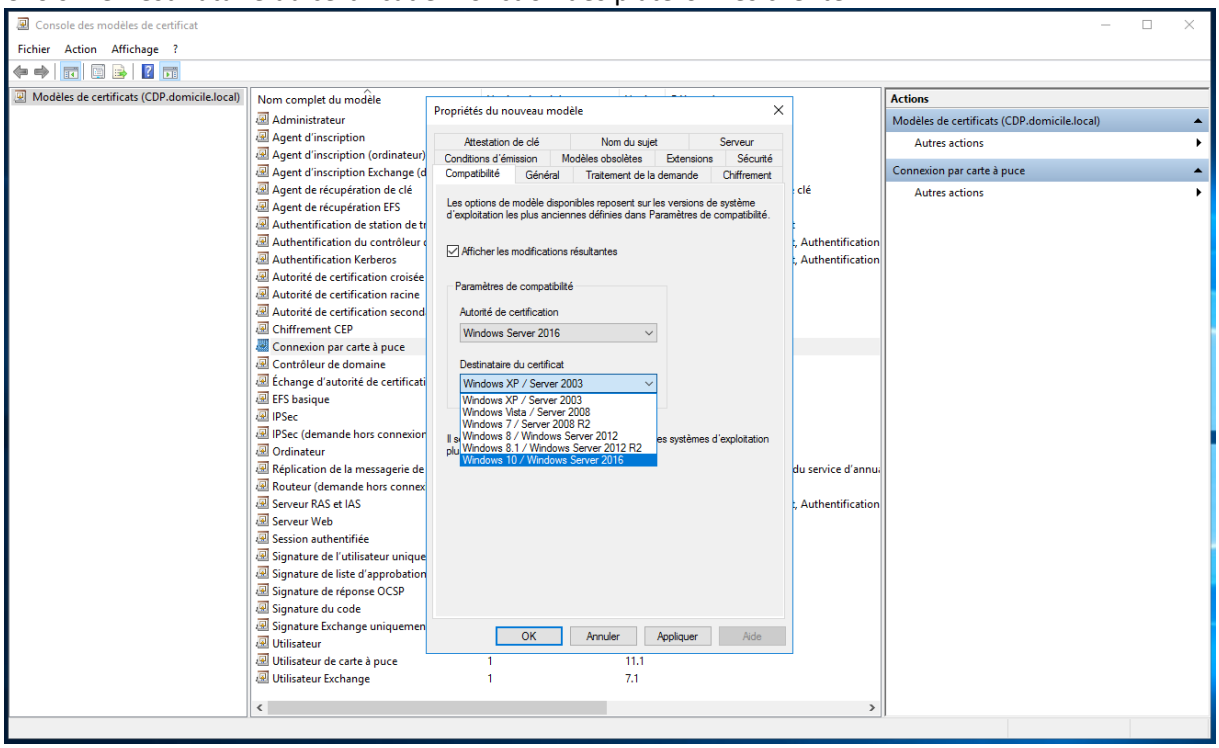


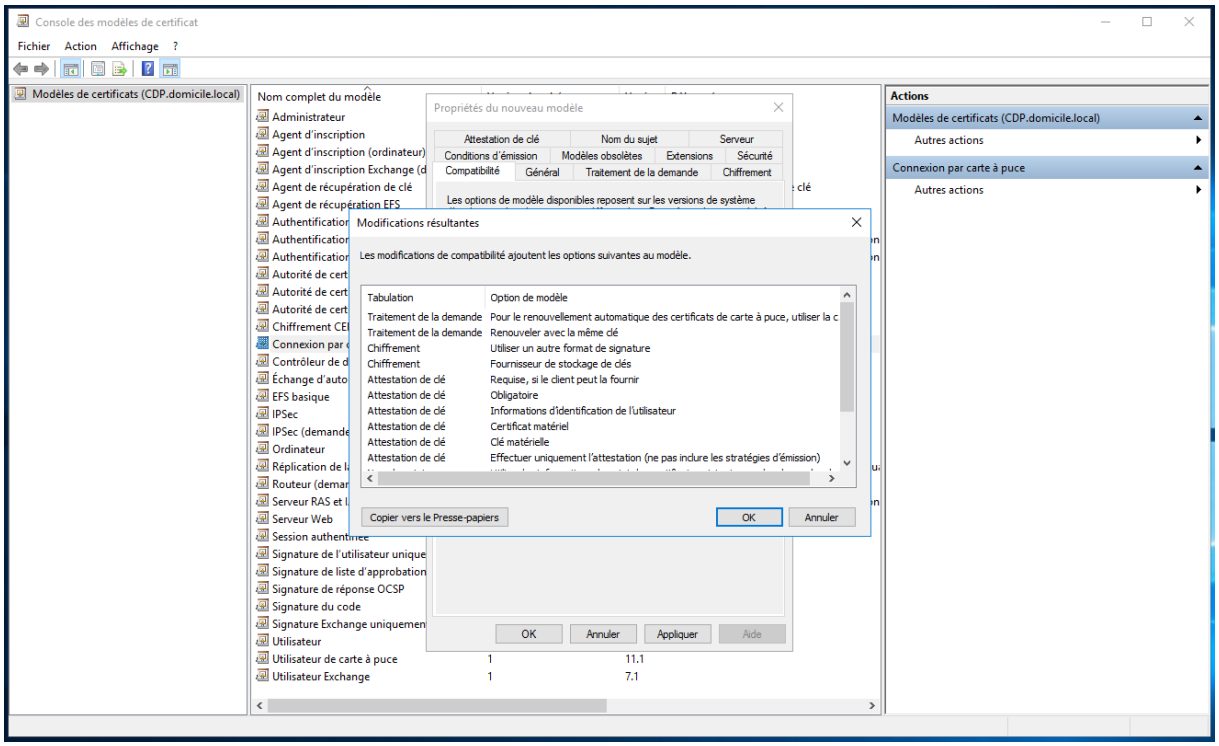
Choisir l'Autorité de certification en fonction de son serveur AD :



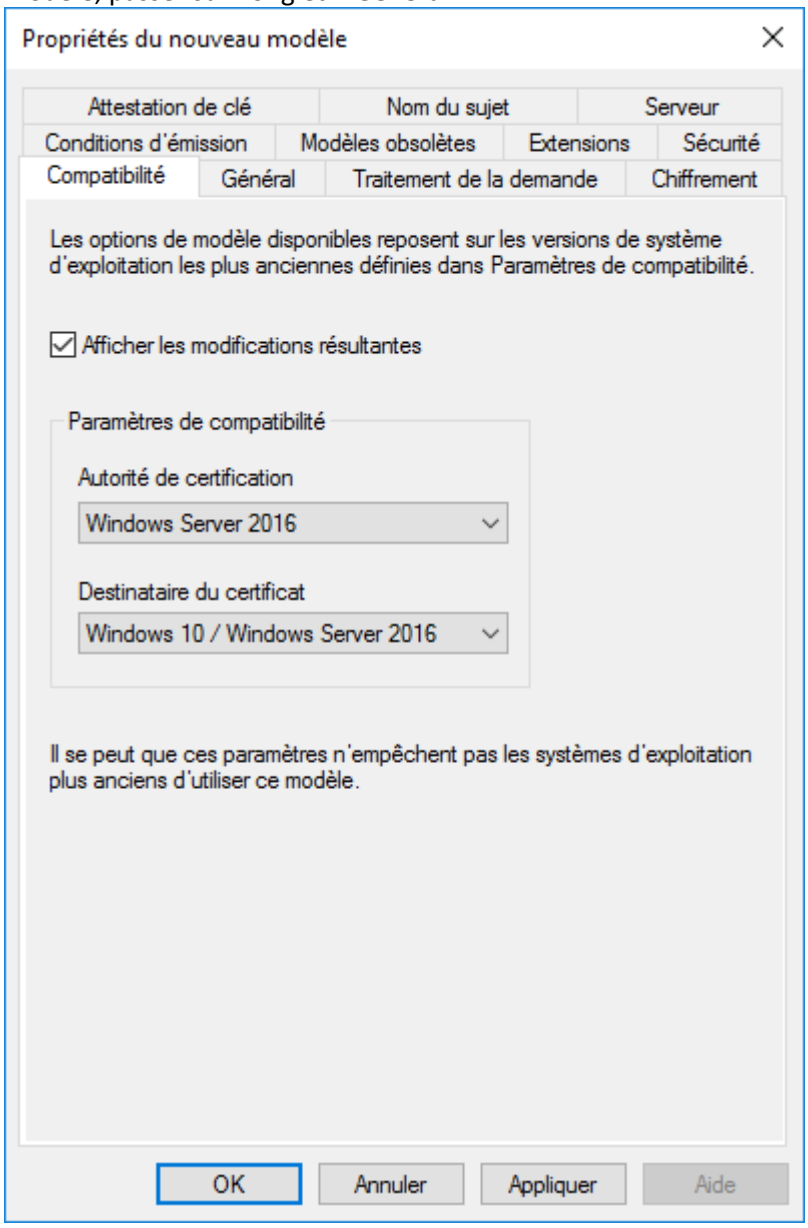


Choisir le Destinataire du certificat en fonction des plateformes cliente :

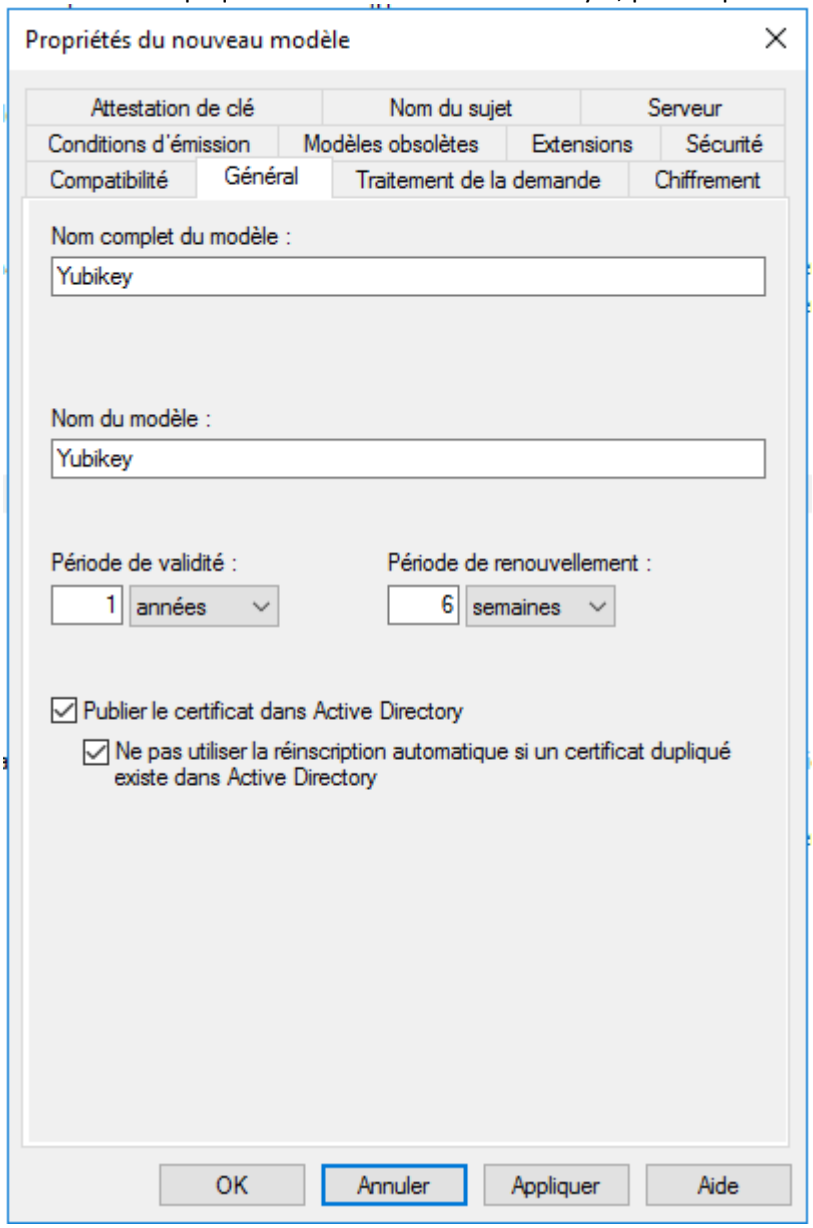




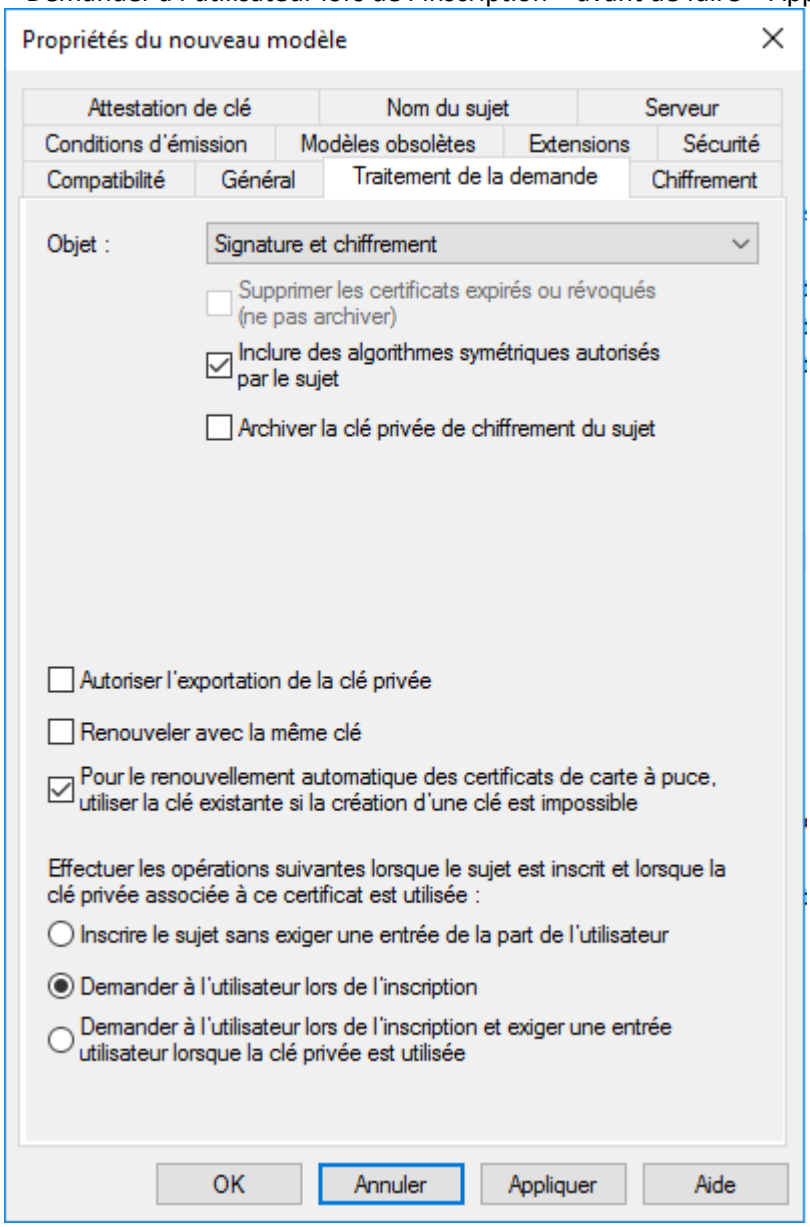
Après avoir configuré l'onglet « Compatibilité » dans la fenêtre de propriétés du nouveau modèle, passer sur l'onglet « Général ».



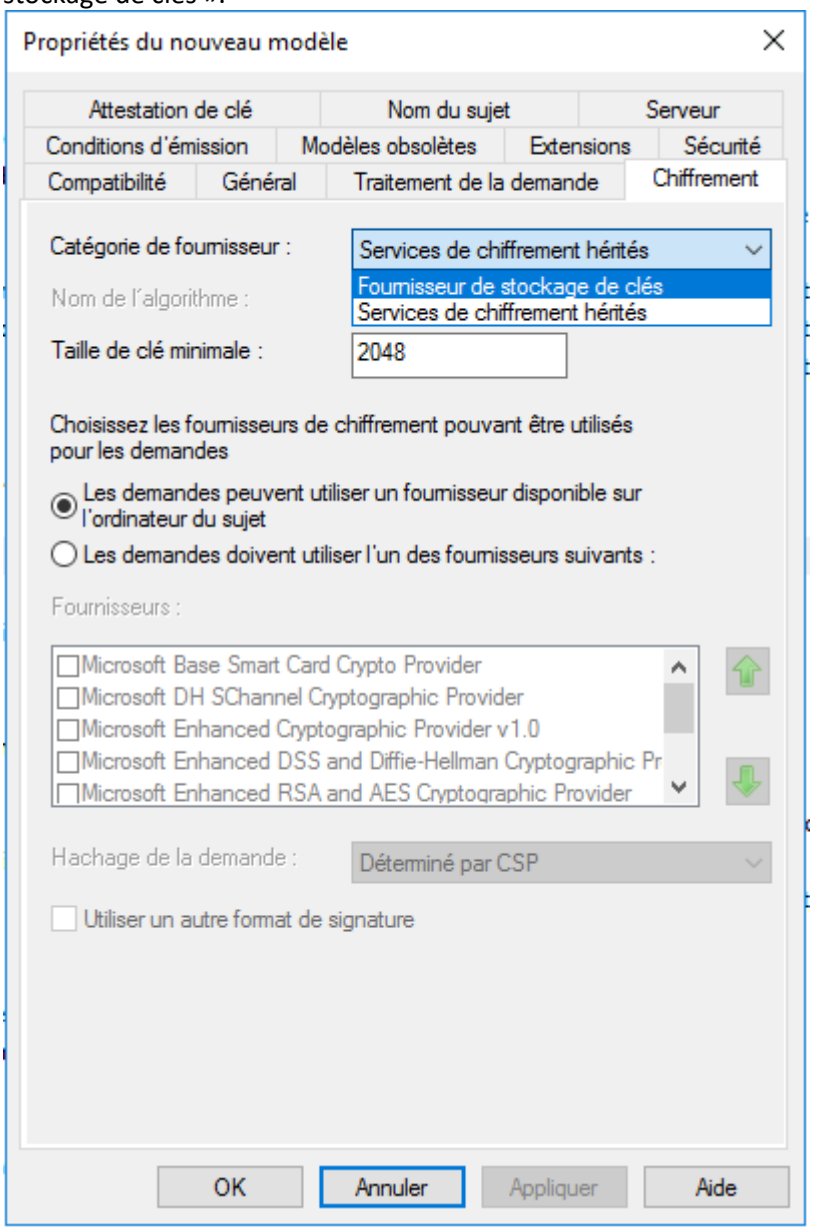
Dans l'onglet « Général », donner un nom complet au modèle « Yubikey » et cocher les cases « Publier le certificat dans Active Directory » et « Ne pas utiliser la réinscription automatique si un certificat dupliqué existe dans Active Directory », puis cliquer sur le bouton « Appliquer ».



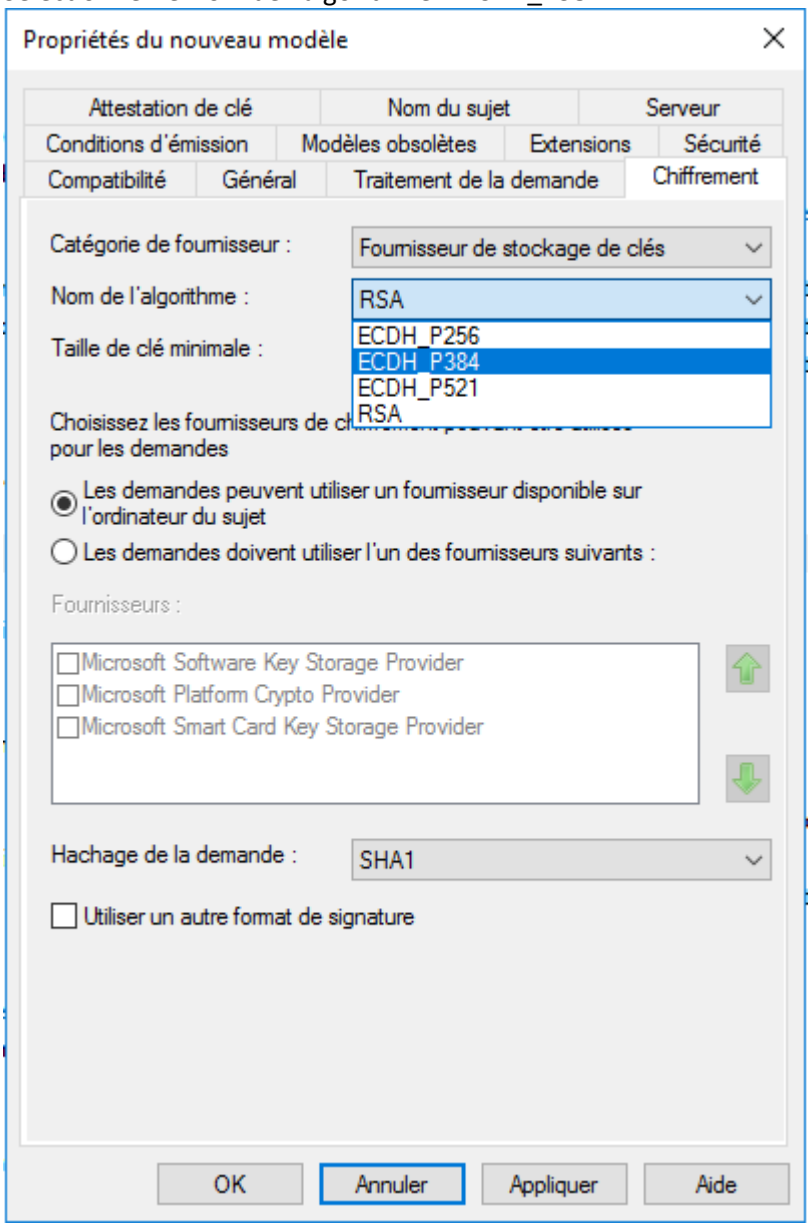
Sélectionner l'onglet « Traitement de la demande », cocher les cases « Inclure des algorithmes symétriques autorisés par le sujet » et « Pour le renouvellement automatique des certificats de carte à puce, utiliser la clé existante si la création d'une clé est impossible » puis sélectionner « Demander à l'utilisateur lors de l'inscription » avant de faire « Appliquer ».



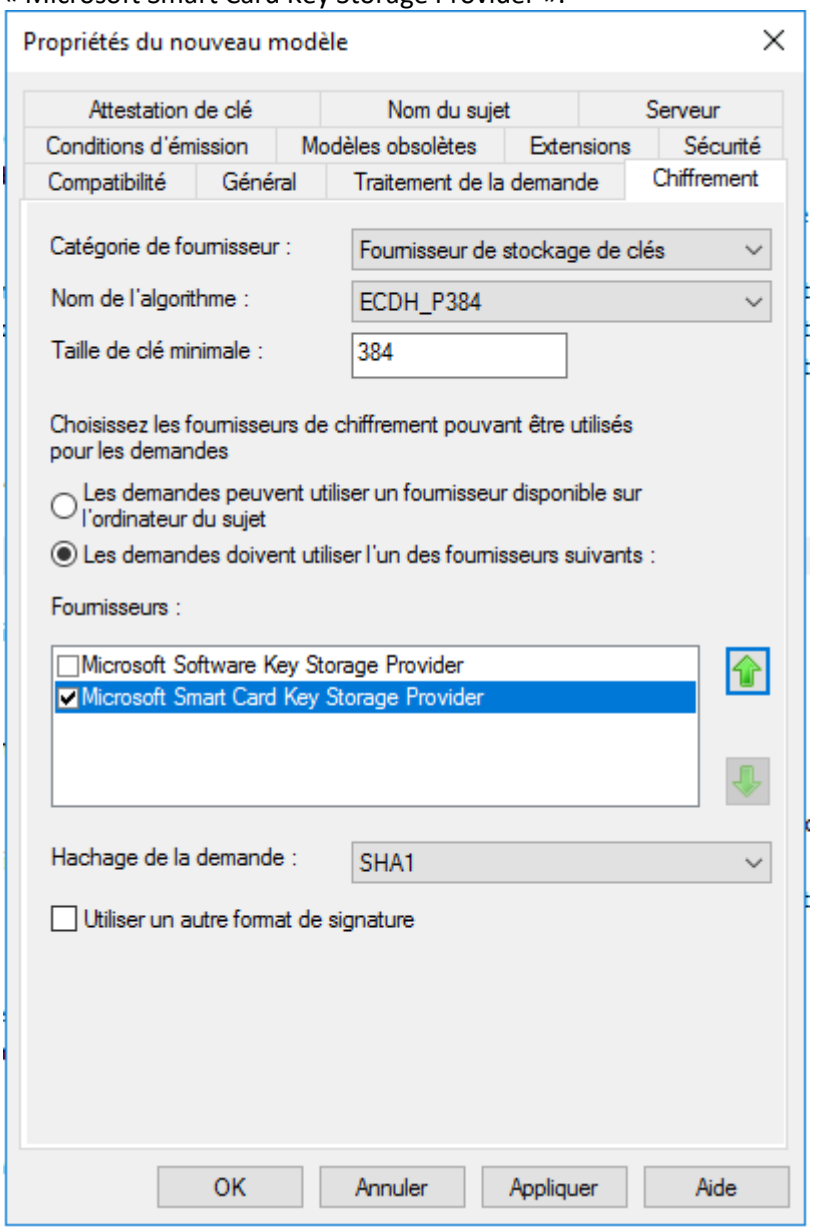
Sélectionner l'onglet « Chiffrement » et dans la catégorie de fournisseur choisir « Fournisseur de stockage de clés ».



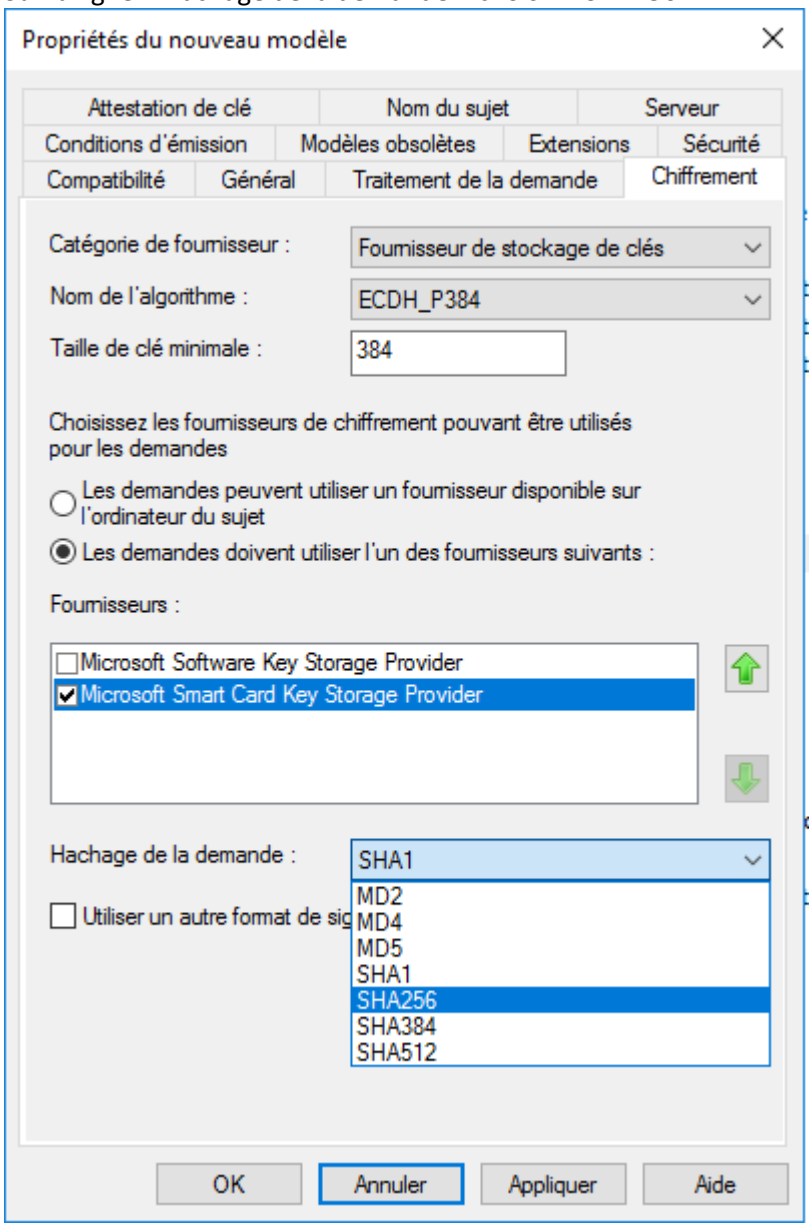
Sélectionner le Nom de l'algorithme « ECDH_P384 ».



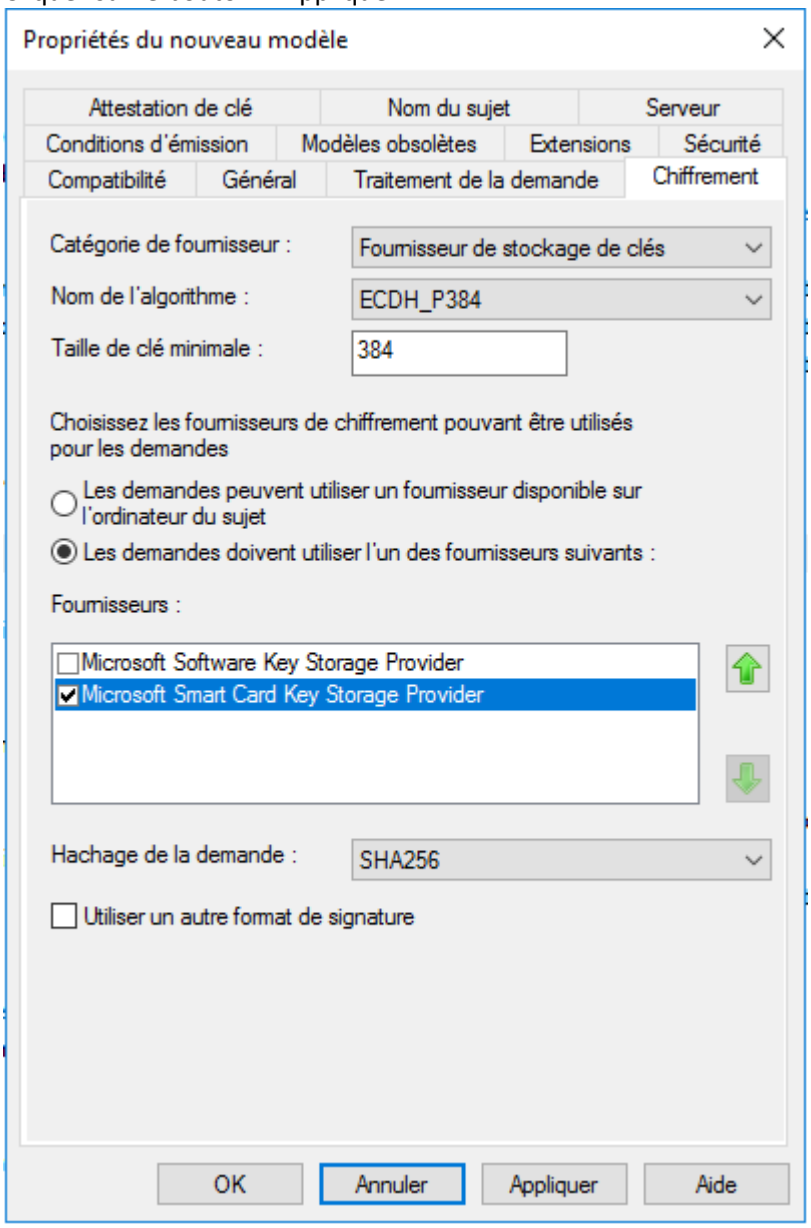
Choisir « Les demandes doivent utiliser l'un des fournisseurs suivants » et cocher la case « Microsoft Smart Card Key Storage Provider ».



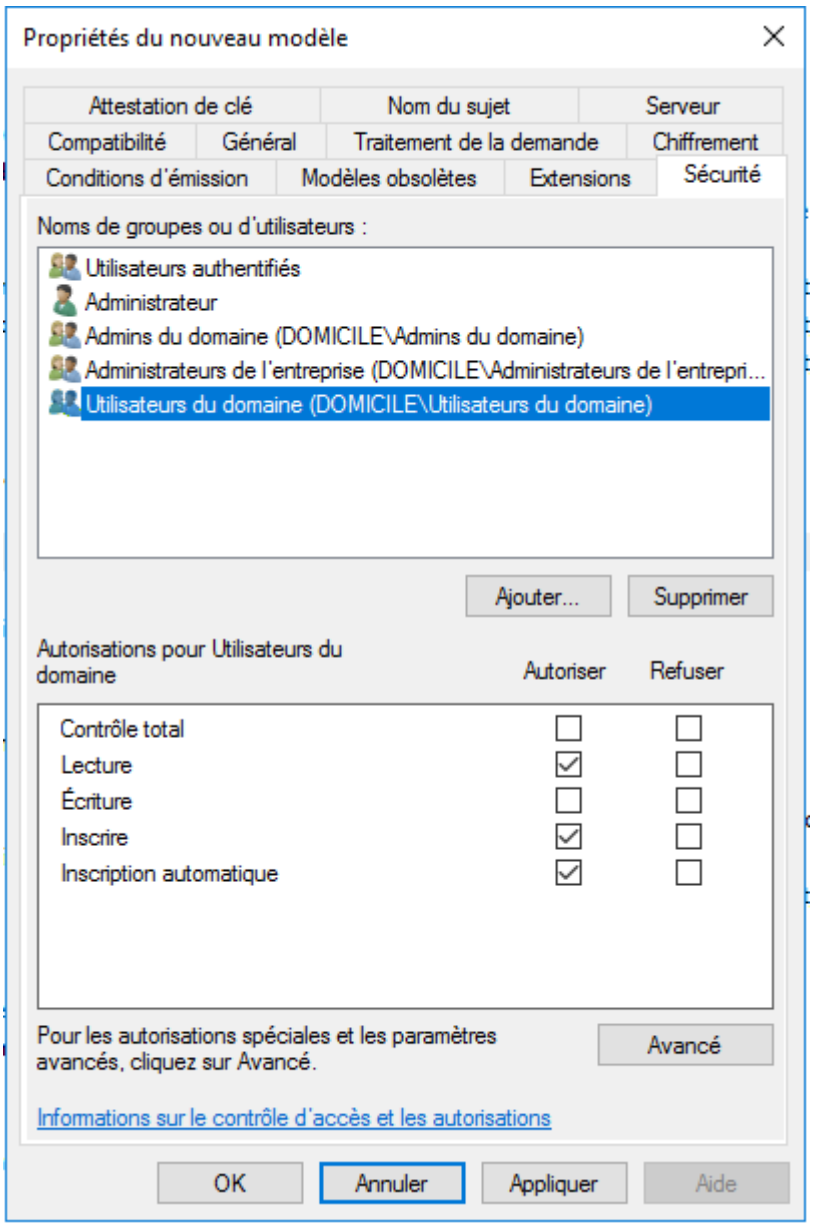
Sur la ligne « Hachage de la demande » choisir « SHA256 ».



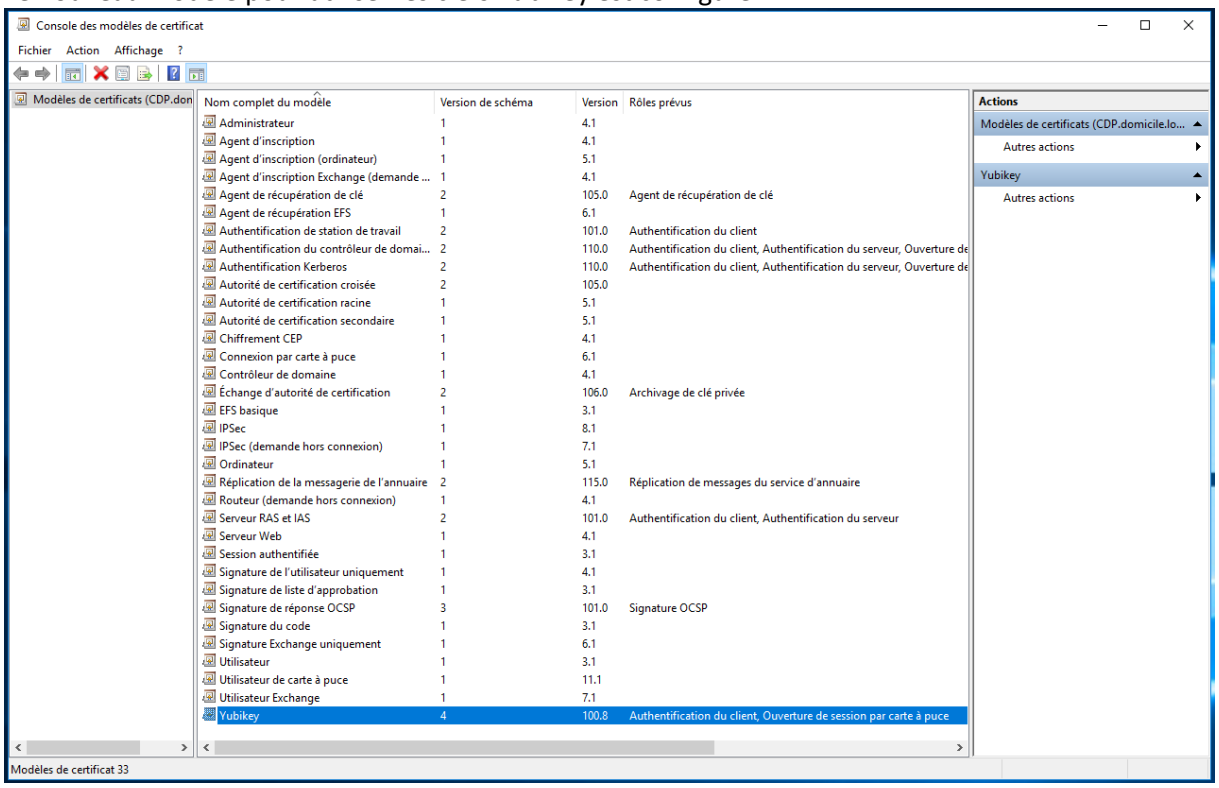
Cliquer sur le bouton « Appliquer » :



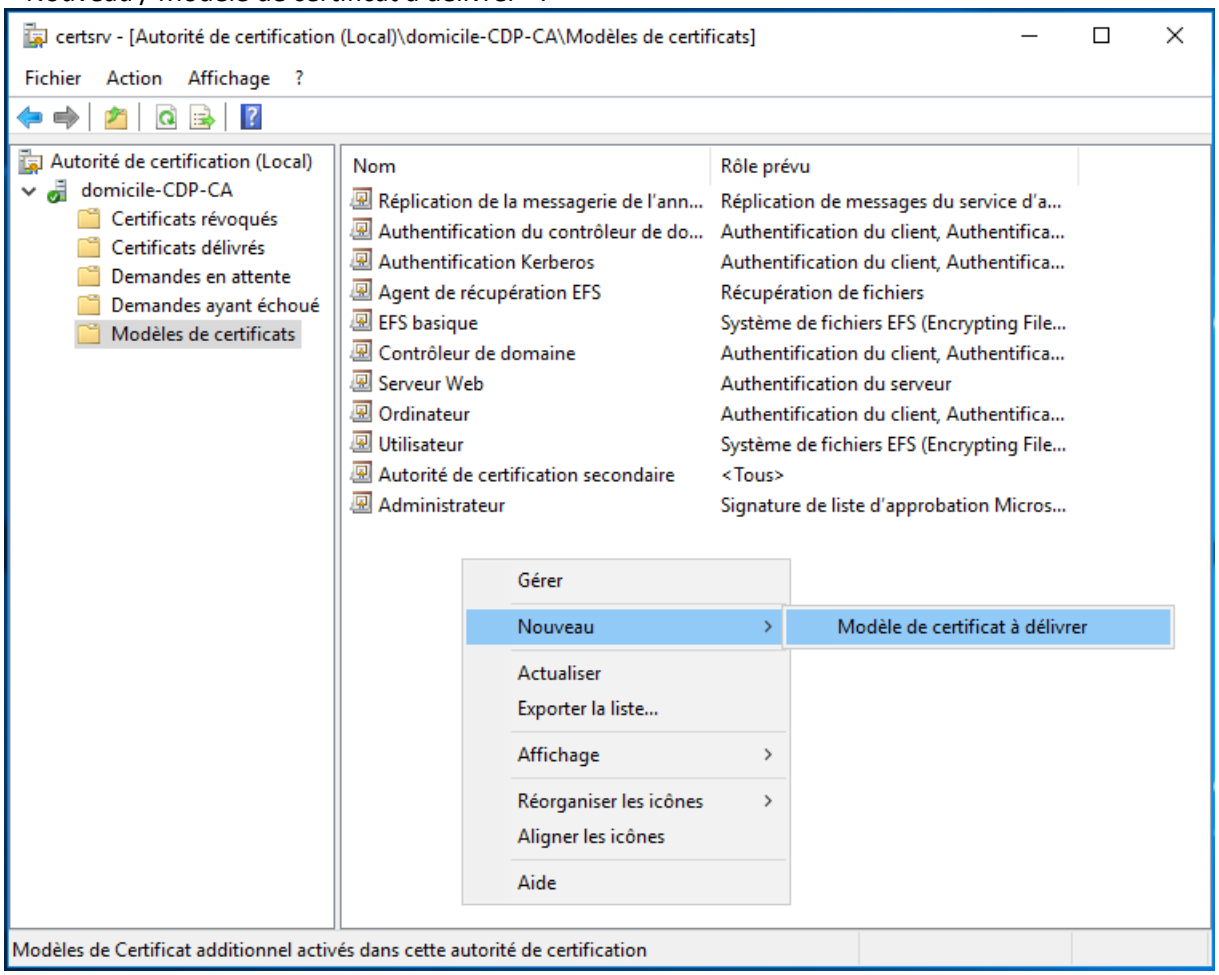
Sélectionner l'onglet « Sécurité », Ajouter le groupe « Utilisateurs du domaine » et pour ce groupe cocher les cases « Inscrire » et « Inscription automatique », cliquer sur « Appliquer » puis « OK ».



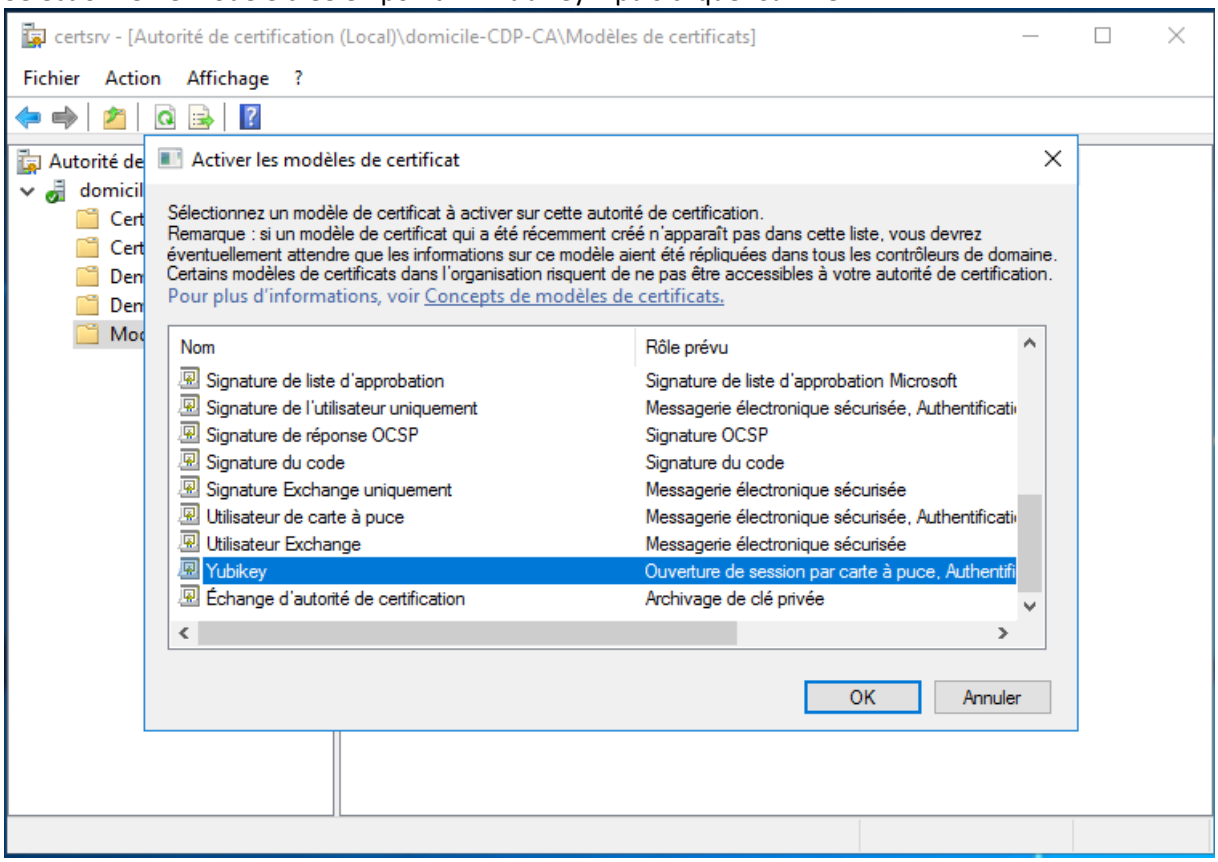
Le nouveau modèle pour utiliser les clefs Yubikey est configuré.



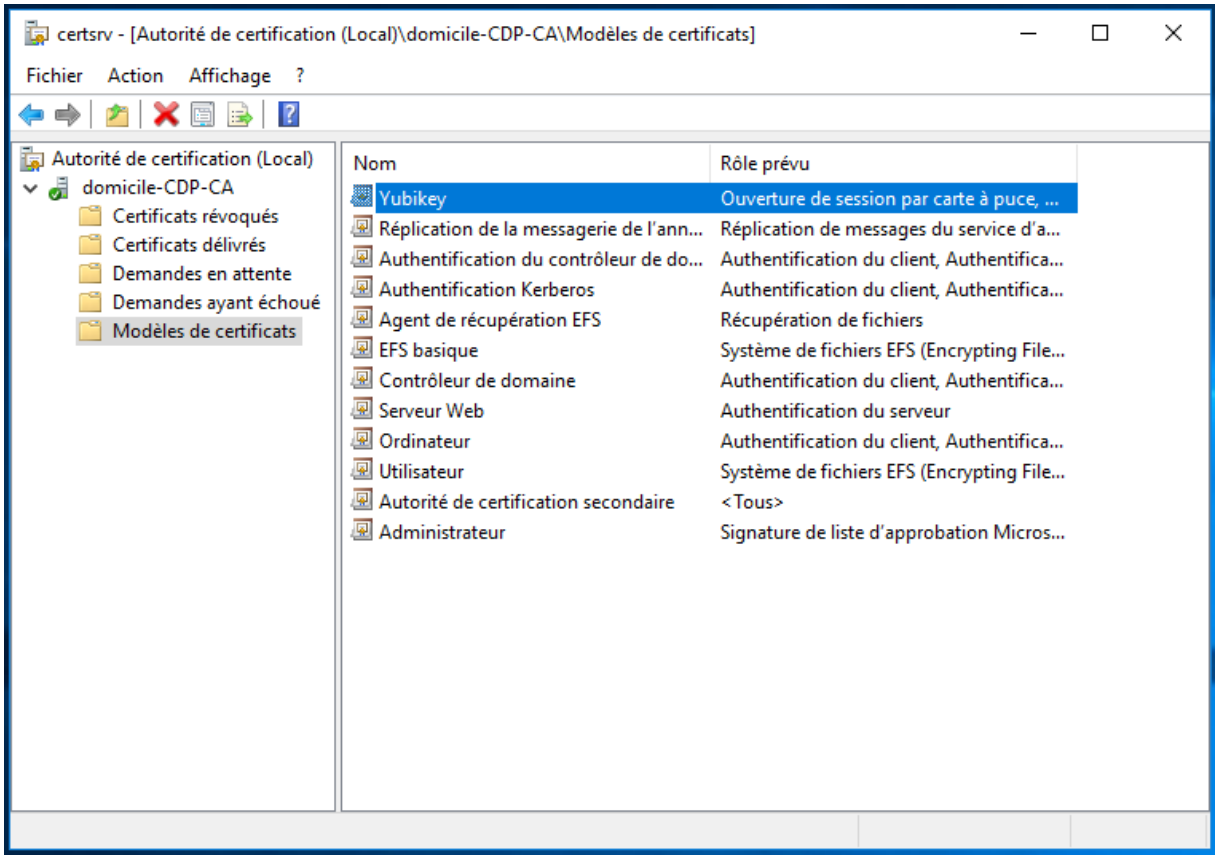
5. Mettre en service le nouveau modèle de certificat « Yubikey » :
   Cliquer sur « Démarrer / Exécuter » et saisir le commande « certsrv.msc ».
   Se rendre dans la rubrique « Modèles de certificats » et l'aide d'un clic droit cliquer sur « Nouveau / Modèle de certificat à délivrer ».



Sélectionner le modèle crée en point 4 « Yubikey » puis cliquer sur « OK ».



La configuration de l'autorité de certificat Active Directory et la prise en charge des clefs Yubkey est maintenant terminée :



6. Mettre en place la GPO pour prendre en compte les Yubikeys :

7. Enregistrement d'une clef :