Compétences	**D1.2 – Choix d'une solution** A1.2.4 Détermination des tests nécessaires à la validation d'un service **D1.3 – Mise en production d'un service** A1.3.1 Tests d'intégration et d'acceptation d'un service A1.3.3 Accompagnement de la mise en place d'un nouveau service A4.1.10 Rédaction d'une documentation d'utilisation
• **Objectif principal**	• **Créer** l'infrastructure de RUNNING HIGHTECH
• **Objectifs intermédiaires**	**Monter** un serveur Windows 2016 en mode graphique Mettre en place Active Directory Créer et gérer des objets de stratégie de groupe Déployer le rôle AD DS Gérer des sites Active Directory Répliquer Active Directory Gérer des certificats avec le rôle AD CS Mettre en place un service DNS et DHCP Installer et configurer la gestion des adresses IPAM Créer une infrastructure ISCI Gérer les contrôles d'accès dynamique Gérer les services de gestions droits avec le rôle AD RMS Installer et configurer AD FS Mettre en œuvre un proxy d'application WEB Gérer la répartition de charge et la répartition réseau Gérer la haute disponibilité
• **Outils utilisés**	• **hyperV ou Vmware client** • **Server Windows 2016 version datacenter en virtuel et en physique**
Mode de travail	• Seuls ou en groupe selon leur préférence
Mode d'évaluation	• Validation des missions au fil de l'eau, en direct, sur une base personnelle et selon son rythme jusqu'à la fin de chaque semestre • Compte-rendu à rendre pour évaluation sommative à la fin de chaque semestre coefficient 2 • Chaque compte-rendu est à poser dans le PFC • Épreuve E4 certificative

Sommaire

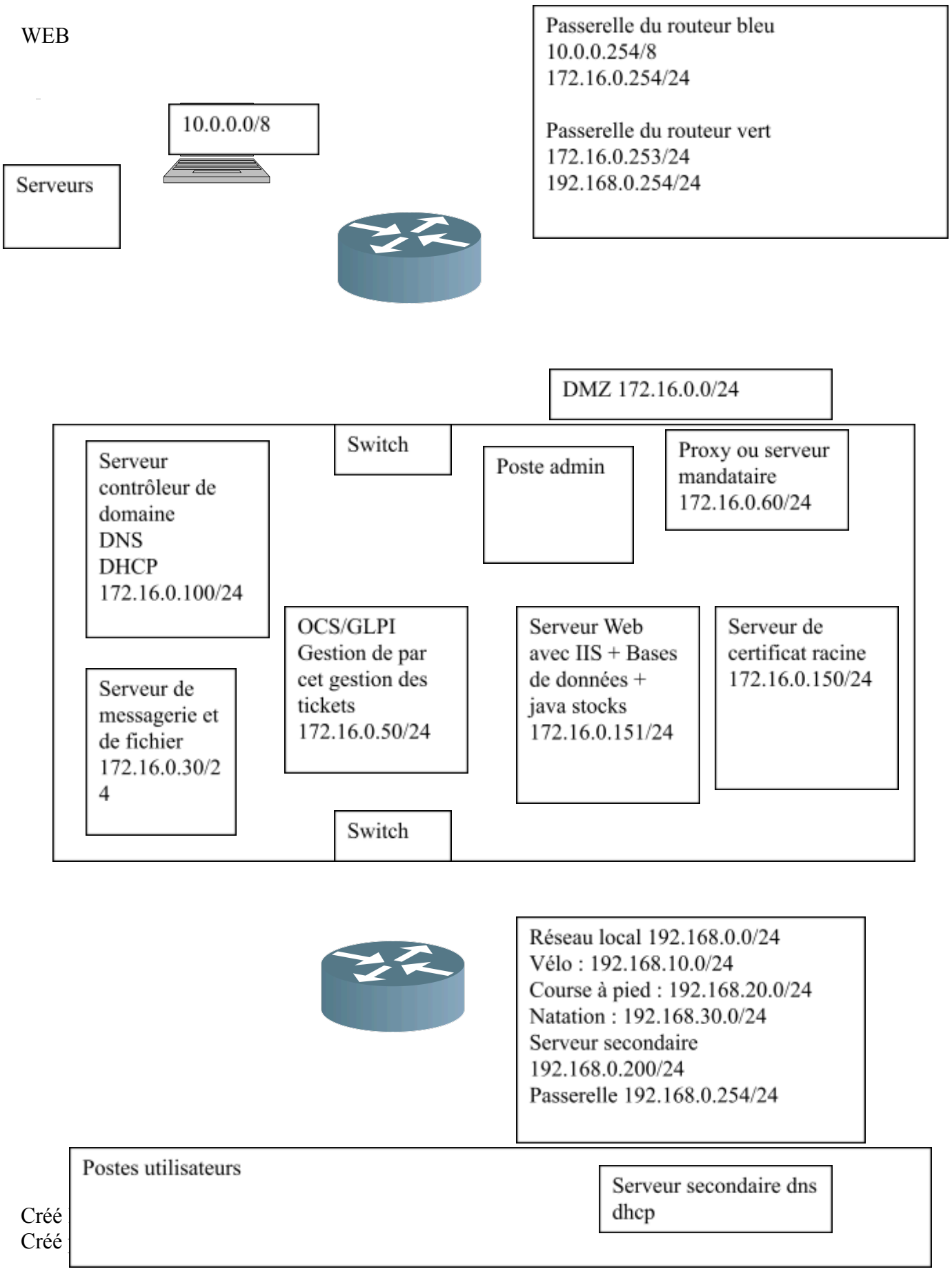
Contexte Running Hightech

L'association Web Courses s'inscrit dans le contexte RUNNING HIGHTECH, qui a pour mission de fournir des espaces et des services à différents clients et à d'autres structures hébergées. La RUNNING HIGHTECH est une structure indépendante.

Afin de répondre aux attentes de ses clients, la RUNNING HIGHTECH veut mettre en place une infrastructure basée sur des serveurs Windows 2016, comprenant :

- La gestion des comptes et des droits utilisateurs ainsi que le déploiement de stratégies de groupe
- La gestion des sites
- La réplication
- Le service de gestion des noms de domaine
- la distribution des adresses dynamiques
- les contrôles des accès dynamiques
- la gestion des services de gestion des droits
- la mise en place d'un espace sécurisé et en particulier un serveur mandataire
- gérer la répartition de charge et la répartition réseau
- gérer la haute disponibilité

Présentation générale de l'infrastructure de base



Créé
Créé

Mission 1 Monter un serveur Windows 2016 version datacenter

Compétences	
Objectif principal	Mettre en place Windows Server 2016
Objectifs intermédiaires	Installer Windows Server 2016 en mode graphique Configurer l'interface réseau Renommer un serveur avec sconfig Configurer l'adressage ip avec sconfig
Vocabulaire à connaître	
Évaluation	Compte-rendu à rendre pour évaluation sommative coefficient 2 Compte-rendu est à poser dans votre PFC Épreuve E4 certificative

Votre mission

Installer Windows Server 2016 en mode graphique.

Informations utiles

Ce serveur sera le contrôleur de domaine principal et contiendra les services suivants :

- Active Directory
- DNS
- DHCP

Adresse IP du serveur contrôleur de domaine : 172.16.0.100 / 24
Adresse de passerelle : 172.16.0.254/24
Nom du domaine à gérer : webcourses.sio
Nom de la machine contrôleur de domaine : srvaddns

1. Configuration des cartes réseaux

a. Démarrer – panneau de configuration – connexion réseau – clic droit sur connexion au réseau local – propriété – protocole internet – propriété – saisir les valeurs des à IP selon le schéma présenté
b. Répéter ce procédé pour chacune des cartes réseaux
c. Vérifier à l'aide de la commande **IPCONFIG /ALL** sous l'interpréteur de commande que les informations ont bien été saisies correctement

2. Le service de routage

Afin que le routeur joue son rôle de routeur, il faut activer le service de routage.
Pour se faire aller dans :

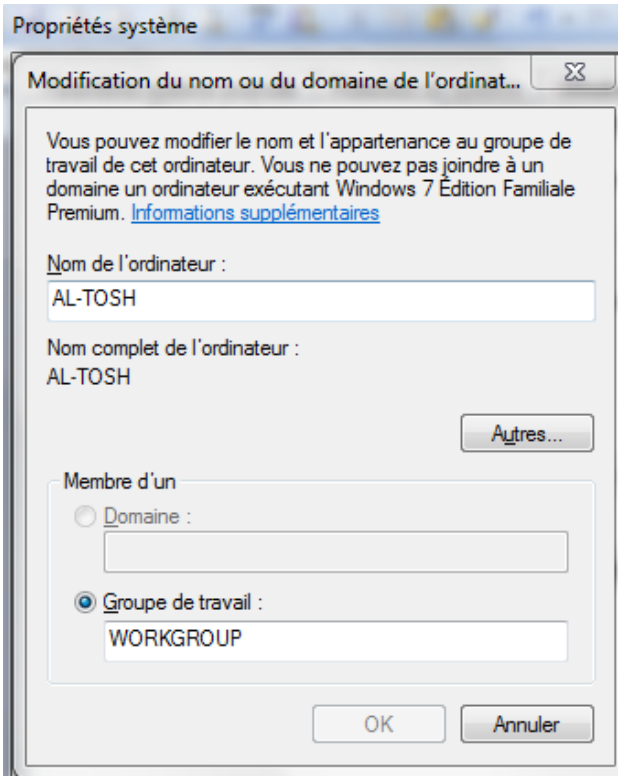
Démarrer – panneau de configuration – outils d'administration – services – routage et accès distant – type de démarrage : automatique – démarrer le service

3. S'assurer que le pare feu est désactivé

Pour se faire aller dans :
Panneau de configuration- système et sécurité – pare feu windows - désactivé

4. Nom des postes

Assurez-vous que les noms des postes soient bien distinct les uns des autres. Vous ne devez pas avoir de nom en double.
Si vous avez besoin de changer le nom d'un poste, aller dans Démarrer – Poste de travail – clic droit – Propriétés – Nom de l'ordinateur – Modifier – Changer le nom du poste dans la zone « nom de l'ordinateur » - OK – redémarrer l'ordinateur

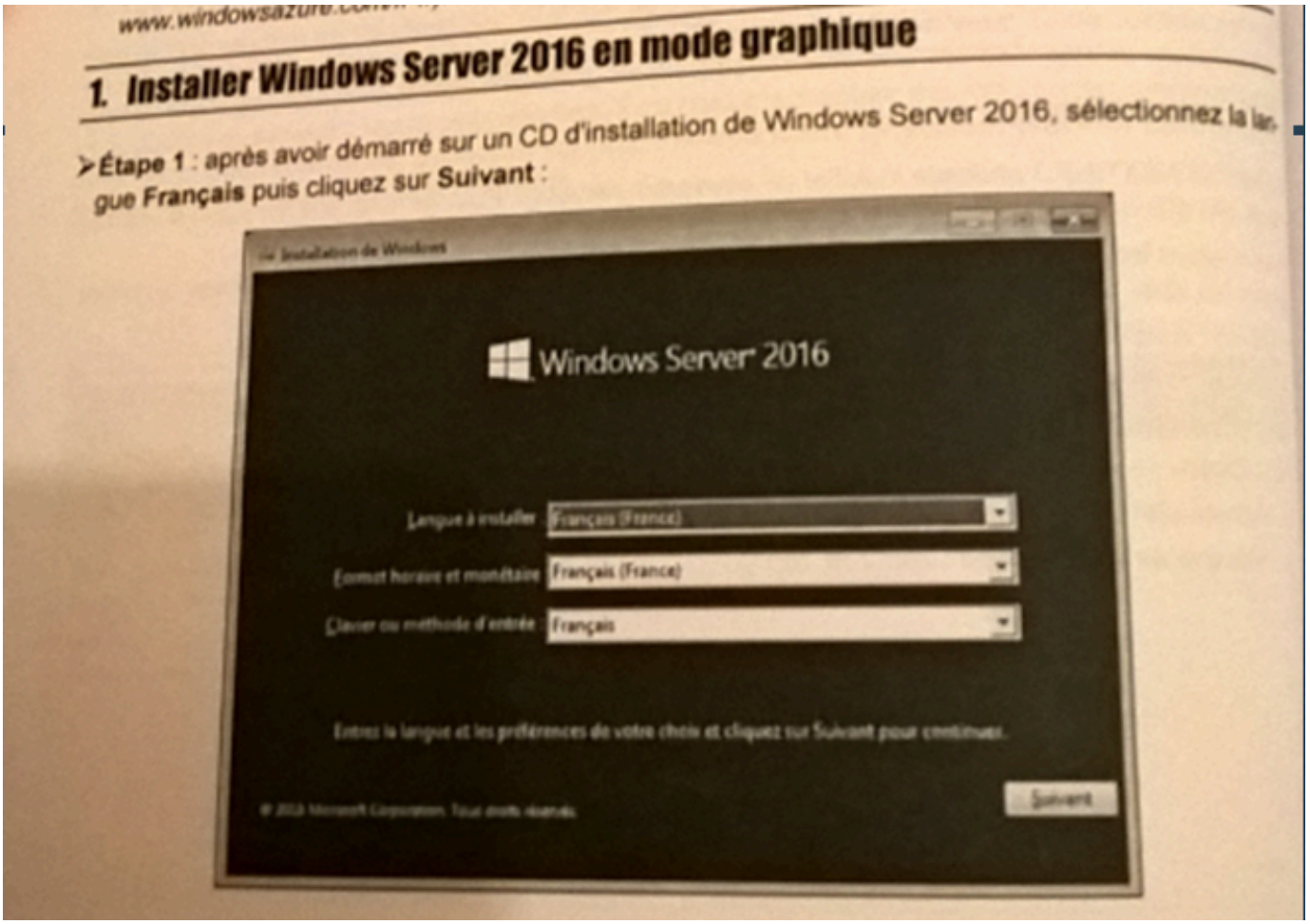


5. Vérification de la connectivité entre chaque poste du réseau

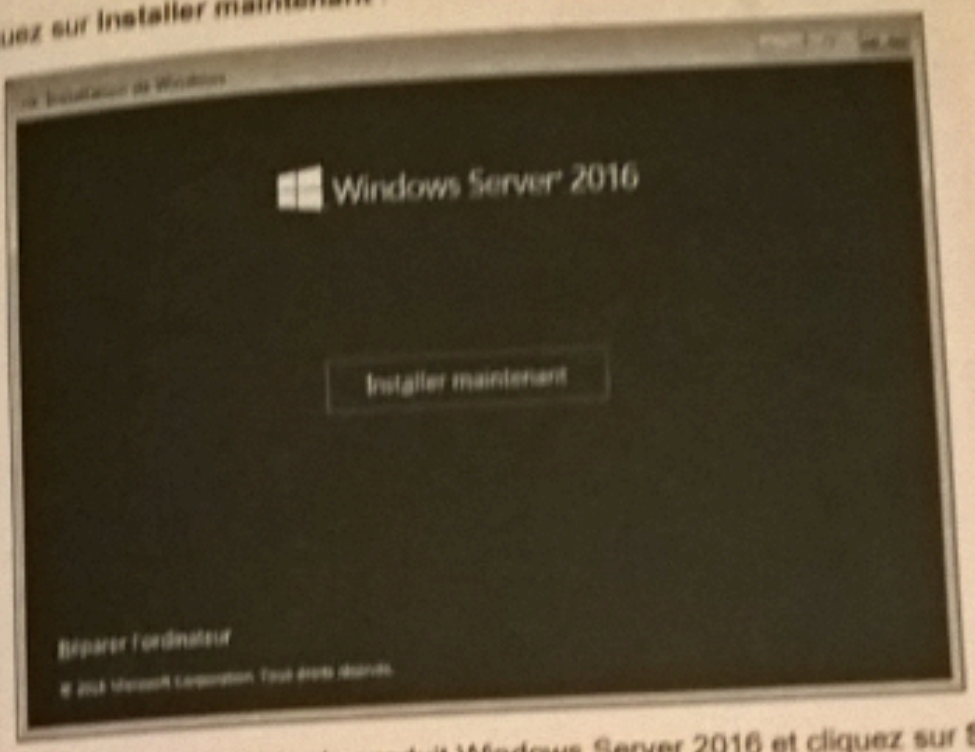
tableau de vérification					
	Poste admin	Serveur contrôleur de domaine	passerelle routeur 2	passerelle routeur 1	poste client
Poste admin					
Serveur contrôleur de domaine					
passerelle routeur 1					
passerelle routeur 2					
poste client					

A faire pour toutes les machines référencées dans le schéma réseau de base

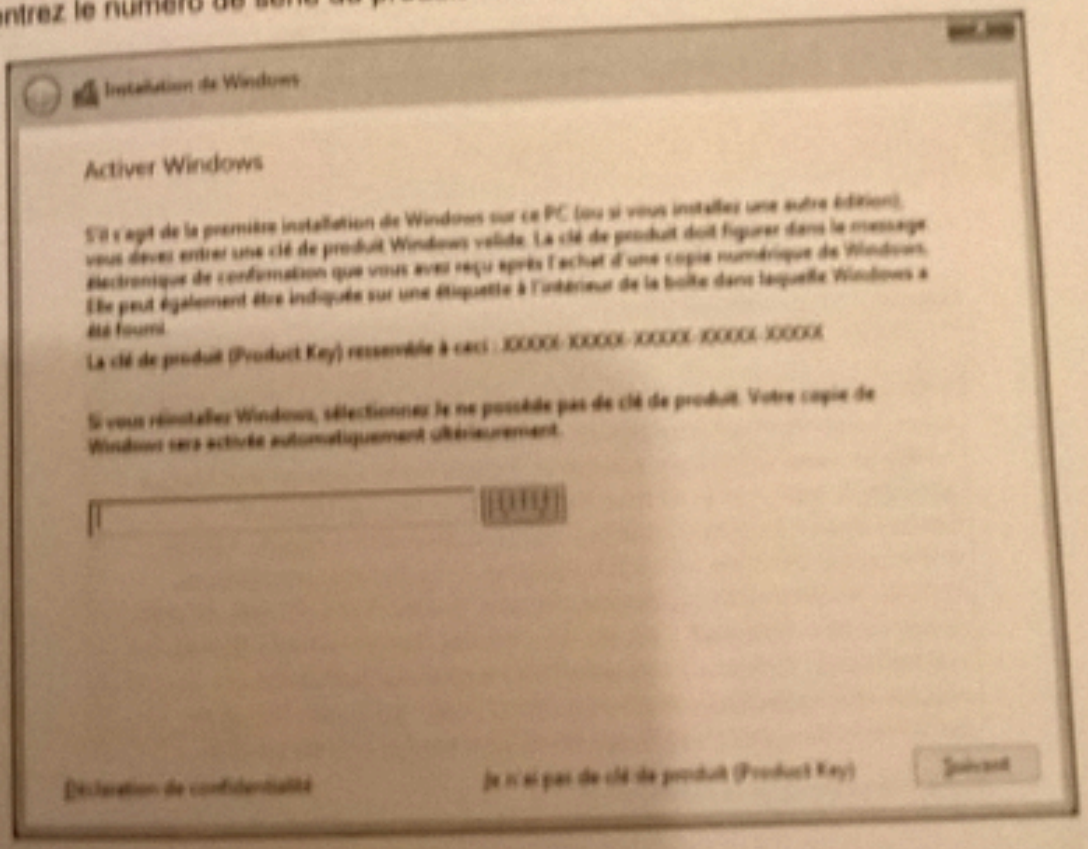
Guide d'installation

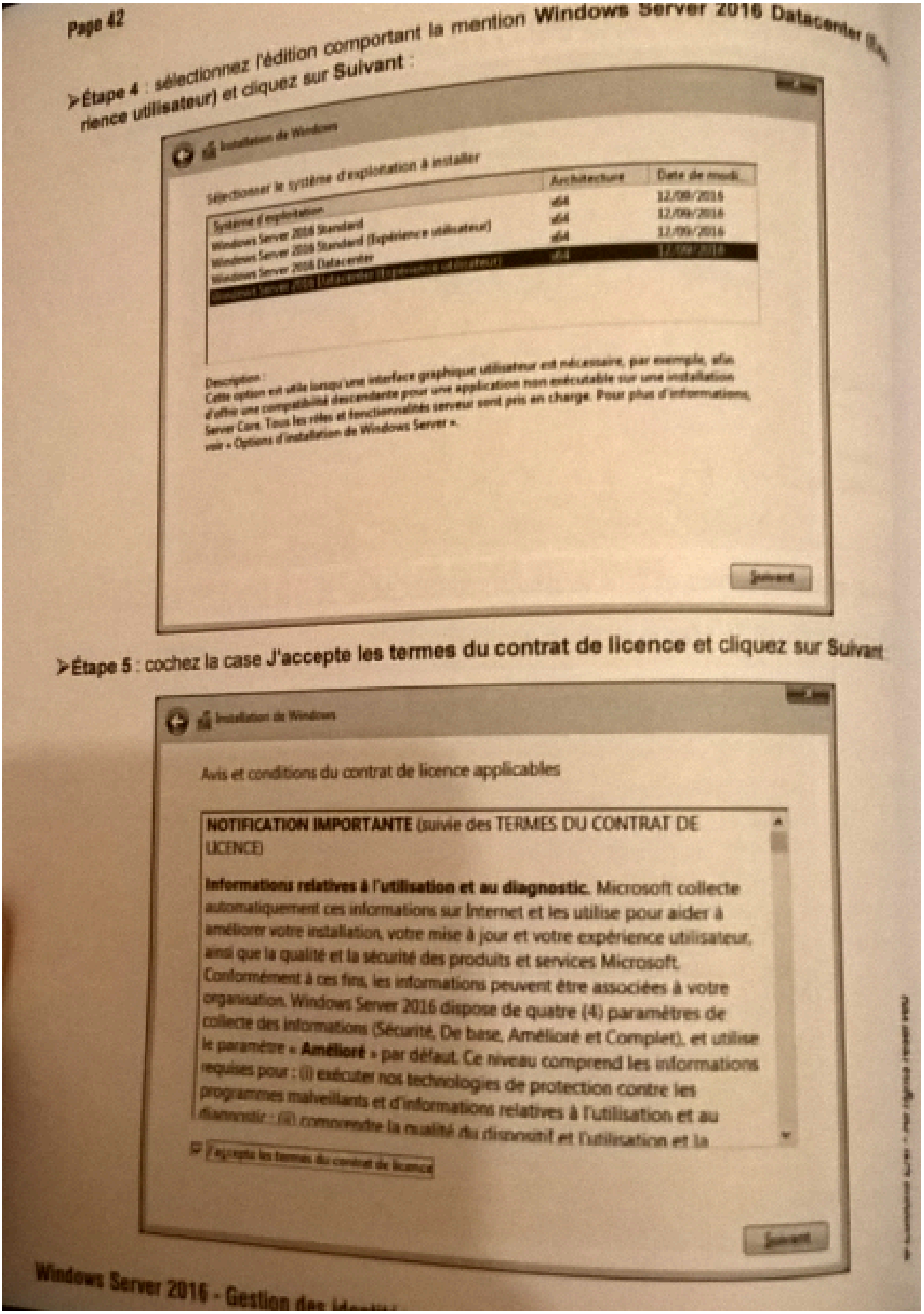


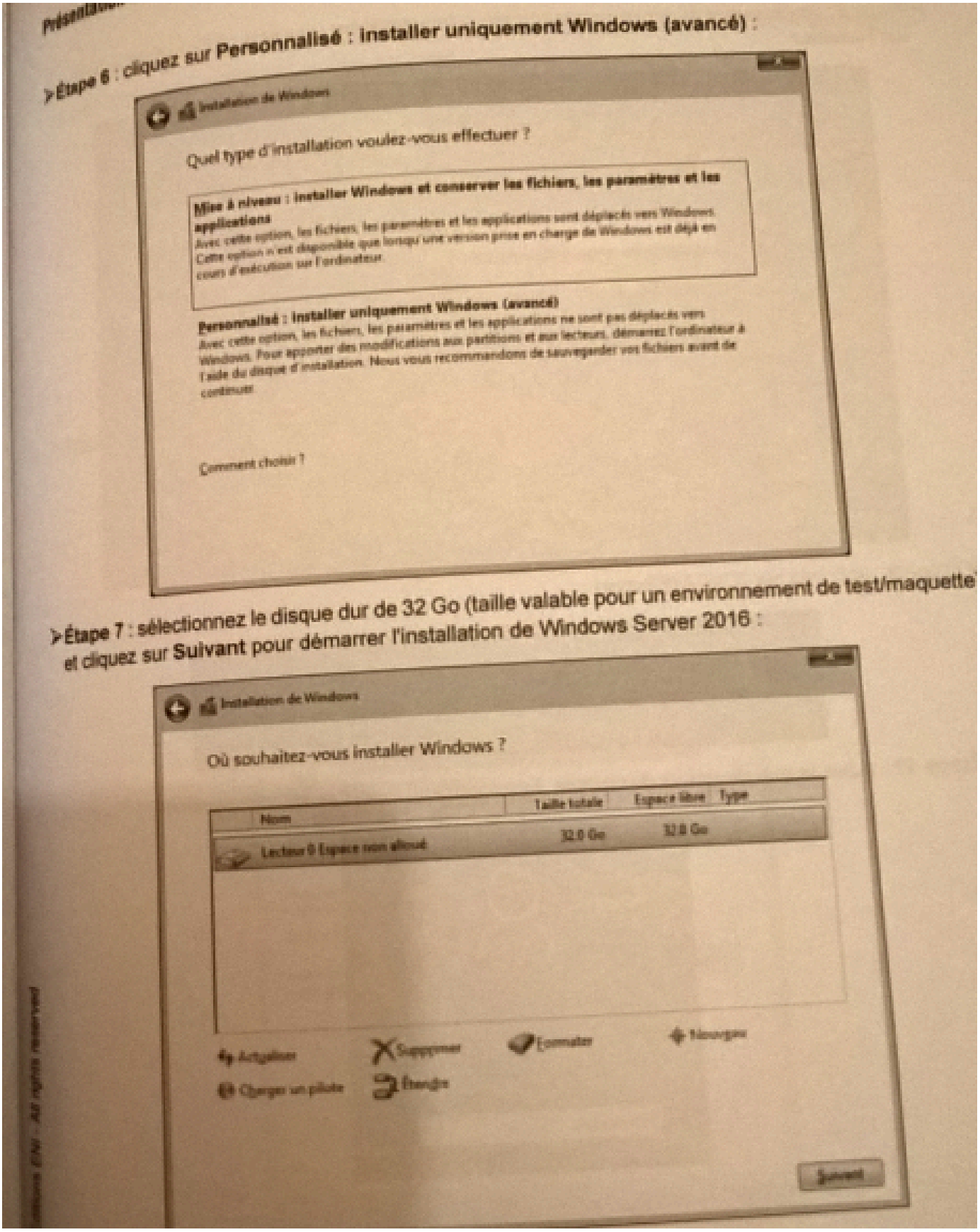
➢ **Étape 2** : cliquez sur **Installer maintenant** :

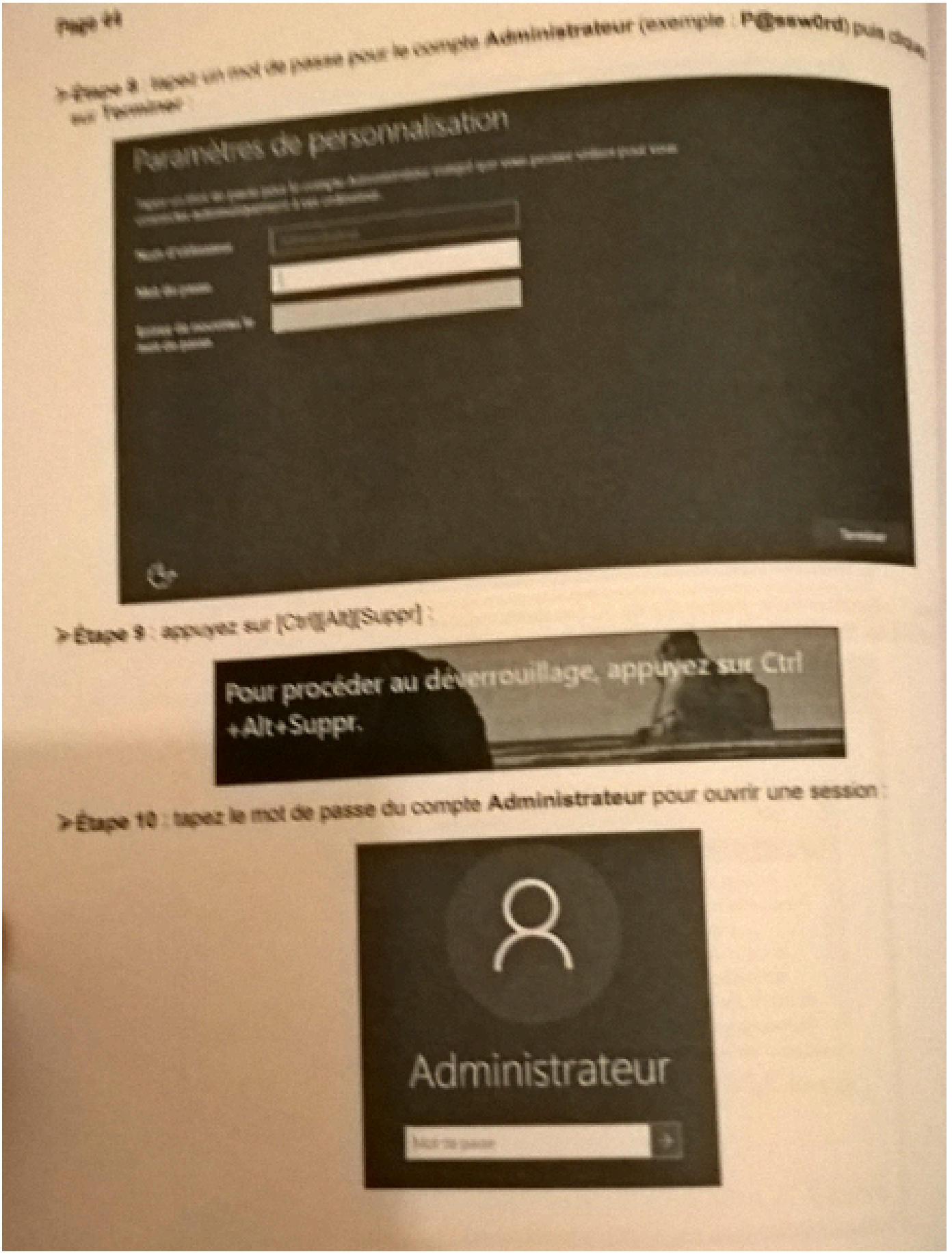


➢ **Étape 3** : entrez le numéro de série du produit Windows Server 2016 et cliquez sur **Suivant** :

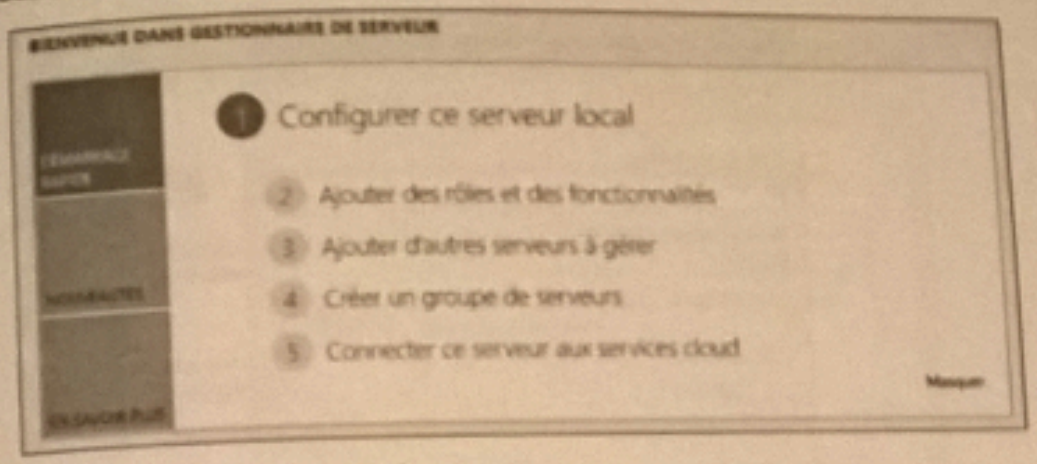



Page 42
➢Étape 4 : sélectionnez l'édition comportant la mention Windows Server 2016 Datacenter (
rience utilisateur) et cliquez sur Suivant :
Installation de Windows
Sélectionner le système d'exploitation à installer
Système d'exploitation
Architecture
Date de modi...
Windows Server 2016 Standard
x64
12/08/2016
Windows Server 2016 Standard (Expérience utilisateur)
x64
12/08/2016
Windows Server 2016 Datacenter
x64
12/08/2016
Description :
Cette option est utile lorsqu'une interface graphique utilisateur est nécessaire, par exemple, afin
d'offrir une compatibilité descendante pour une application non exécutable sur une installation
Server Core. Tous les rôles et fonctionnalités serveur sont pris en charge. Pour plus d'informations,
voir « Options d'installation de Windows Server ».
Suivant
➢Étape 5 : cochez la case J'accepte les termes du contrat de licence et cliquez sur Suivant
Installation de Windows
Avis et conditions du contrat de licence applicables
NOTIFICATION IMPORTANTE (suivie des TERMES DU CONTRAT DE
LICENCE)
Informations relatives à l'utilisation et au diagnostic. Microsoft collecte
automatiquement ces informations sur Internet et les utilise pour aider à
améliorer votre installation, votre mise à jour et votre expérience utilisateur,
ainsi que la qualité et la sécurité des produits et services Microsoft.
Conformément à ces fins, les informations peuvent être associées à votre
organisation. Windows Server 2016 dispose de quatre (4) paramètres de
collecte des informations (Sécurité, De base, Amélioré et Complet), et utilise
le paramètre « Amélioré » par défaut. Ce niveau comprend les informations
requises pour : (i) exécuter nos technologies de protection contre les
programmes malveillants et d'informations relatives à l'utilisation et au
diagnostic ; (ii) connaître la qualité du diagnostic et l'utilisation et la
J'accepte les termes du contrat de licence
Suivant
Windows Server 2016 - Gestion des

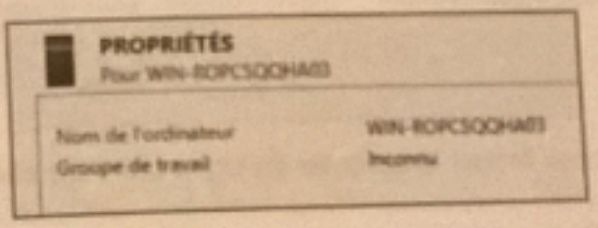

Présentation
Étape 6 : cliquez sur Personnalisé : installer uniquement Windows (avancé) :
Installation de Windows
Quel type d'installation voulez-vous effectuer ?
Mise à niveau : installer Windows et conserver les fichiers, les paramètres et les applications
Avec cette option, les fichiers, les paramètres et les applications sont déplacés vers Windows.
Cette option n'est disponible que lorsqu'une version prise en charge de Windows est déjà en cours d'exécution sur l'ordinateur.
Personnalisé : installer uniquement Windows (avancé)
Avec cette option, les fichiers, les paramètres et les applications ne sont pas déplacés vers Windows. Pour apporter des modifications aux partitions et aux lecteurs, démarrez l'ordinateur à l'aide du disque d'installation. Nous vous recommandons de sauvegarder vos fichiers avant de continuer.
Comment choisir ?
Étape 7 : sélectionnez le disque dur de 32 Go (taille valable pour un environnement de test/maquette)
et cliquez sur Suivant pour démarrer l'installation de Windows Server 2016 :
Installation de Windows
Où souhaitez-vous installer Windows ?
Nom
Taille totale
Espace libre
Type
Lecteur 0 Espace non alloué
32.0 Go
32.0 Go
Actualiser
Supprimer
Formater
Nouveau
Charger un pilote
Étendre
Suivant


Paramètres de personnalisation
Pour procéder au déverrouillage, appuyez sur Ctrl +Alt+Suppr.
Administrateur

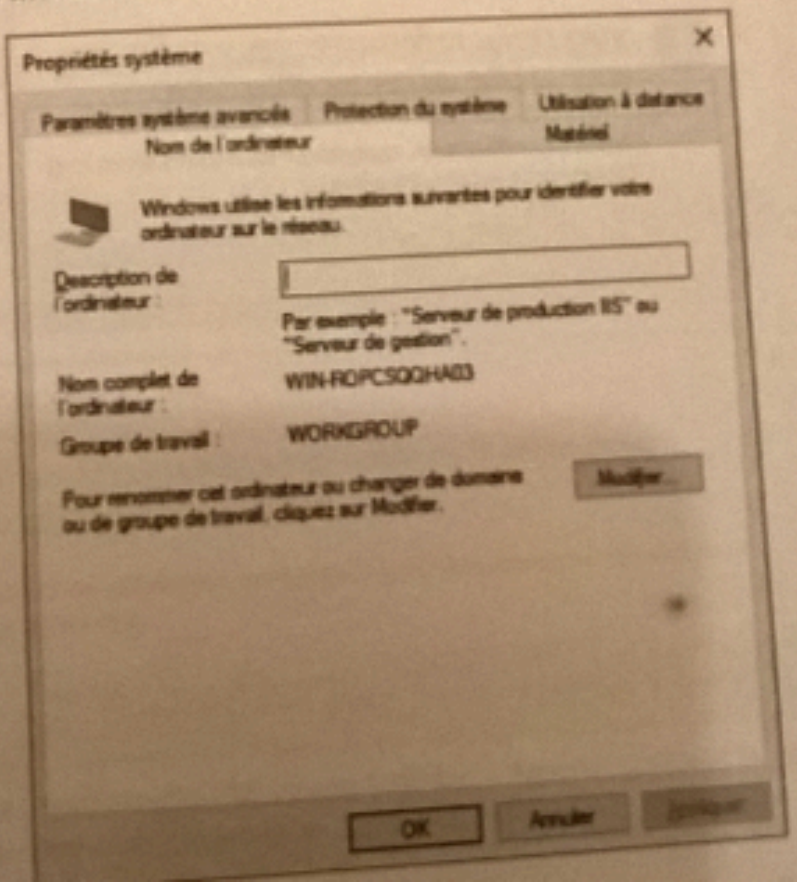
➢**Étape 11** : à l'ouverture de la session, la console **Gestionnaire de serveur** s'ouvre automatiquement. Cliquez sur **Configurer ce serveur local** :



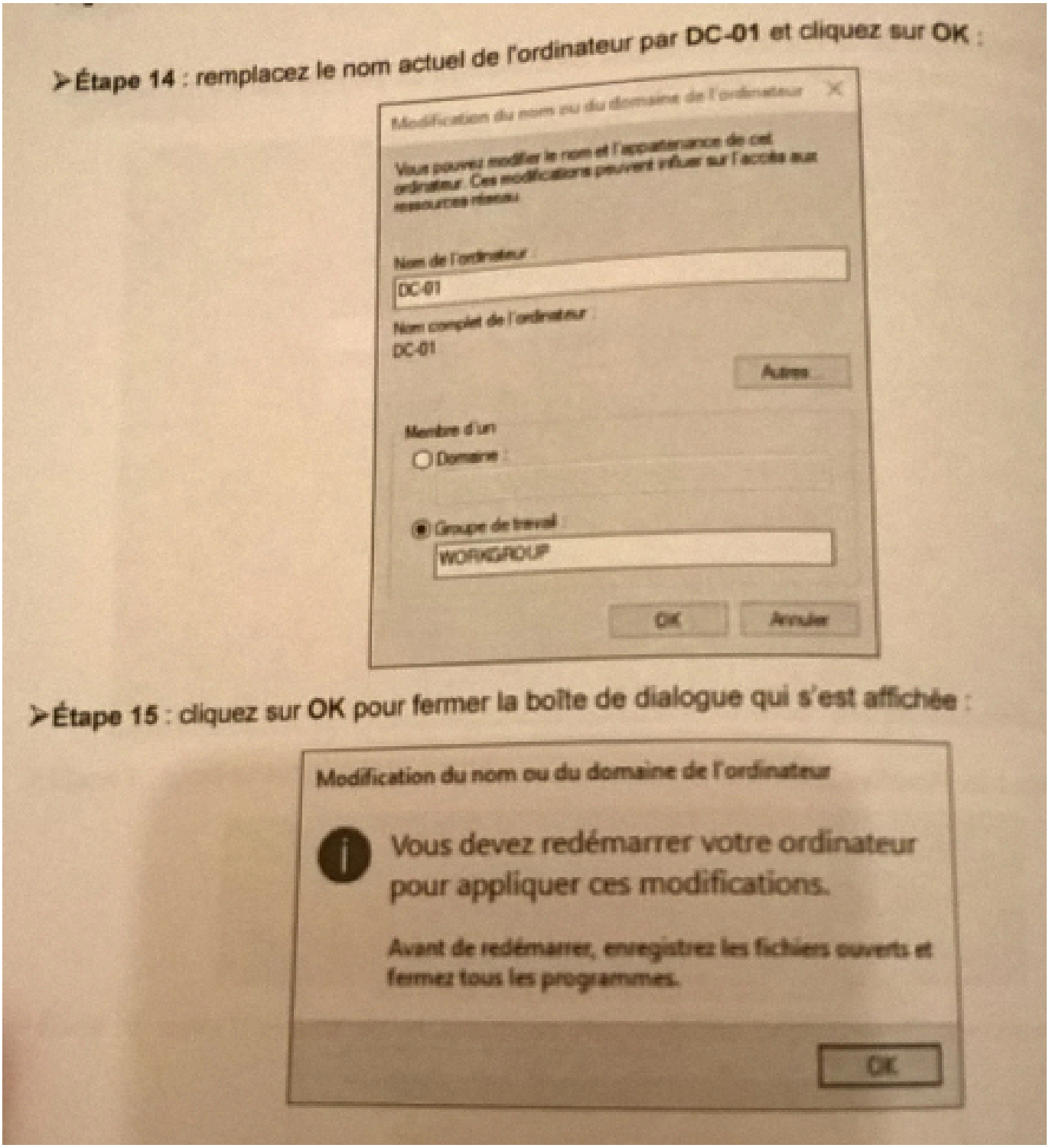
➢**Étape 12** : cliquez ensuite sur le nom du serveur :



➢**Étape 13** : cliquez sur **Modifier...** :

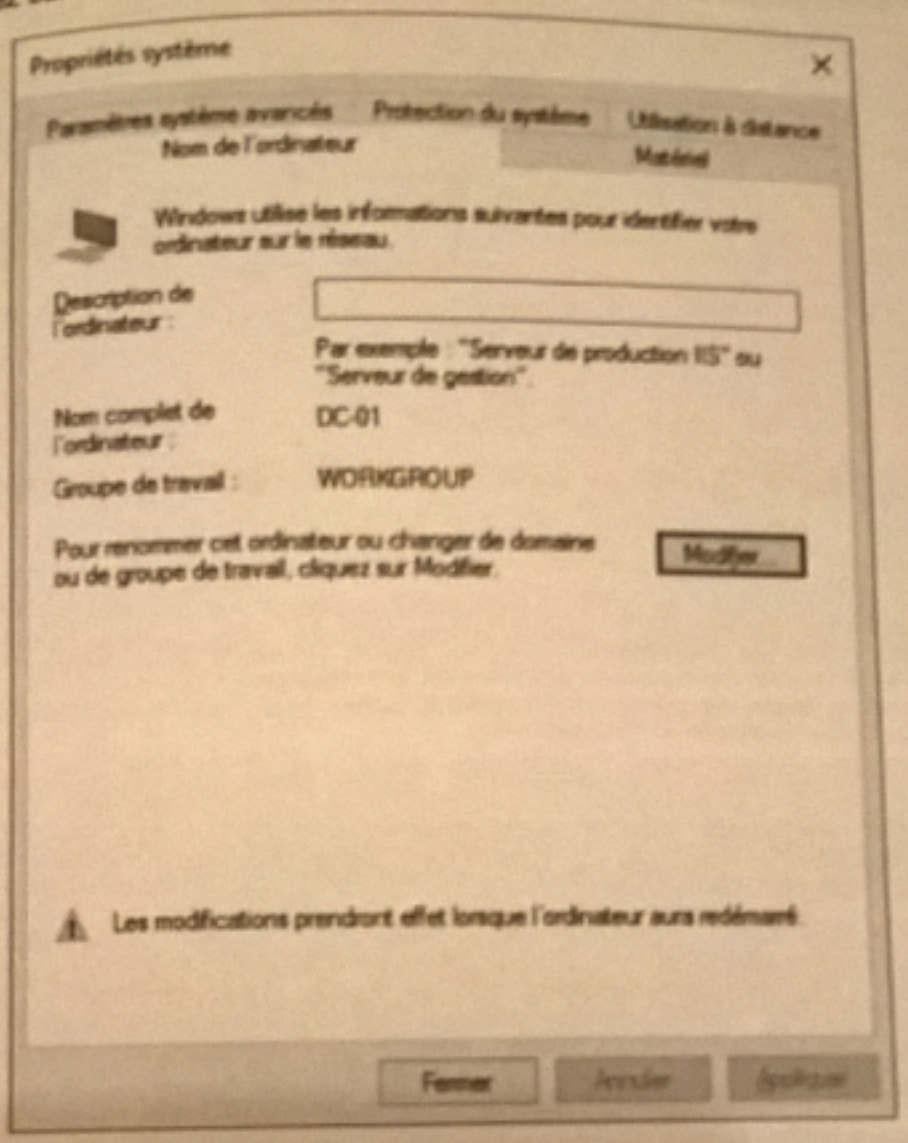


➢ **Étape 14** : remplacez le nom actuel de l'ordinateur par **DC-01** et cliquez sur **OK** :

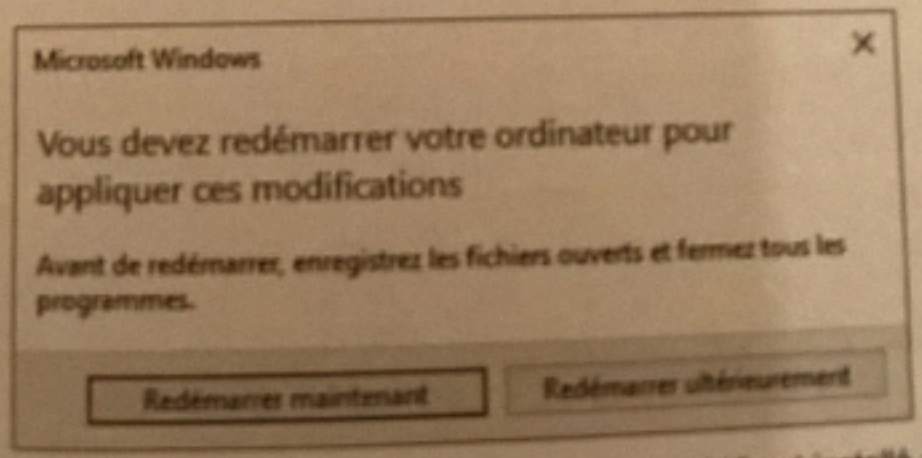


➢ **Étape 15** : cliquez sur **OK** pour fermer la boîte de dialogue qui s'est affichée :

➢Étape 16 : cliquez sur **Fermer** :



➢Étape 17 : cliquez sur **Redémarrer maintenant** :



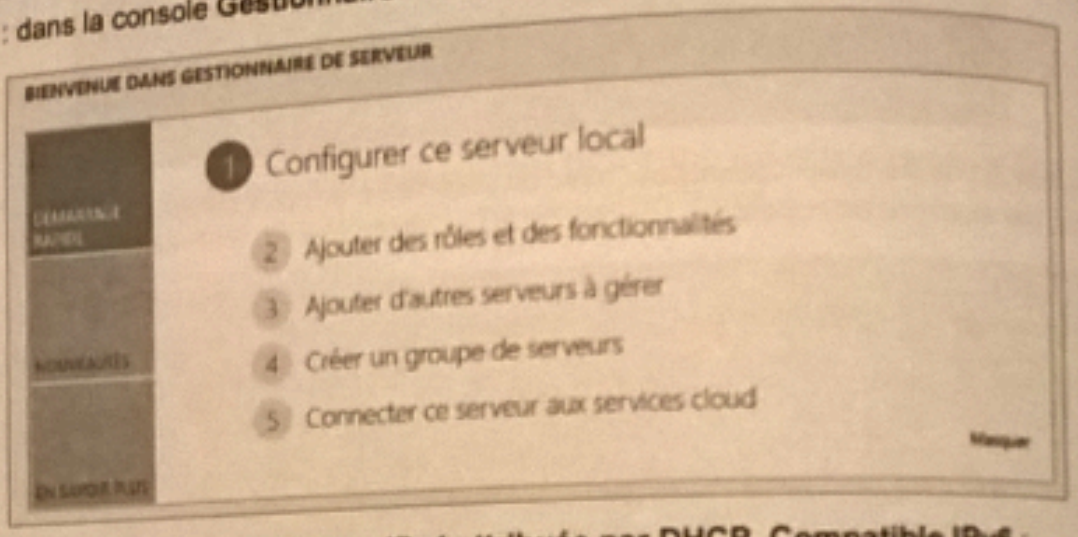
À ce stade, le système d'exploitation Microsoft Windows Server 2016 est installé avec l'interphique et dispose d'un nom conforme à la stratégie de nommage.

3. Configurer l'interface réseau

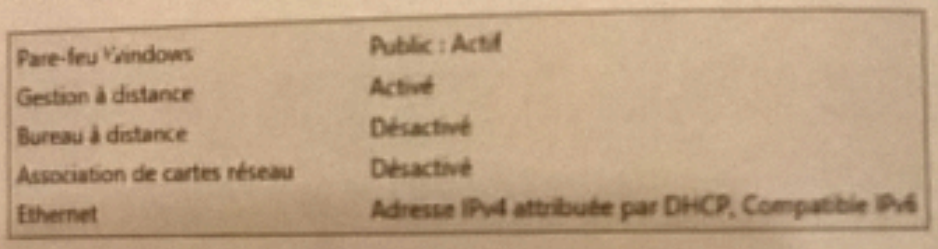
Dans ce TP, la configuration d'une interface réseau sera réalisée en mode graphique et en ligne de commande.

Configuration en mode graphique

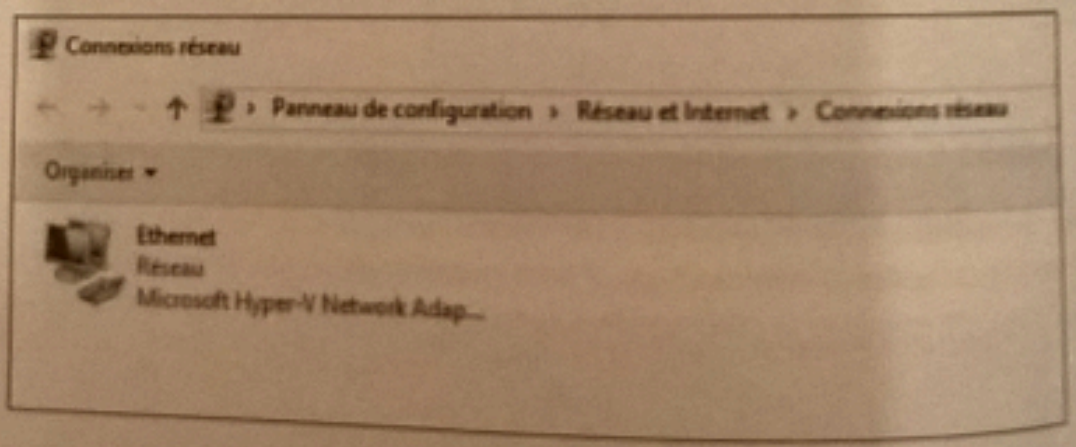
➢ **Étape 1** : dans la console **Gestionnaire de serveur**, cliquez sur **Configurer ce serveur local**



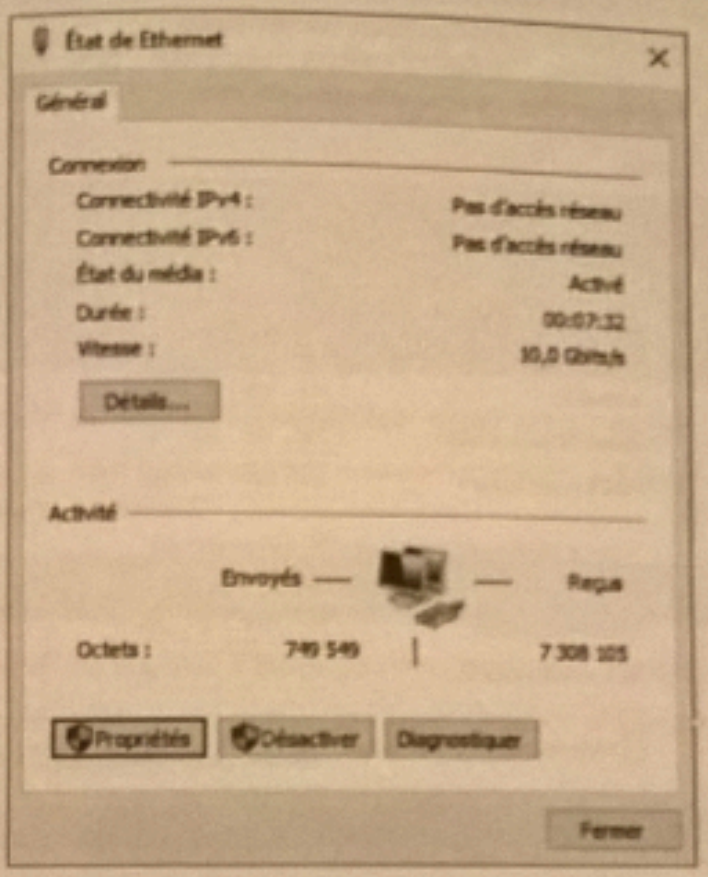
➢ **Étape 2** : cliquez ensuite sur **Adresse IPv4 attribuée par DHCP, Compatible IPv6** :



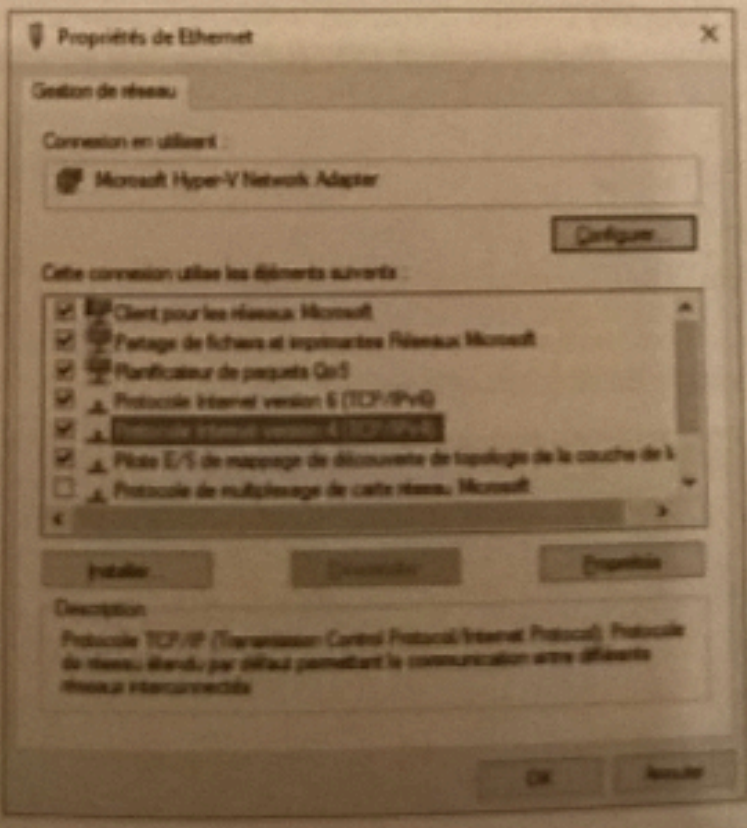
➢ **Étape 3** : double cliquez sur la carte réseau à configurer :



➢Étape 4 : cliquez sur **Propriétés** de la carte réseau sélectionnée :



➢**Étape 5** : sélectionnez le protocole réseau **TCP/IPv4** et cliquez sur **Propriétés** :



Etape 6

Cocher la case **Utiliser l'adresse IP suivante** et paramétrer votre carte réseau.

Adresse IP : 172.16.0.100
Masque de sous-réseau : 255.255.255.0
Passerelle par défaut : 172.16.0.254

Serveur DNS préféré : 172.16.0.100
Serveur DNS auxiliaire : 127.0.0.1 (adresse de loopback)

Cliquer sur ok, fermer la fenêtre des propriétés des cartes réseaux

Mission 2 Ajouter le service Active Directory

Compétences	
Objectif principal	Mettre en place le rôle AD DS Active Directory
Objectifs intermédiaires	Installer le rôle AD DS via l'interface graphique Installer le rôle AD DS sur une installation minimale
Vocabulaire à connaître	
Évaluation	Compte-rendu à rendre pour évaluation sommative coefficient 2 Compte-rendu est à poser dans votre PFC Épreuve E4 certificative

Votre mission

Ajouter le service Active Directory sur le contrôleur de domaine

Informations utiles

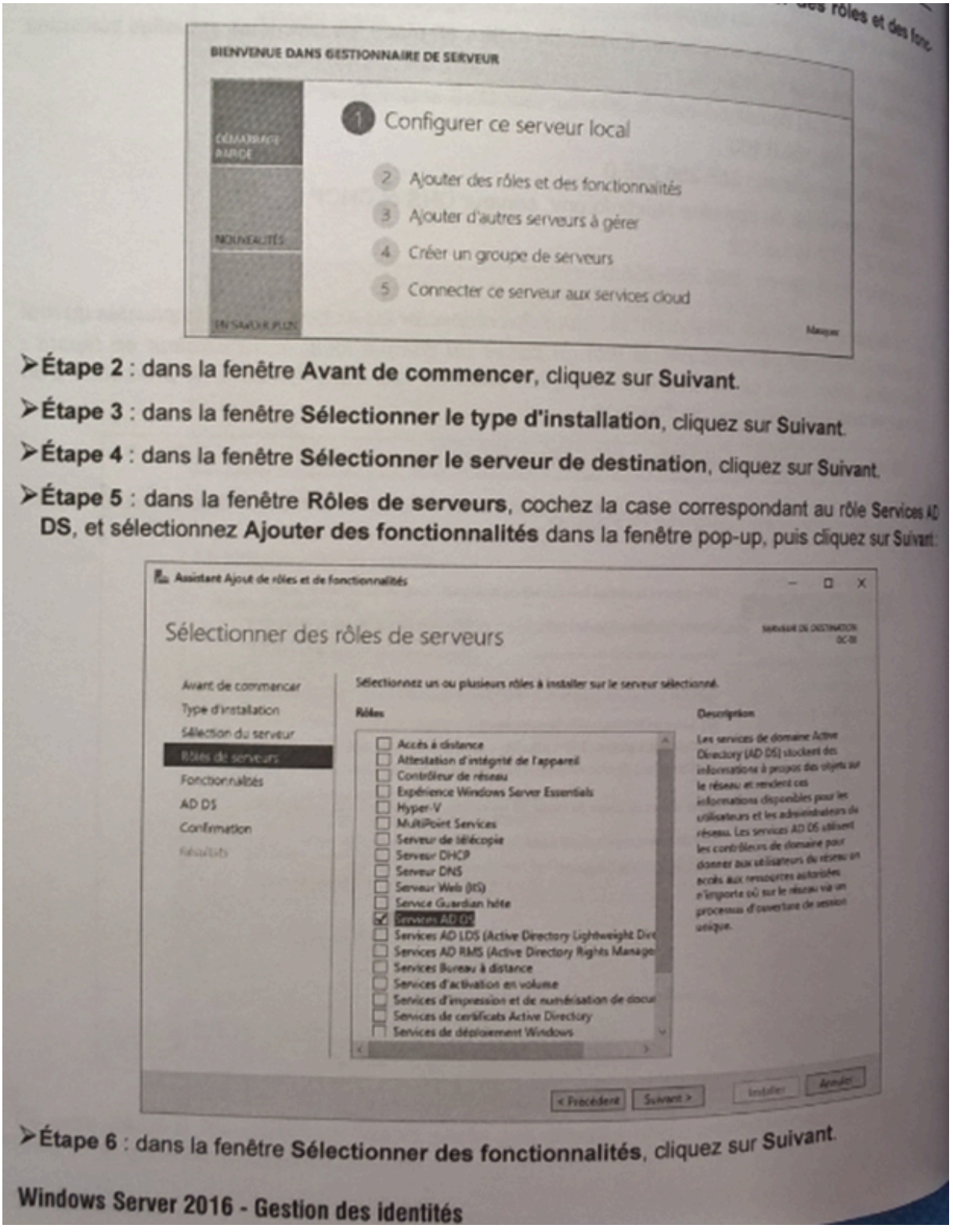
Ce serveur sera le contrôleur de domaine principal et contiendra les services suivants :

- Active Directory
- DNS
- DHCP

Adresse IP du serveur contrôleur de domaine : 172.16.0.100 / 24
Nom du domaine à gérer : webcourses.sio

Guide d'installation

Etape 1 : sur votre contrôleur de domaine, dans le gestionnaire de serveur, cliquer sur Ajouter des rôles et des fonctionnalités



➢ **Étape 2** : dans la fenêtre **Avant de commencer**, cliquez sur **Suivant**.

➢ **Étape 3** : dans la fenêtre **Sélectionner le type d'installation**, cliquez sur **Suivant**.

➢ **Étape 4** : dans la fenêtre **Sélectionner le serveur de destination**, cliquez sur **Suivant**.

➢ **Étape 5** : dans la fenêtre **Rôles de serveurs**, cochez la case correspondant au rôle **Services AD DS**, et sélectionnez **Ajouter des fonctionnalités** dans la fenêtre pop-up, puis cliquez sur **Suivant**.

➢ **Étape 6** : dans la fenêtre **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.

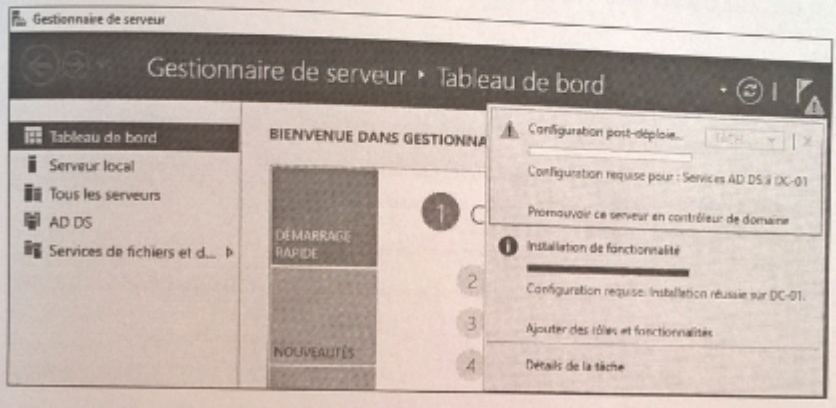
Windows Server 2016 - Gestion des identités

➢ **Étape 7** : dans la fenêtre **Services de domaine Active Directory**, cliquez sur **Suivant**.

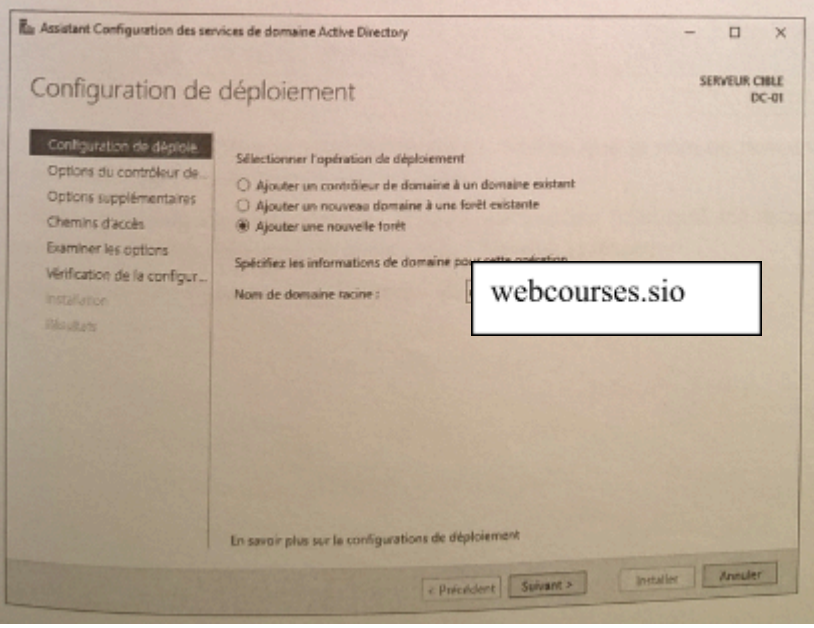
➢ **Étape 8** : dans la fenêtre **Confirmer les sélections d'installation**, cliquez sur **Installer**.

➢ **Étape 9** : dans la fenêtre **Progression de l'installation**, cliquez sur **Fermer**.

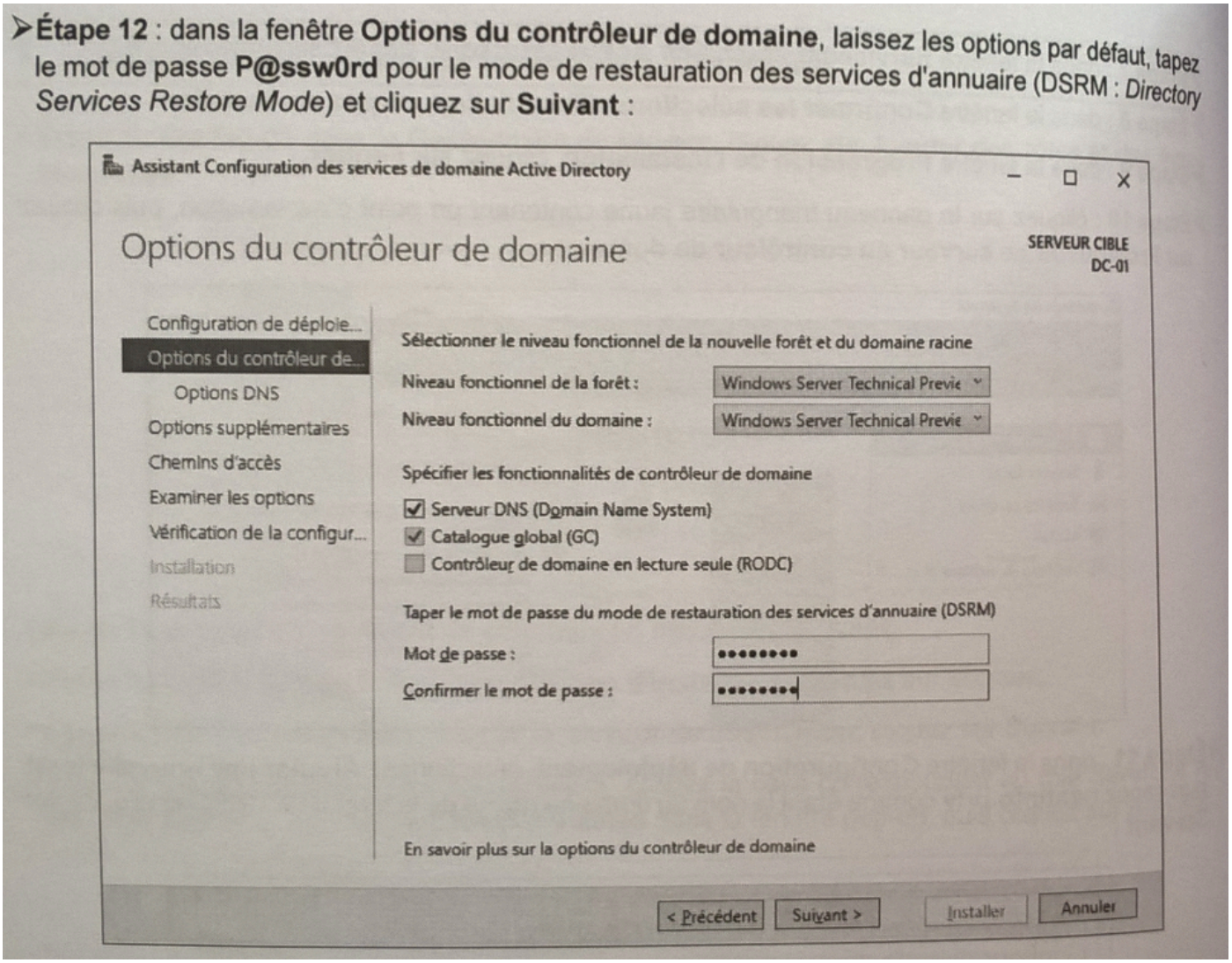
➢ **Étape 10** : cliquez sur le panneau triangulaire jaune contenant un point d'exclamation, puis cliquez sur **Promouvoir ce serveur en contrôleur de domaine** :



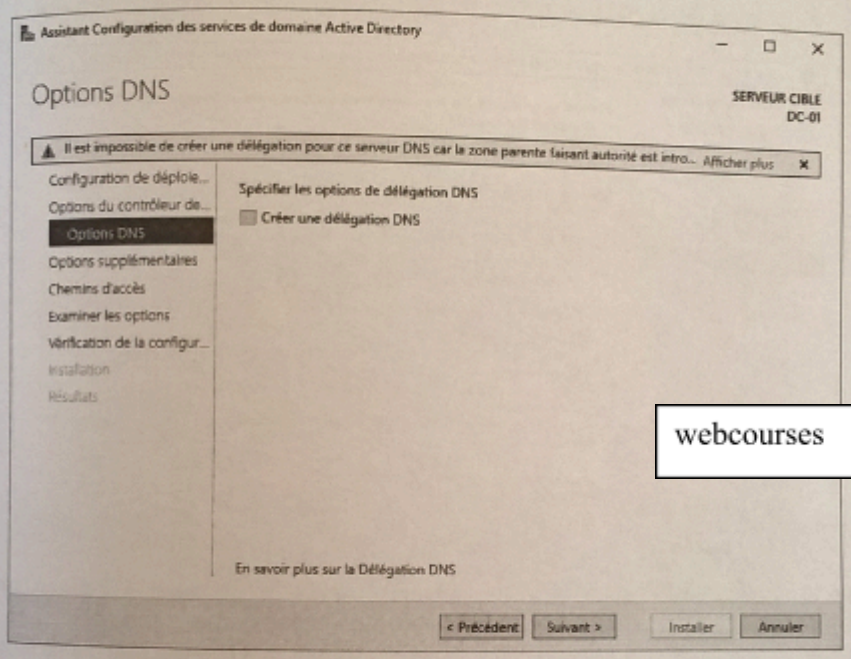
➢ **Étape 11** : dans la fenêtre **Configuration de déploiement**, sélectionnez **Ajouter une nouvelle forêt** puis tapez **nextinfo.priv** comme étant le nom du domaine racine de la forêt NEXTINFO et cliquez sur **Suivant** :



➢ **Étape 12** : dans la fenêtre **Options du contrôleur de domaine**, laissez les options par défaut, tapez le mot de passe **P@ssw0rd** pour le mode de restauration des services d'annuaire (DSRM : *Directory Services Restore Mode*) et cliquez sur **Suivant** :



➢ **Étape 13** : dans la fenêtre **Options DNS**, ignorez le message d'erreur indiquant qu'il est impossible de créer une délégation pour ce serveur DNS. À ce stade, aucune zone de recherche directe n'a été créée, donc il est normal qu'il ne puisse y avoir de délégation sur une zone existante. Cliquez sur **Suivant** :

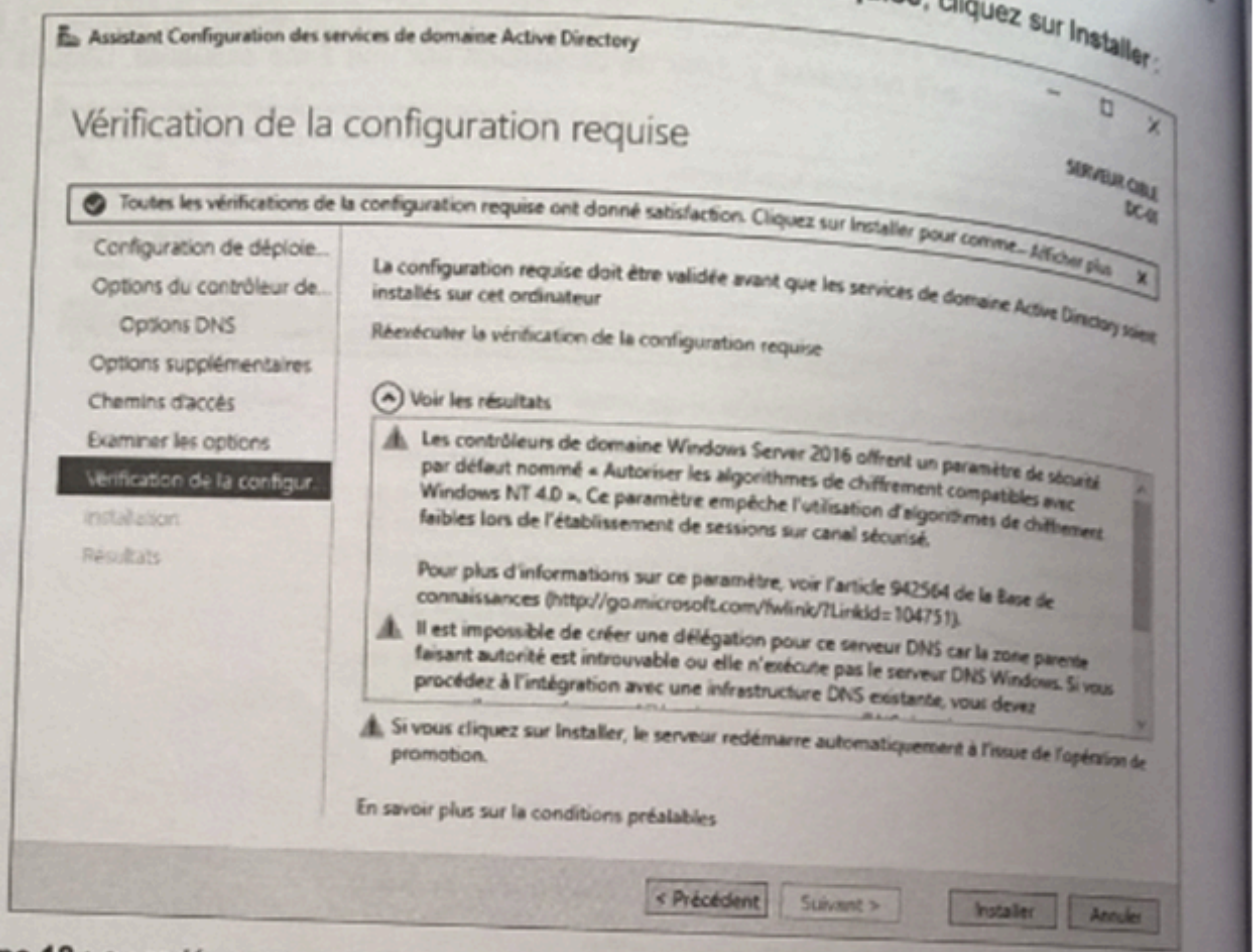


➢ **Étape 14** : dans la fenêtre **Options supplémentaires**, vérifiez que le nom de domaine NetBIOS affiché est bien NE[redacted], puis cliquez sur **Suivant**.

➢ **Étape 15** : dans la fenêtre **Chemin d'accès**, cliquez sur **Suivant** (bien qu'il soit recommandé de spécifier des emplacements différents du lecteur hébergeant le système).

➢ **Étape 16** : dans la fenêtre **Examiner les options**, cliquez sur **Suivant**.

➢**Étape 17** : dans la fenêtre **Vérification de la configuration requise**, cliquez sur **Installer** :



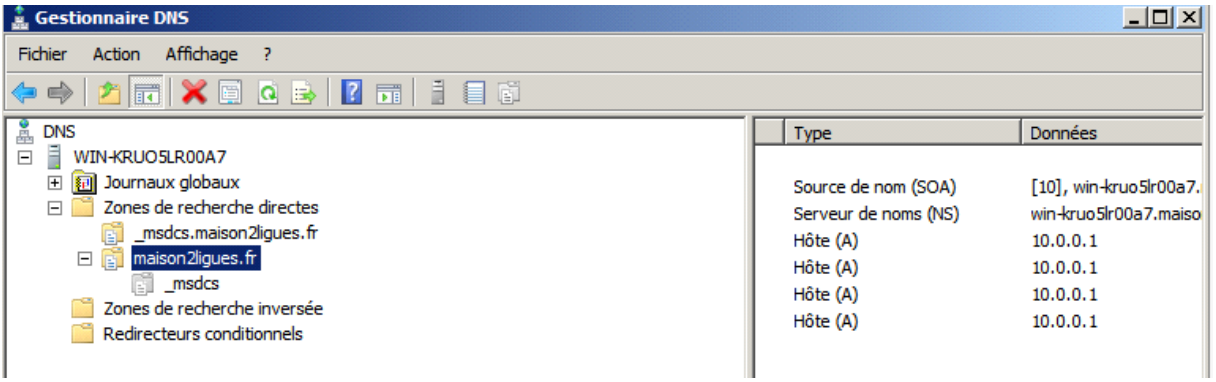
➢**Étape 18** : au redémarrage du serveur, ouvrez une session sur le domaine N[redacted] en tapant le login [redacted]**D\Administrateur** et le mot de passe **P@ssw0rd**.

webcourses

À ce stade, votre premier contrôleur de domaine pour la société [redacted] été créé via l'interface graphique. Un nouvel onglet nommé AD DS apparaît désormais dans le tableau de bord de la console **Gestionnaire de serveur**. Vous pouvez accéder aux outils d'administration et gérer votre contrôleur de domaine au travers du composant logiciel enfichable **dsa.msc**, disponible dans le menu Démarrer Windows Server 2016, sous le nom **Utilisateurs et ordinateurs Active Directory**.

Vérifier le DNS

- Au redémarrage : Menu > Démarrer > Outils d'administration > Dns.
- Vérifier que la Zone correspondant au nom du domaine a bien été créée ainsi que la Zone "_Msdcs.nom du domaine".



- Vérifier aussi que l'enregistrement «Hôte (A) » avec le nom de l'ordinateur y figure avec son adresse IP.

- Si ce n'est pas le cas, s'assurer que le serveur est bien client DNS de lui-même dans les propriétés IP de la carte réseau et forcer un réenregistrement avec la commande

- **ipconfig / RegisterDNS**. Ou bien vous pouvez forcer par désactiver et Activer la carte réseau.

Mission 3 Paramétrer Active Directory

Compétences	
Objectif principal	**Créer** et **gérer** des objets de stratégies de groupe
Objectifs intermédiaires	**Créer** l'arborescence d'unité d'organisation et les comptes AD **Créer** une GPO d'installation logiciel **Créer** des préférences de stratégie de groupe
Vocabulaire à connaître	Compte-rendu à rendre pour évaluation sommative coefficient 2 Compte-rendu est à poser dans votre PFC Épreuve E4 certificative
Évaluation	

Votre mission

Paramétrer Active Directory

Informations utiles

Présentation de l'outil d'administration "Utilisateurs et ordinateurs Active Directory"

Menu > Démarrer > Outils d'administration > Utilisateurs et ordinateurs

La console 'Utilisateurs et ordinateurs Active Directory' gère les objets de comptes de **domaine**. Les objets Active Directory sont gérés au niveau du domaine.

Placer sur votre bureau un raccourci pour accéder à Active Directory. (Programme Démarrer / outils d'administration / Utilisateurs et ordinateurs Active Directory).

Lancer ce programme. Vous ouvrez une console qui vous propose tous les objets sous forme d'une arborescence qui contient les dossiers suivants :

- **Builtin** : les groupes par défaut avec une étendue de domaine local.
- **Computers** : les comptes d'ordinateurs des stations clientes appartenant au domaine.
- **Domain Controllers** : les contrôleurs de domaine du domaine Windows 2000.
- **ForeignSecurityPrincipals** : stocke les identificateurs de sécurité (SID) associés à es objets externes de domaines approuvés.
- **Users** est le conteneur par défaut des utilisateurs du domaine.

Guide d'installation

1. Gérer des comptes utilisateurs

1.1. Déclaration des unités d'organisation et groupes

Pour pouvoir déclarer un compte utilisateur, il faut que les unités d'organisation soient créées. D'après le tableau ci-dessous, on peut remarquer d'après la colonne unité d'appartenance, qu'il faudra créer 5 unités d'organisation et 3 groupes spécifiques selon la catégorie.

1.1.1. Création d'une unité logique d'organisation

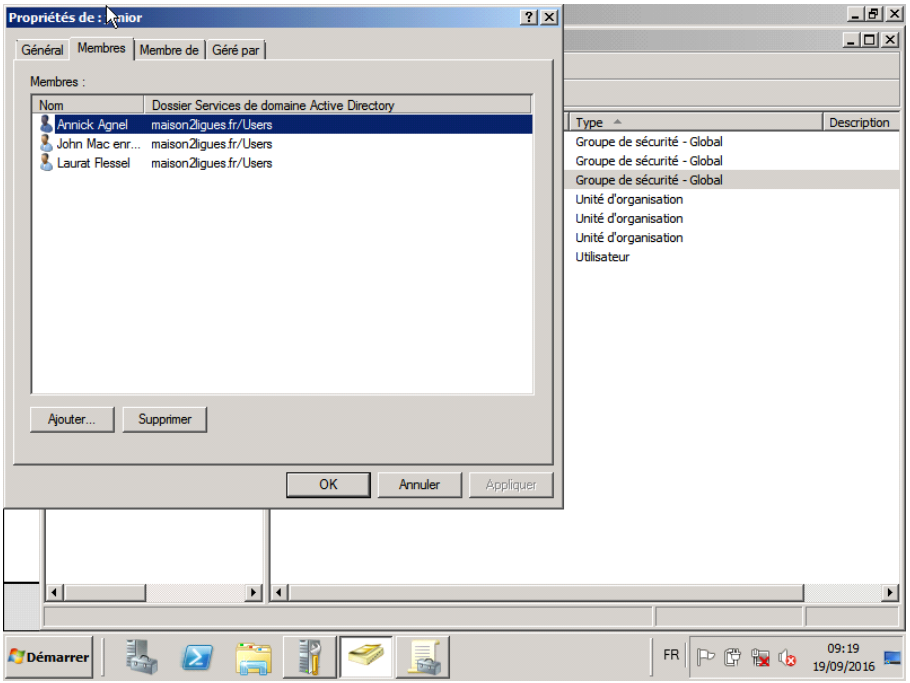
- Dans la console AD, Clic droit sur le nom du domaine,
- cliquer sur Nouveau - Unité d'organisation.

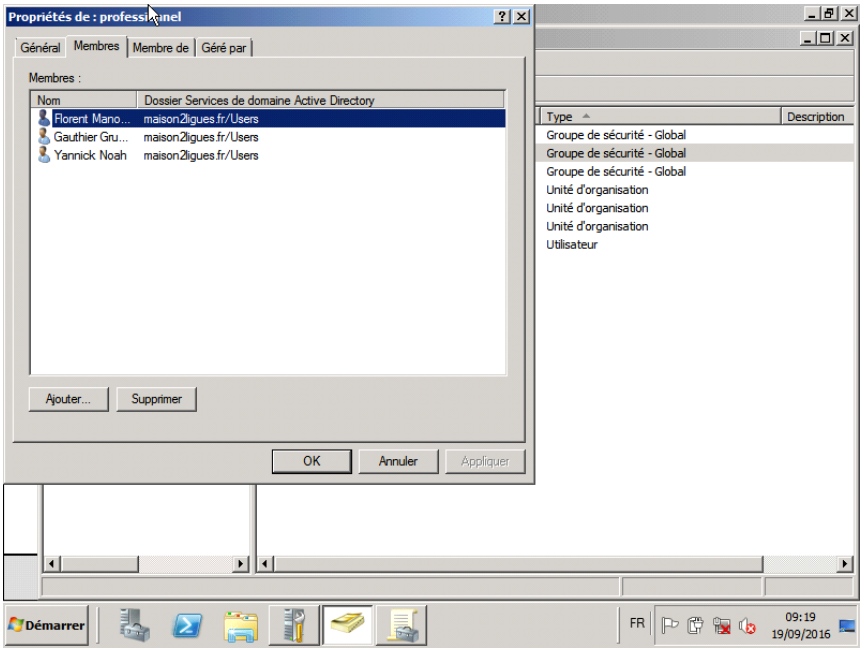
1.1.2. Création d'un groupe

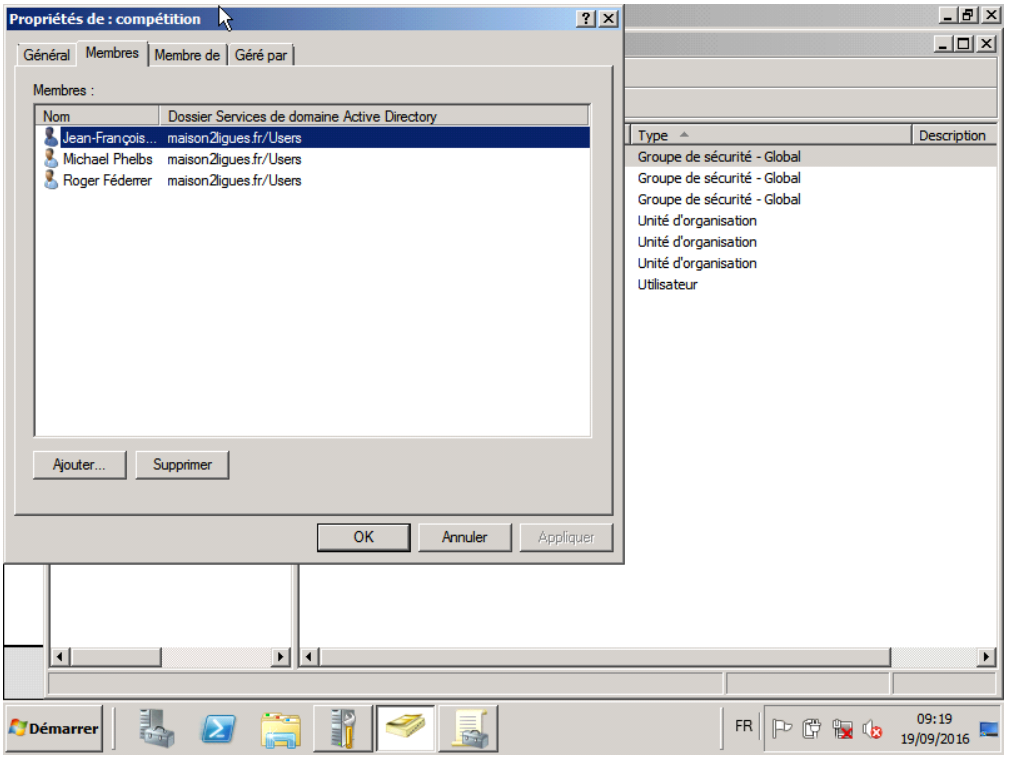
- Dans la console AD, Clic droit sur le nom du domaine,
- Créer les groupes dans l'UO adéquat
- Clic droit sur le conteneur,
- cliquer sur Nouveau - Groupe,
- spécifier le nom du groupe et son étendue.

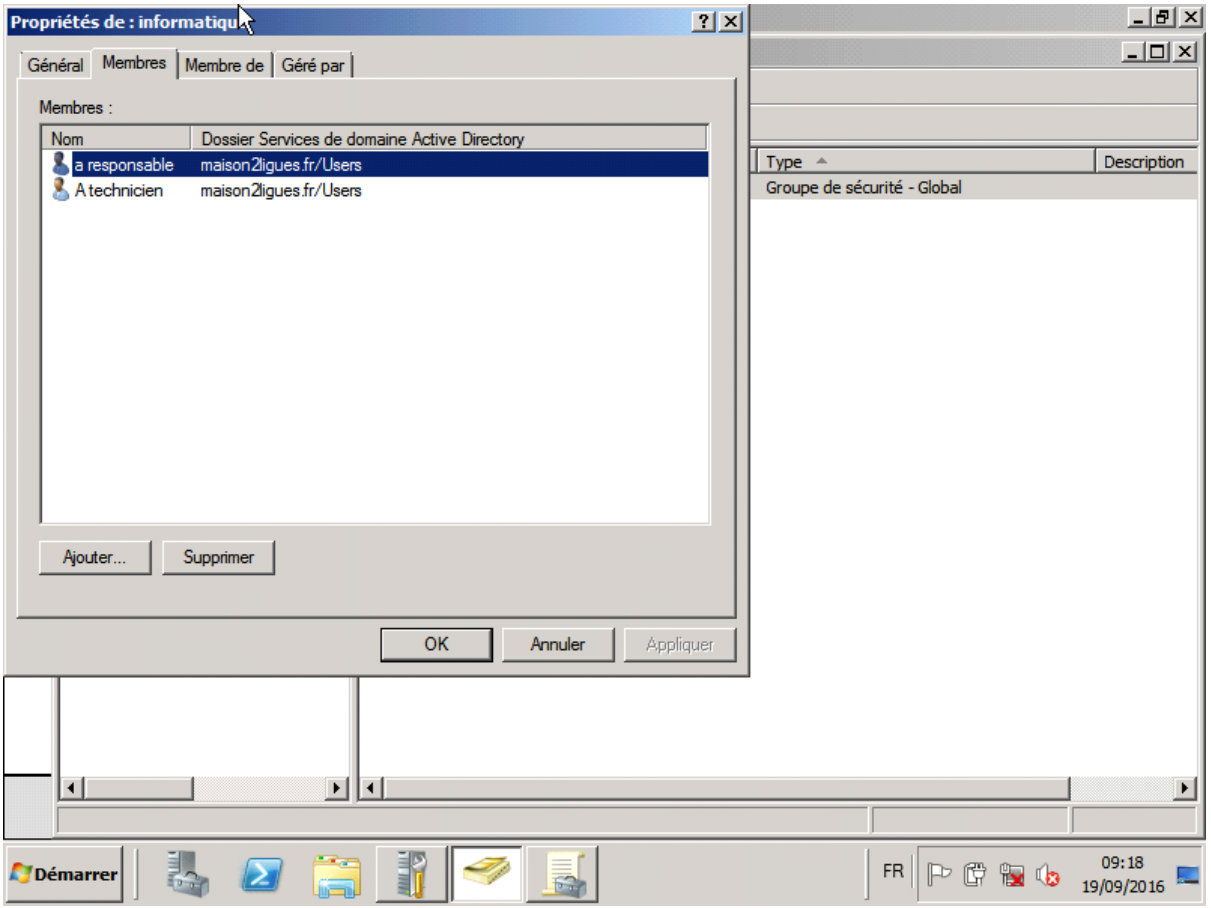
1.1.3. Ajouter des membres à un groupe

- Clic droit sur le groupe
- Propriétés / onglet Membres, bouton Ajouter
- Bouton Type d'objet : choisir le type d'objet puis OK
- Bouton Avancé : construire une requête ET/OU bouton rechercher
- Choisir les utilisateurs à ajouter au groupe.




Propriétés de : professionnel
Général
Membres
Membre de
Géré par
Membres :
Nom
Dossier Services de domaine Active Directory
Florent Mano...
maison2ligues.fr/Users
Gauthier Gru...
maison2ligues.fr/Users
Yannick Noah
maison2ligues.fr/Users
Ajouter...
Supprimer
OK
Annuler
Appliquer
Type
Description
Groupe de sécurité - Global
Groupe de sécurité - Global
Groupe de sécurité - Global
Unité d'organisation
Unité d'organisation
Unité d'organisation
Utilisateur
Démarrer
FR
09:19
19/09/2016


Propriétés de : compétition
Général
Membres
Membre de
Géré par
Membres :
Nom
Dossier Services de domaine Active Directory
Jean-François...
maison2ligues.fr/Users
Michael Phelps
maison2ligues.fr/Users
Roger Féderer
maison2ligues.fr/Users
Ajouter...
Supprimer
OK
Annuler
Appliquer
Type
Description
Groupe de sécurité - Global
Groupe de sécurité - Global
Groupe de sécurité - Global
Unité d'organisation
Unité d'organisation
Unité d'organisation
Utilisateur
Démarrer
FR
09:19
19/09/2016



1.2. Déclaration des comptes

- Rentrer en tant qu'administrateur dans AD.
- Aller dans Outils d'administration – utilisateur et ordinateur Active Directory – users – nouveau – utilisateur
- Créer les comptes utilisateurs suivants

Compte utilisateur	Unité d'appartenance	catégorie	
Geraint Thomas	vélo	Professionnel vélo	
Dylan van Baarle		Compétition vélo	
Raymond Poulidor		Senior vélo	
Annick Agnel	Natation	Compétition Natation	
Florent Mandou		professionnel Natation	
Michael Phelbs		Senior Natation	
Maurice Greene	Course à pied	Senior Course à pied	
Christian Coleman		Compétition Course à pied	
Nesta Carter		professionnel Course à pied	
A technicien	Informatique	Informatique	Cela signfie qu'il est rattaché directement à l'UO informatique

A responsable		Informatique	Cela signfie qu'il est rattachée directement à l'UO informatique
PDG	Administration	Toute catégorie	Cela signfie qu'il est rattachée directement au domaine webcourses.sio
Adhérent1	Vélo	Adhère1	Cela signfie qu'il est rattachée directement à l'UO vélo
Adhérent2	Natation	Adhère2	Cela signfie qu'il est rattachée directement à l'UO natation
Adhérent3	Course à pied	Adhère3	Cela signfie qu'il est rattachée directement à l'UO course à pied

1.3. Contraintes liées au compte

Chaque utilisateur devra se connecter par le login suivant :

- Première lettre du prénom, nom complet
- Mot de passe: Azerty15*
- Attention : la stratégie de mot de passe est activée – respecter le format demandé
- **COCHER L'utilisateur ne doit pas changer son mot de passe**
- Faites en sorte que les utilisateurs puissent se connecter seulement de 8h à 18h sauf les informaticiens
- faire un test de connexion pour vérifier l'autorisation des horaires

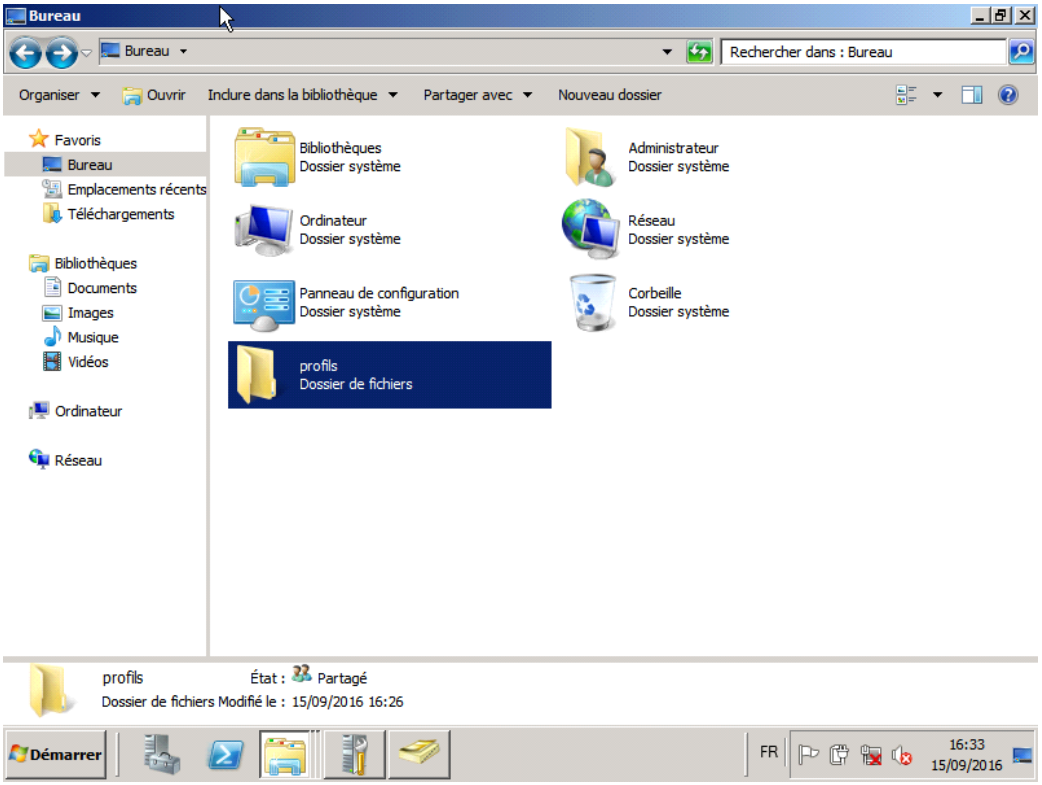
1.4. Gérer des profils en fonction des utilisateurs

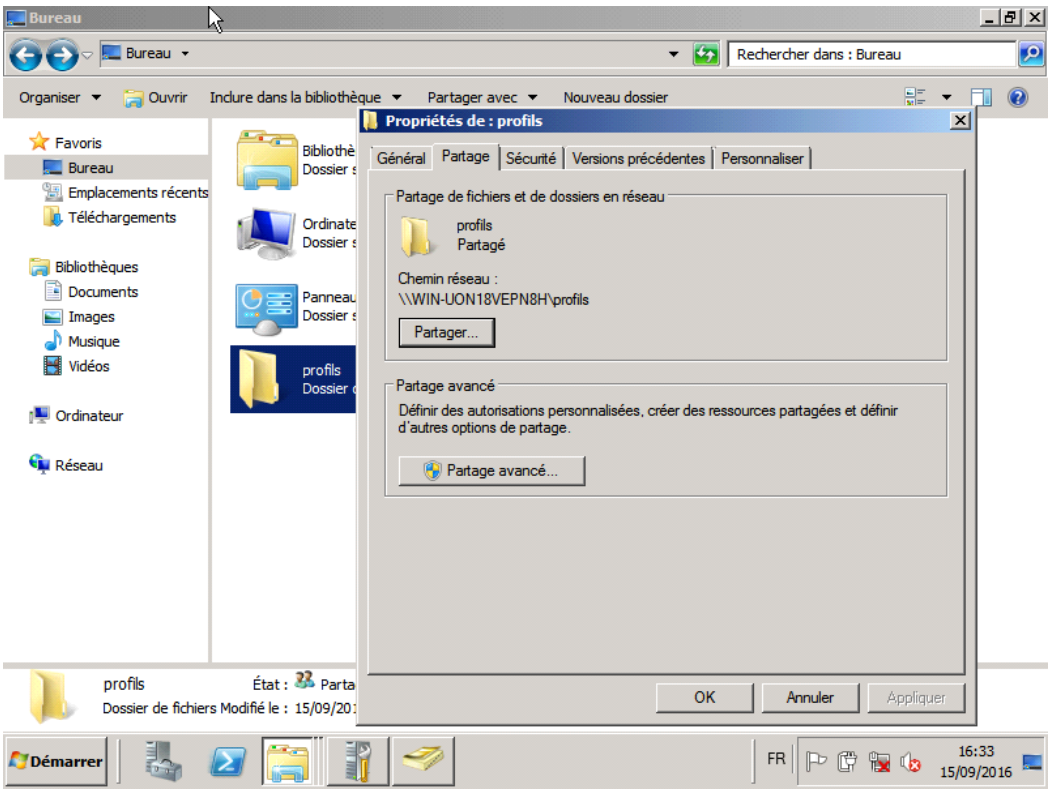
1.4.1. Définition

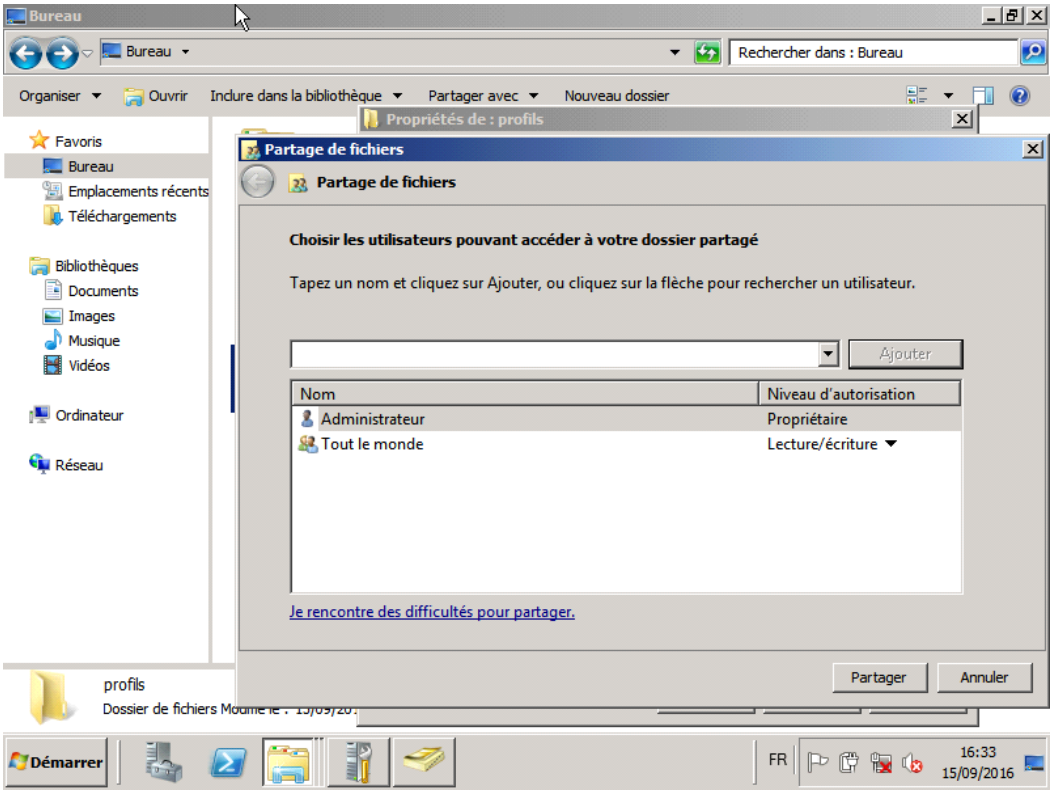
- Un profil utilisateur est un ensemble de documents stockés dans un dossier portant le nom d'ouverture de session de l'utilisateur. Le profil est dit local lorsqu'il est enregistré sur le poste client.
- Pour que l'utilisateur retrouve son environnement de travail quel que soit le poste d'ouverture de session, le profil doit être enregistré sur le serveur.
- On parle de **profil errant**.

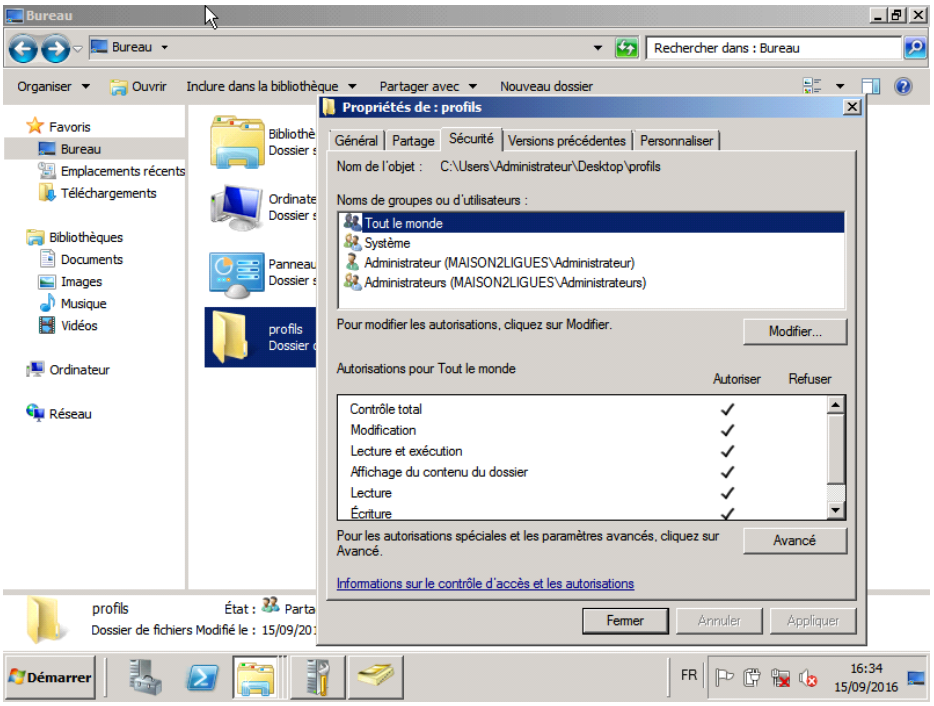
1.4.2. Manipulations

- Sur le bureau, créez un dossier nommé ***Profils*** qui contiendra tous les profils des utilisateurs créés
- partagez-le en conservant le nom de partage par défaut.
- modifiez les autorisations de **partage** (onglet partage et sécurité) en donnant le contrôle d'accès à tout le monde.


Bureau
Bureau
Rechercher dans : Bureau
Organiser
Ouvrir
Inclure dans la bibliothèque
Partager avec
Nouveau dossier
Favoris
Bureau
Emplacements récents
Téléchargements
Bibliothèques
Documents
Images
Musique
Vidéos
Ordinateur
Réseau
Bibliothèques
Dossier système
Administrateur
Dossier système
Ordinateur
Dossier système
Réseau
Dossier système
Panneau de configuration
Dossier système
Corbeille
Dossier système
profils
Dossier de fichiers
profils
État : Partagé
Dossier de fichiers Modifié le : 15/09/2016 16:26
Démarrer
FR
16:33
15/09/2016


Bureau
Rechercher dans : Bureau
Organiser
Ouvrir
Inclure dans la bibliothèque
Partager avec
Nouveau dossier
Propriétés de : profils
Général
Partage
Sécurité
Versions précédentes
Personnaliser
Partage de fichiers et de dossiers en réseau
profils
Partagé
Chemin réseau :
\\WIN-UON18VEPN8H\profils
Partager...
Partage avancé
Définir des autorisations personnalisées, créer des ressources partagées et définir d'autres options de partage.
Partage avancé...
OK
Annuler
Appliquer
Favoris
Bureau
Emplacements récents
Téléchargements
Bibliothèques
Documents
Images
Musique
Vidéos
Ordinateur
Réseau
profils
Dossier de fichiers Modifié le : 15/09/20
Démarrer
FR
16:33
15/09/2016





Dans la console AD, **créez des profils errants pour tous vos utilisateurs**

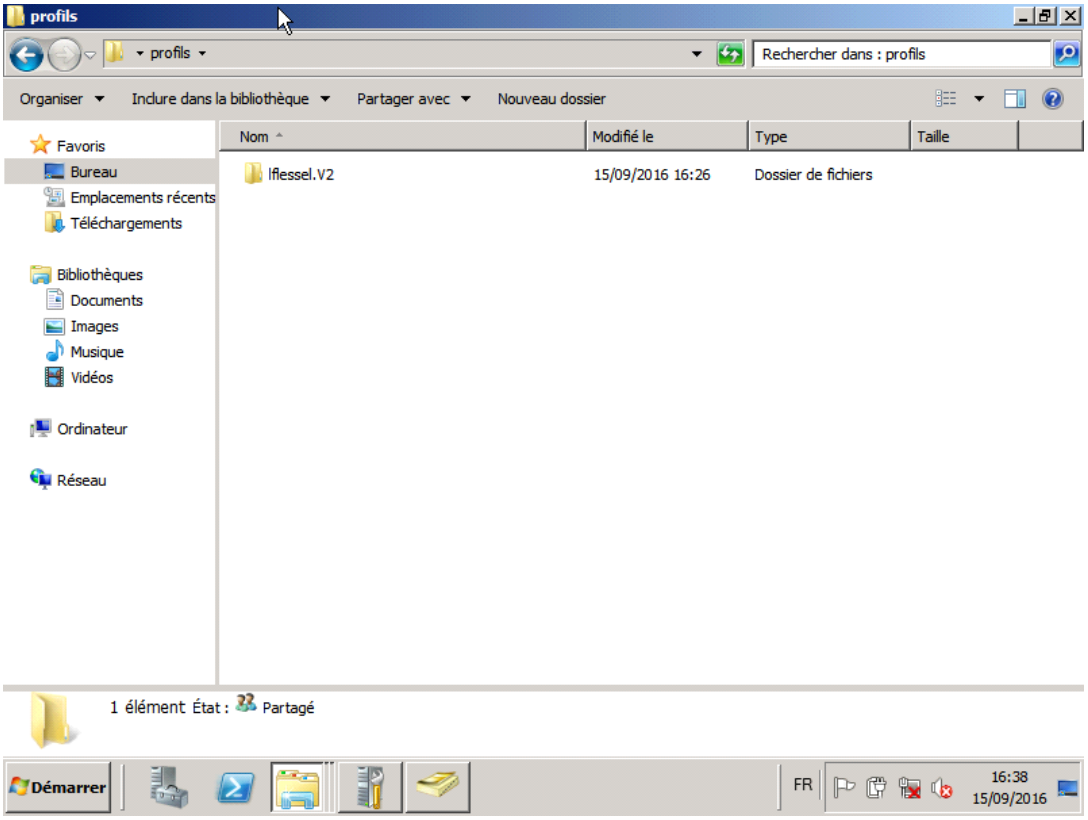
- double clic sur l'utilisateur concerné, Onglet Profils,
- saisir le chemin menant au profil de l'utilisateur :

\\nom_machine_contrôleur_du_domaine\Profils\%username%

- Ouvrez une session cliente avec un compte utilisateur sur le poste client

- A partir de ce compte, modifier l'arrière-plan du poste, ajoutez un icône sur le bureau puis fermer la session.

- ouvrez une session Administrateur de domaine
- Vérifier que dans le dossier ***Profil*** un répertoire a bien été créé pour votre compte utilisateur



ON EST ICIA1111111111111111111111111111111111111111111111111111111111111

- Vérifiez que les profils sont bien errants, Pour cela, sur le poste client rouvrez une session avec le compte utilisateur et vérifiez que vous retrouvez bien votre profil itinérant à savoir les mises à jour effectuées plus haut.
- fermez votre session

1.5. Gestion des dossiers personnels

Chaque utilisateur peut disposer d'un dossier personnel sur le serveur

- créer sur le bureau de votre serveur AD un dossier nommé ***Private*** qui contiendra tous les dossiers personnels des utilisateurs et partager-le en conservant le nom de partage par défaut.
- Créer le lecteur réseau correspondant sur le serveur AD
- Aller sur le compte utilisateur et affichez ses propriétés, onglet Profils

- Dans la partie Dossier de base, connecter à, choisir une lettre et indiquer *nom_machine_contrôleur_du_domaine*\ Private\%username%

    - Tester l'accès au dossier personnel

2. Ajouter une machine au domaine

Comme votre DNS Local se trouve sur votre contrôleur de domaine, indiquez l'adresse de cette machine dans la zone DNS pour votre station cliente.

- On doit créer des comptes d'ordinateur pour pouvoir mettre en place une administration centralisée, que ce soit par le biais d'une prise en main à distance ou à travers l'application des stratégies de groupe.
- On peut procéder de deux manières. Soit on crée d'abord l'objet « Ordinateur » dans l'OU où il va être géré. Soit l'objet « Ordinateur » sera créé automatiquement lors de l'ajout au domaine.

Pour joindre une station au domaine, il faut se connecter au poste client en tant qu'administrateur

- Se connecter à la machine cliente (Windows XP ou 7)
- « Démarrer > Ordinateur », sélectionner « Propriétés »
- Dans la fenêtre « Système » Sélectionner « Paramètres système avancés » Sélectionner l'onglet
« Nom de l'ordinateur »
- Renommer l'ordinateur si n'a pas été déjà fait et taper ensuite le nom du domaine **webcourses** auquel il doit être ajouté
- Le système vous demande une authentification s authentifier en tant qu'administrateur de ce domaine.
- Redémarrer la machine

- Ouvrir une session d'une machine cliente
- Utiliser les comptes créés plus haut pour vérifier qu'on peut ouvrir la session sur le domaine webcourses

3. Création de script pour la maintenance

3.1. Pourquoi des scripts avec AD ?

Utiliser les interfaces graphiques pour créer les comptes utilisateurs est une technique convivial mais peu pratique quand il s'agit de créer beaucoup de comptes utilisateurs à la fois. Aussi la création en masse à la main peut induire des erreurs de saisie par exemple ; la création à la main prend énormément de temps, et présente un travail très fastidieux.

Le script permet de remplir ce rôle rapidement et efficacement. Il existe plusieurs langages permettant de concevoir et exécuter un script, ne citons que les plus courants : WSH, Visuel

basic, DOS… Powershell, le plus simple mais pas moins efficace est celui qui utilise les commandes DOS. C'est ce dernier que nous allons utiliser dans notre STS.

La commande **DSADD** permet de créer une multitude d'objets dans un domaine Microsoft tels que les Unités d'Organisation, groupes, comptes utilisateurs…etc.

3.2. Mise en place du script de chargement d'un lecteur réseau

Chaque utilisateur doit avoir accès **lors du démarrage de sa session** au lecteur réseau suivant de sa catégorie.
Par exemple, Laurat Flessel devra avoir accès au lecteur E mais pas aux autres lecteurs,
Seul le PDG devra pour accéder à tous les réseaux.

Répartition des lecteurs réseaux :

- Pour la ligue de natation : lecteur réseau N
- Pour la ligue de escrime : lecteur réseau E
- Pour la ligue de tennis : lecteur réseau T

Pour cela, créer 3 dossiers partagés nommés natation, escrime, tennis sur le bureau.
Créer un fichier **.bat**. en utilisant ces commandes :

- Pour connecter un lecteur réseau, utilisez la commande :
  net use X: \\nom-machine_contrôleur_domaine\nom_du_dossier_partagé
  où X: est la lettre de lecteur que vous souhaitez affecter à la ressource partagée.

  - Poser votre script dans la directory
    C:\Windows\SYSVOL\sysvol\<nom_domaine>\scripts
  - Aller sur le compte utilisateur et affichez ses propriétés, onglet Profils. Dans la partie script de connexion, indiquer le nom de votre script.

  - Tester le montage du lecteur réseau pour chacune des ligues.

3.3. Création de scripts pour alimenter la base AD en cas de forte volumétrie

- **Phase 1**

Créer un script **basuser.bat** **dynamique** qui créera un fichier texte appelé **user.txt** contenant les informations relatives aux comptes utilisateurs à savoir :

Compte_utilisateur, nom_de_la_ligue_d'appartenance, mot_de_passe, groupe_d'appartenance

Contraintes :

- Créer au minimum 3 nouveaux adhérents
- Utiliser des variables
- Sortir proprement du script

- Indiquer la procédure de saisie à l'utilisateur
- Générer un fichier de log contenant la date, heure et le contenu de l'enregistrement traité

Rappel de la procédure de création de script :

- Ouvrir le bloc note
- Saisir dans le bloc note les lignes de commandes du tableau colonne de gauche ci-dessous
- Sauvegarder votre fichier en le nommant nom_du_fichier.bat
- Tester le script et vérifier le résultat obtenu

- **Phase 2**

Concevoir un deuxième script nommé **chargead.bat dynamique,** permettant de créer dans le groupe **adherent** relié à l'unité d'organisation **Ligue**, les nouveaux comptes utilisateurs et ce à partir des informations stockées dans le fichier **user.txt**.

Contraintes

- Utiliser des variables
- Vérifier que l'unité d'organisation Ligue existe
- Si oui afficher un message sinon la créer à l'aide de la commande DSADD UO
- Créer le nouveau groupe à l'aide de la commande DSADD groupe
- S'il existe déjà afficher un message sinon le créer dans la base de données.
- Créer les comptes utilisateur à l'aide de la commande DSADD user
- Positionner l'attribut –disabled no pour chaque compte utilisateur
- Utiliser la commande DSQUERRY pour afficher le contenu de la base de données
- Générer un fichier de log contenant la date, heure et le contenu de l'enregistrement traité

Rappel :

Pour lire séquentiellement les informations contenues dans un fichier texte, utiliser la commande :

For /f "tokens=nombre_de_colonne_à_traiter delims=séparateur_de_données" %%a in (chemin d'accès:\nom du fichier) DO (création des comptes utilisateurs)

Et la commande générale de création des comptes utilisateurs est :

Dsadd user "CN=nom_utilisateur, OU=nom_unité_organisation, DC=nom_sous_domaine, DC=nom_domaine" - pwd mot_de_passe -memberof CN=nom_du groupe –disabled no

4. Mise en place des stratégies de groupe dans le domaine

Il s'agit de mettre en place les stratégies de groupes Windows ou GPO (Group Policy Object) :
Les trois phases de la création d'une GPO sont les suivantes :

- Création de la GPO
- Liaison de la GPO
- Application de la GPO

4.1. Création des GPO

- La console gpedit.msc (à lancer depuis Démarrer > Exécuter) permet d'éditer individuellement les stratégies de groupes locales.
- Cette console existe pour tous les Windows y compris les versions clientes.
- Elle permet une gestion centralisée des GPO dans Active Directory.
- On peut aussi la trouver dans le menu :
- Outils d'administration > Gestion des stratégies de groupe.

4.2. Liaison des stratégies de groupe

- Après avoir créé une stratégie de groupe, elle doit être liée à AD, à un domaine ou à une UO.
- Attention, les objets enfants d'Active Directory héritent des objets parents !
- Un utilisateur peut donc se voir appliquer plusieurs GPO.

4.3. Application des stratégies de groupe

- Le client de stratégie de groupe du poste récupère la configuration (par défaut au bout de 60 à 120 minutes) qui est applicable à l'ordinateur et/ou à l'utilisateur connecté.
- C'est un peu long, donc on peut forcer la mise à jour des GPO.

Pour forcer l'application des GPO, vous pouvez utiliser la commande **gpupdate /force**
Pour vérifier le résultat de l'application des GPO, vous pouvez utiliser la commande :
gpresult /h rapport.htm

4.4. Mise en place des stratégies de groupe

Pour le groupe compétition

· Désactiver l'accès à l'invite de commande.

Les Groupes adhérents

· Empêcher les utilisateurs

- de modifier le fond d'écran.
- d'utiliser les gadgets du bureau
- masquer et désactiver tous les éléments du bureau

Service Informatique

- d'utiliser la corbeille

Pour le groupe adhérent

Créer les lecteurs réseaux associés via une stratégie de groupe

Vérifier

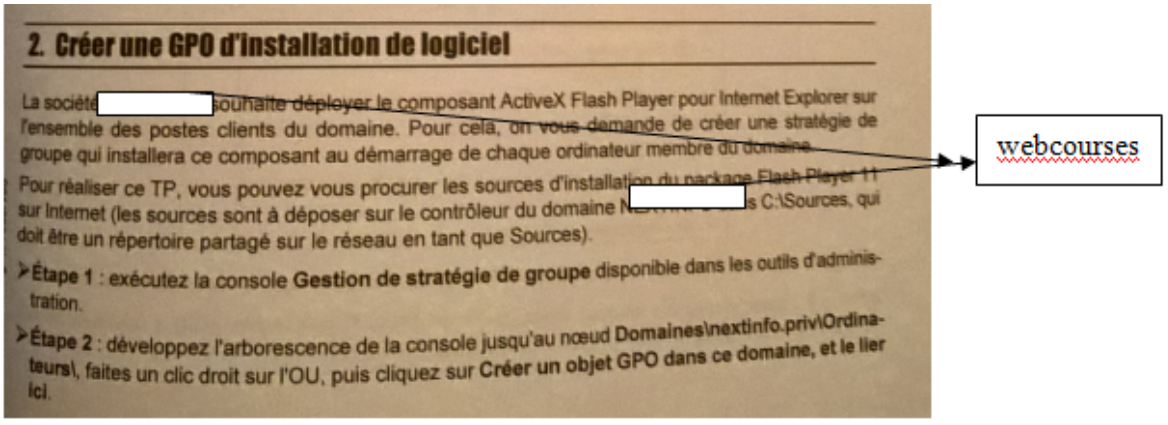
· Appliquez cette GPO (clic droit sur son nom > Appliqué)

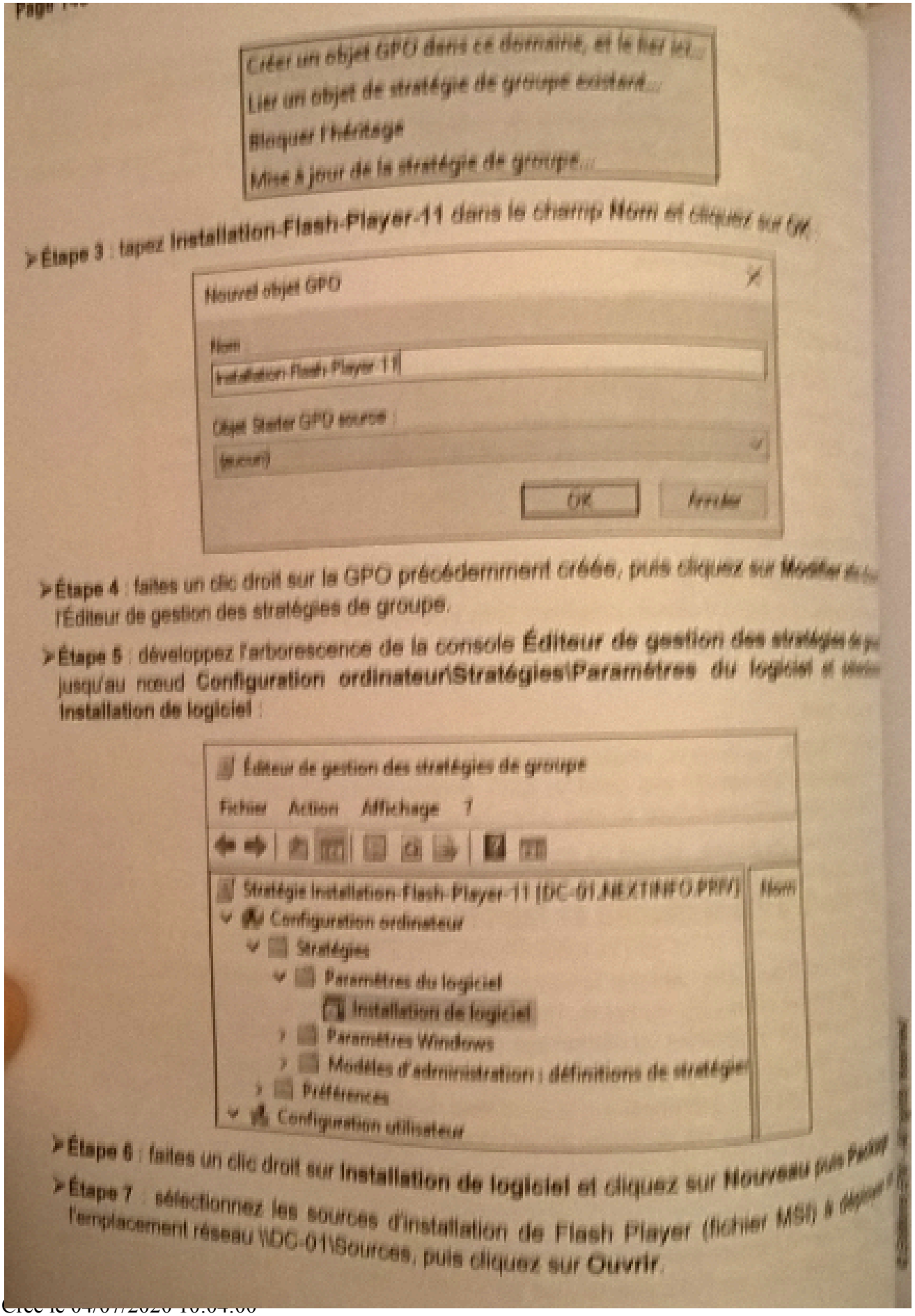
· Forcez la mise à jour des GPO

· Vérifiez que les stratégies s'appliquent bien aux utilisateurs des différentes unités d'organisation.

· Si les GPO ont bien fonctionné, dans la partie Objets de stratégies de groupes, sauvegardez toutes les GPO sur votre Bureau.

5. Mise en place d'une stratégie de groupe d'installation logiciel





➢ **Étape 3** : tapez **Installation-Flash-Player-11** dans le champ **Nom** et cliquez sur **OK**.

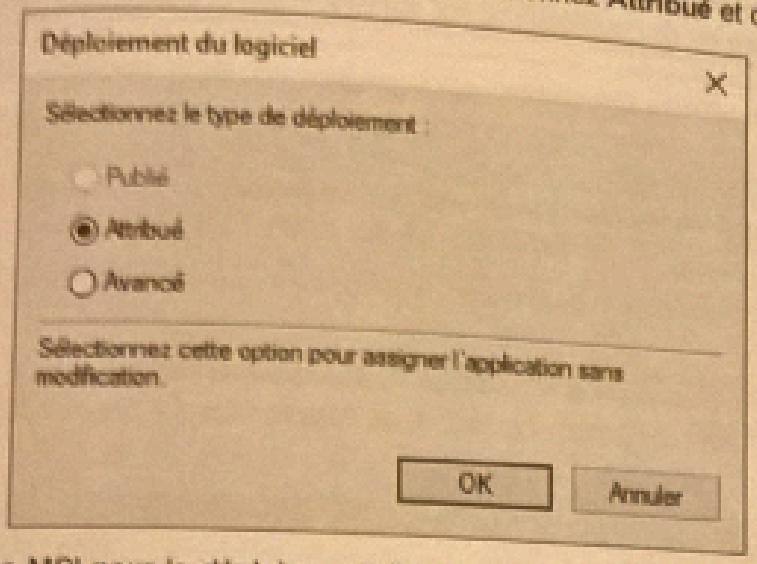
➢ **Étape 4** : faites un clic droit sur la GPO précédemment créée, puis cliquez sur **Modifier** de l'Éditeur de gestion des stratégies de groupe.

➢ **Étape 5** : développez l'arborescence de la console **Éditeur de gestion des stratégies de g** jusqu'au nœud **Configuration ordinateur\Stratégies\Paramètres du logiciel** et **Installation de logiciel** :

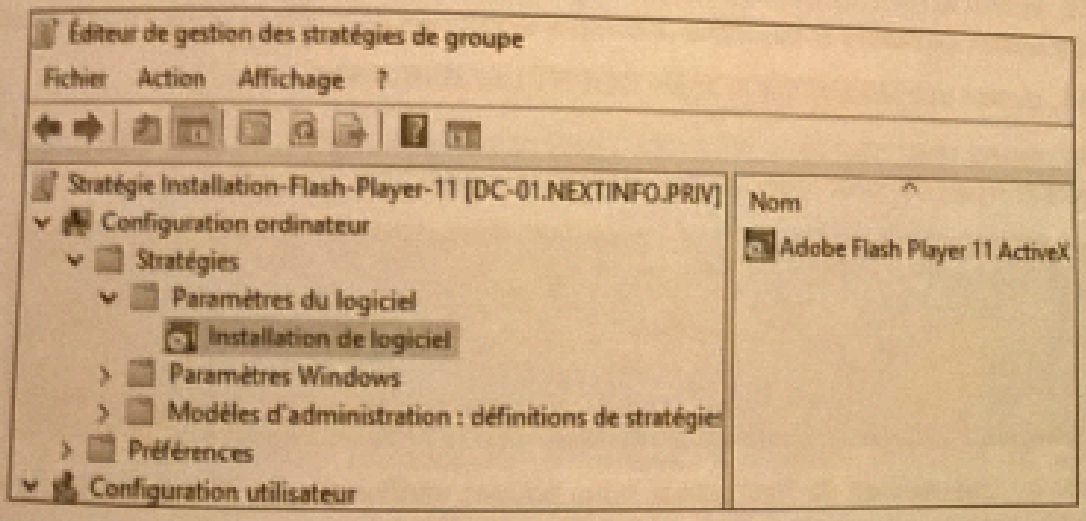
➢ **Étape 6** : faites un clic droit sur **Installation de logiciel** et cliquez sur **Nouveau** puis **Paket**

➢ **Étape 7** : sélectionnez les sources d'installation de Flash Player (fichier MSI) à déployer l'emplacement réseau \\DC-01\Sources, puis cliquez sur **Ouvrir**.

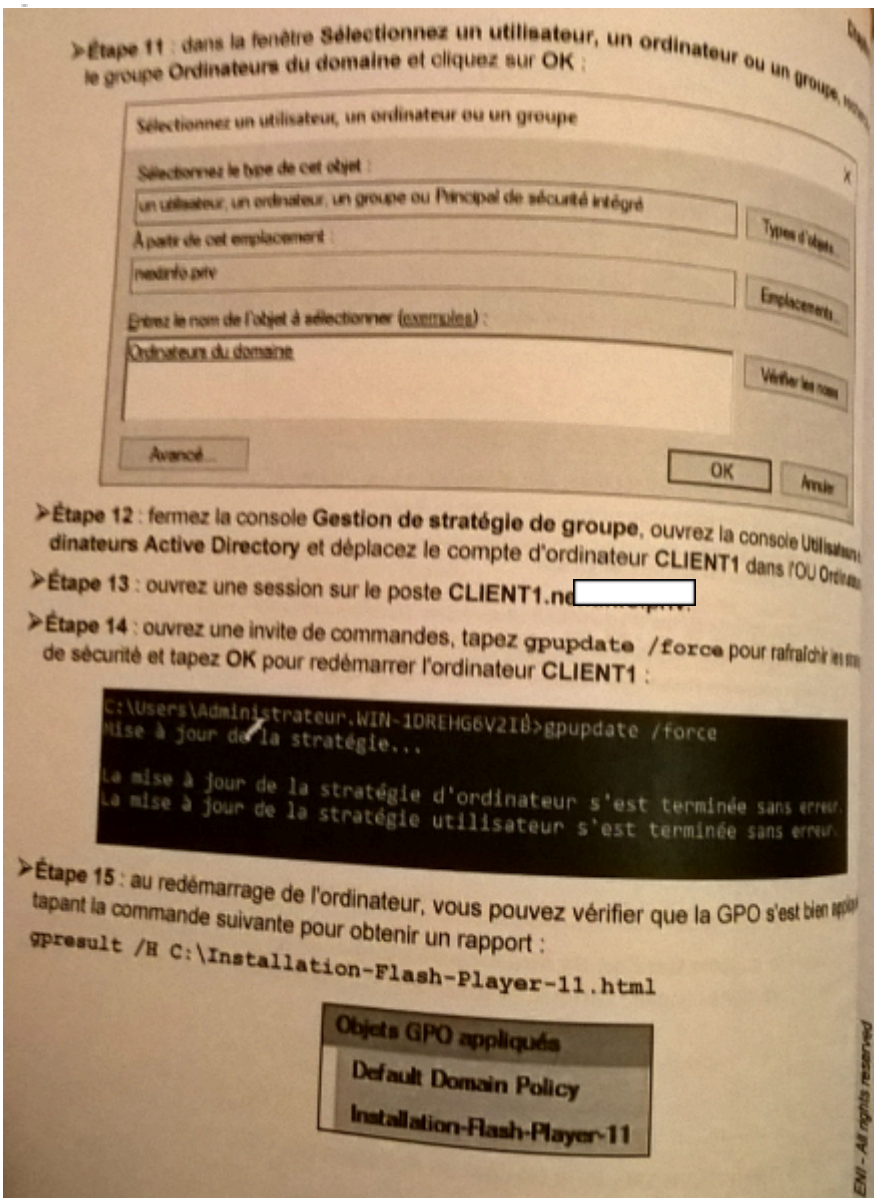
Étape 8 : dans la fenêtre **Déploiement du logiciel**, sélectionnez **Attribué** et cliquez sur **OK** :



Étape 9 : le package MSI pour le déploiement d'ActiveX Flash Player apparaît dans la fenêtre de l'Éditeur de gestion des stratégies de groupe. Fermez la fenêtre.



Étape 10 : depuis la console **Gestion de stratégie de groupe**, sélectionnez la GPO **Installation-Flash-Player-11** puis, dans l'onglet **Étendue**, cliquez sur le bouton **Ajouter** de la section **Filtrage de sécurité**.



➢ **Étape 11** : dans la fenêtre **Sélectionnez un utilisateur, un ordinateur ou un groupe**, le groupe **Ordinateurs du domaine** et cliquez sur **OK** :

Sélectionnez un utilisateur, un ordinateur ou un groupe

Sélectionnez le type de cet objet :

un utilisateur, un ordinateur, un groupe ou Principal de sécurité intégré — Types d'objets...

À partir de cet emplacement :

nestinfo.priv — Emplacements...

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

Ordinateurs du domaine — Vérifier les noms

Avancé... OK Annuler

➢ **Étape 12** : fermez la console **Gestion de stratégie de groupe**, ouvrez la console Utilisateurs dinateurs Active Directory et déplacez le compte d'ordinateur **CLIENT1** dans l'OU Ordinateurs

➢ **Étape 13** : ouvrez une session sur le poste **CLIENT1.nestinfo.priv**

➢ **Étape 14** : ouvrez une invite de commandes, tapez `gpupdate /force` pour rafraîchir les stratégies de sécurité et tapez **OK** pour redémarrer l'ordinateur **CLIENT1** :

```
C:\Users\Administrateur.WIN-1DREHG6V2IB>gpupdate /force
Mise à jour de la stratégie...

La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.
La mise à jour de la stratégie utilisateur s'est terminée sans erreur.
```

➢ **Étape 15** : au redémarrage de l'ordinateur, vous pouvez vérifier que la GPO s'est bien appliquée tapant la commande suivante pour obtenir un rapport :

```
gpresult /H C:\Installation-Flash-Player-11.html
```

Objets GPO appliqués
Default Domain Policy
Installation-Flash-Player-11

ENI - All rights reserved

webcourses

3. Créer des préférences de stratégies de groupe

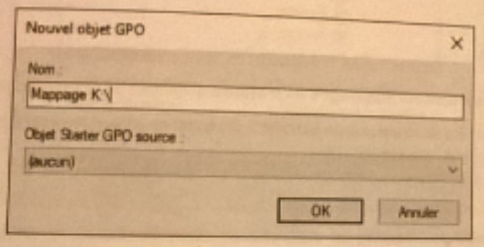
La société NE[redacted]haite créer un mappage de lecteur réseau ainsi qu'un déploiement de fichiers.

Pour réaliser ce TP, créez au préalable le dossier *C:\Temp* sur l'ordinateur CLIENT1 ainsi que les dossiers *C:\PARTAGE* et *C:\FICHIERS* sur le contrôleur de domaine DC-01, puis partagez ces derniers. Créez le fichier texte Fichier1.txt dans le dossier *C:\FICHIERS*.

➢ **Étape 1** : démarrez la console **Gestion de stratégie de groupe** disponible dans les outils d'administration.

➢ **Étape 2** : développez l'arborescence de la console jusqu'au nœud **Domaines\nextinfo.priv\Utilisateurs**, faites un clic droit sur l'OU, puis cliquez sur **Créer un objet GPO dans ce domaine, et le lier ici**.

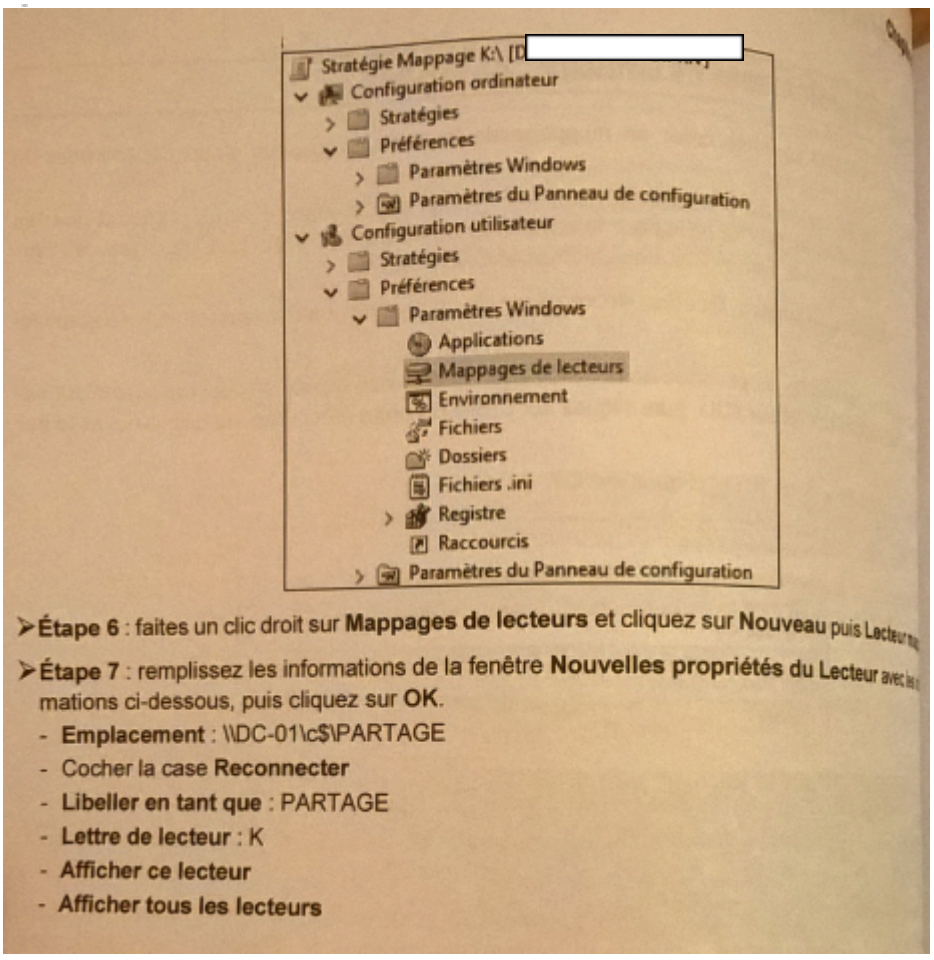
➢ **Étape 3** : tapez **Mappage K:** et cliquez sur **OK**.



➢ **Étape 4** : faites un clic droit sur la GPO précédemment créée, puis cliquez sur **Modifier** afin d'ouvrir l'Éditeur de gestion des stratégies de groupe.

➢ **Étape 5** : développez l'arborescence de la console **Éditeur de gestion des stratégies de groupe** jusqu'au nœud **Configuration utilisateur\Préférences\Paramètres Windows** et sélectionnez **Mappages de lecteurs**.

webcourses

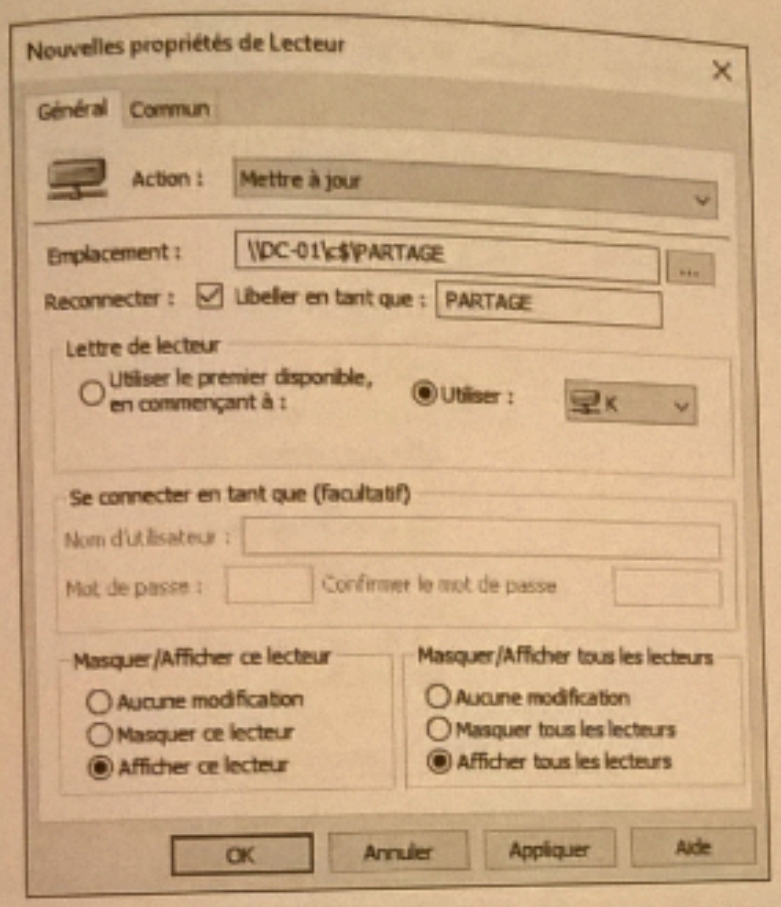


➢ **Étape 6** : faites un clic droit sur **Mappages de lecteurs** et cliquez sur **Nouveau** puis Lecteur ma

➢ **Étape 7** : remplissez les informations de la fenêtre **Nouvelles propriétés du Lecteur** avec les informations ci-dessous, puis cliquez sur **OK**.

- **Emplacement** : \\DC-01\c$\PARTAGE
- Cocher la case **Reconnecter**
- **Libeller en tant que** : PARTAGE
- **Lettre de lecteur** : K
- **Afficher ce lecteur**
- **Afficher tous les lecteurs**

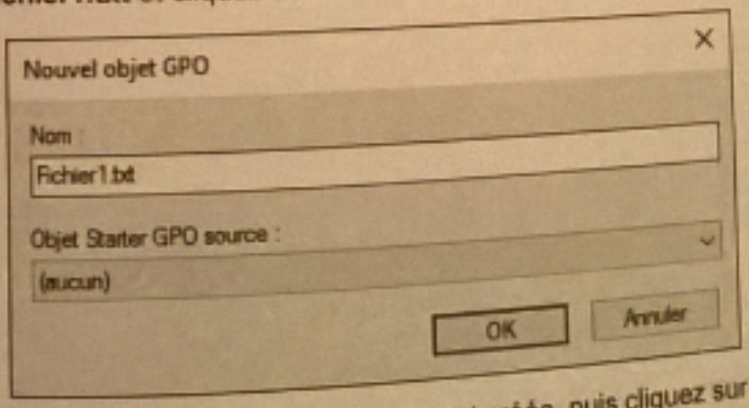
srvaddns.
webcourses.sio



➢ **Étape 8** : retournez sur la console **Gestion de stratégie de groupe**, sélectionnez l'OU **Externes**, faites un clic droit puis cliquez sur **Bloquer l'héritage**.

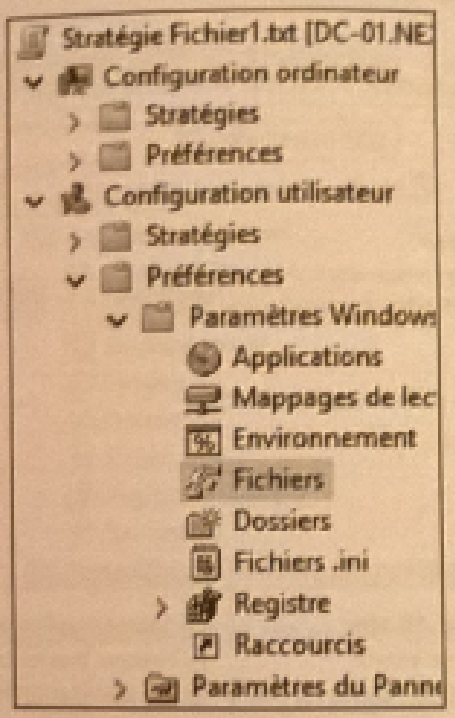
➢ **Étape 9** : faites un clic droit sur l'OU **Utilisateurs**, puis cliquez sur **Créer un objet GPO dans ce domaine, et le lier ici** :

➢ **Étape 10** : tapez **Fichier1.txt** et cliquez sur **OK**.



➢ **Étape 11** : faites un clic droit sur la GPO précédemment créée, puis cliquez sur **Modifier** afin d'ouvrir l'Éditeur de gestion des stratégies de groupe.

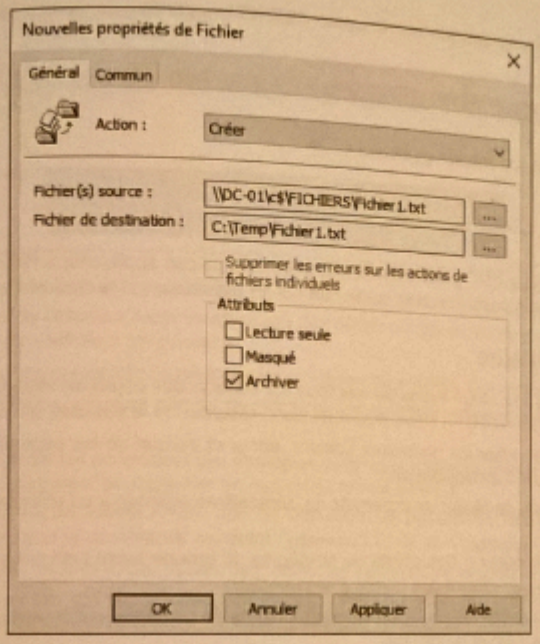
➢ **Étape 12** : développez l'arborescence de la console **Éditeur de gestion des stratégies de** jusqu'au nœud **Configuration utilisateur\Préférences\Paramètres Windows** et **Fichiers** :



➢ **Étape 13** : faites un clic droit sur **Fichiers** et cliquez sur **Nouveau** puis **Fichier**.

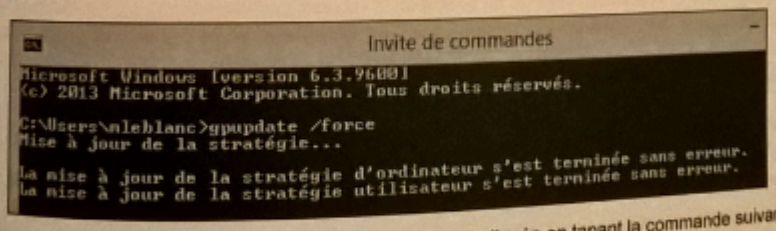
➢ **Étape 14** : remplissez les informations de la fenêtre **Nouvelles propriétés de Fichier** avec les informations ci-dessous, puis cliquez sur **OK** et fermez la fenêtre.

- **Action** : Créer
- **Fichier source** : \\DC-01\c$\FICHIERS\Fichier1.txt
- **Fichier de destination** : C:\Temp\Fichier1.txt



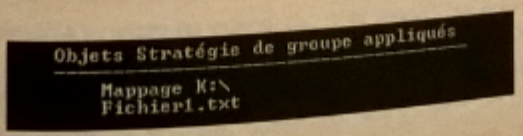
➢ **Étape 15** : ouvrez une session sur le poste **CLIENT1.nextinfo.priv** avec le compte de domaine **mleblanc**.

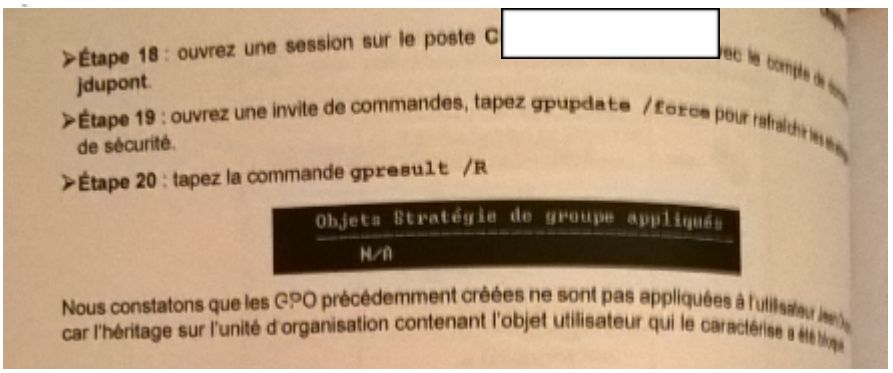
➢ **Étape 16** : ouvrez une invite de commandes, tapez `gpupdate /force` pour rafraîchir les stratégies de sécurité :



➢ **Étape 17** : vous pouvez vérifier que la GPO s'est bien appliquée en tapant la commande suivante :

```
gpresult /R
```





➢ **Étape 18** : ouvrez une session sur le poste C[redacted] avec le compte de [illegible] jdupont.

➢ **Étape 19** : ouvrez une invite de commandes, tapez `gpupdate /force` pour rafraîchir les [illegible] de sécurité.

➢ **Étape 20** : tapez la commande `gpresult /R`

Nous constatons que les GPO précédemment créées ne sont pas appliquées à l'utilisateur Jean[illegible] car l'héritage sur l'unité d'organisation contenant l'objet utilisateur qui le caractérise a été bloqué

Client1. webcourses.sio

Mission 4 Documenter AD DS 1ère partie

Compétences	Reprendre toutes les compétences relatives aux différentes missions
Objectifs	Documenter Active Directory AD DS
Vocabulaire à connaître	
Évaluation	Compte-rendu à rendre pour évaluation sommative coefficient 2 Compte-rendu est à poser dans votre PFC Épreuve E4 certificative

Page de garde

1. **L'entête de chaque page doit contenir les informations suivantes :**
    1. Nom de l'établissement
    2. Titre complet de l'activité
    3. La version du document

2. **Le pied de chaque page doit contenir les informations suivantes :**
    4. L'auteur / les auteurs
    5. Numéro de page
    6. Date

3. **Au centre de la page**
    7. Donner l'objectif principal de l'activité

Sommaire ou table des matières

1. **Automatiser** votre sommaire

Introduction

1. **Présenter**
   1.1. le contexte sur lequel vous travaillez (Description de la ligue de marathon)
   1.2. Description de son logo (celui que vous avez choisi sur votre site) représentation, symbole, lien Internet si vous l'avez récupéré sur une bibliothèque d'images

Déroulé de la mission 2 et 3

1. **Donner** le schéma réseau global associé au contexte des missions 1 à 7
2. **Préciser** les contraintes liées aux Prérequis si nécessaires
3. **Notifier** les points de vigilance de chaque mission
4. **Expliquer** les points de blocage et les solutions apportées
5. **Montrer** à l'aide d'une copie écran les résultats obtenus après les mises en place des missions

Analyse de l'activité

1. **Spécifier** les difficultés rencontrées au cours des différentes phases de mise en place
2. **Mentionner** les apports professionnels acquis à travers cette expérience
3. **Préciser** les apports personnels acquis à travers cette expérience

Mission 5 Administrer le service DNS sur le contrôleur de domaine

Compétences	
Objectif principal	**Gérer** un service DNS statique
Objectifs intermédiaires	**Installer** et **configurer** le service DNS **Montrer** la synchronisation de serveur, La continuité de service, La répartition de charge avec la mise en place d'un serveur DNS secondaire statique **Cibler** l'intérêt d'un DNS dynamique et évolutif Pour la maintenance **Montrer** l'intérêt de contrôler le trafic DNS à travers la mise en place d'une Délégation et d'une redirection
Vocabulaire à connaître	Épreuve E4 certificative
Évaluation	

Votre mission

Administrer le service DNS sur le contrôleur de domaine

Informations utiles

Adresse du serveur DNS primaire (contrôleur de domaine): 172.16.0.100/24
Nom de la machine : srvaddns

Un nouveau serveur DNS secondaire : 192.168.0.200/24
Passerelle : 172.16.0.254
Nom de la machine : srvdns2

Guide d'installation

1ère partie
Mise en place d'un serveur DNS primaire statique

Le serveur primaire = serveur contrôleur de domaine

1. Configuration d'un serveur DNS primaire statique

1.1. Création d'une zone de recherche directe

- Vérifier que **webcourses.sio** existe sinon

- Démarrer – outils d'administration – DNS – clic droit sur zone de recherche directe – nouvelle zone – suivant – zone principale – dans le nom de la zone indiquer **webcourses.sio –** suivant – ne pas autoriser les mises à jours – suivant – terminer

1.2. Création des mappages

- Clic droit sur la zone **webcourses.sio –** nouvel hôte – saisir **le** nom du poste servant de serveur DNS primaire et son @ IP
- Actualiser la mise à jour
- Répéter cette opération pour tous les postes du schéma se trouvant en p3.
  Rappel : le routeur possède 2 cartes.
  - Au final, vous devez avoir un mappage contenant:
  - passerelle 1 du routeur bleu
  - passerelle 2 du routeur bleu
  - passerelle 1 du routeur vert
  - passerelle 2 du routeur vert
  - Poste client vélo
  - Poste client course à pied
  - Poste client natation
  - Poste admin
  - Serveur contrôleur de domaine qui est aussi le serveur dns

1.3. Ajout de la suffixe dans la propriété TCP/IP

A ce niveau, la zone de recherche directe fonctionne bien à condition de spécifier le FQDN associé.
Pour que la résolution de nom fonctionne avec le FQDN, mais sans avoir à le saisir à chaque fois, on peut alors l'indiquer au niveau de la carte réseau. Pour cela faire :

Démarrer – panneau de configuration – connexion réseau – clic droit sur la carte réseau – propriété – protocol Internet – propriété – avané – DNS – cliquer sur ajouter ces suffixes DNS – dans la zone suffixe DNS pour cette connexion saisir le nom FQDN à savoir **webcourses.sio** – ok – ok

Sur le serveur, vérifier que l'ajout du FQDN sur la carte réseau fonctionne en ouvrant l'invite de commande et saisir **nslookup serveur**

1.4. Création d'une zone de recherche inversée

Afin de pouvoir utiliser le lien @IP nom, il faut créer une zone de recherche inversée. Sans ce lien la commande nslookup ne fonctionne pas.

- Démarrer – outils d'administration – DNS – clic droit sur zone de recherche inversée – ouvelle zone – suivant – zone principale – saisir l'ID du LAN 1 à savoir **172.16.1 –** suivant – ne pas autoriser les mises à jours – suivant – terminer
- Clic droit sur la zone de recherche inversée **172.16.1.x Subnet** – nouveau pointeur – saisir la partie Identificateur Machine du poste concerné – parcourir – aller chercher le nom du poste correspond à l'@IP que vous venez de saisir

- Refaire cette opération pour chacun des postes à identifier sur le réseau que vous venez d'ouvrir
- Refaire l'opération pour chaque LAN présent sur votre schéma

1.5. Phase de vérification

- Vérifier à partir du poste serveur que la zone de recherche directe et indirecte fonctionne.

Sur le Serveur primaire, vérifier que la zone de recherche directe fonctionne en ouvrant l'invite de commande et saisir **nslookup Poste Admin**

Quel est le résultat de la commande ? Pourquoi ?

Recommencer l'opération mais cette fois en saisissant le nom FQDN de Poste Admin c'est-à-dire suivi de son nom de domaine **webcourses.sio**

Quel est le résultat de la commande ? Pourquoi ?

1.6. Ajout de la suffixe dans la propriété TCP/IP

Comme nous venons de le constater, la zone de recherche directe fonctionne bien à condition de spécifier le FQDN associé.
Pour que la résolution de nom fonctionne avec le FQDN, mais sans avoir à le saisir à chaque fois, on peut alors l'indiquer au niveau de la carte réseau. Pour cela faire :

Démarrer – panneau de configuration – connexion réseau – clic droit sur la carte réseau – propriété – Protocol Internet – propriété – avancé – DNS – cliquer sur ajouter ces suffixes DNS – dans la zone suffixe DNS pour cette connexion saisir le nom FQDN à savoir **webcourses.sio**– ok – ok

Sur le Serveur primaire, vérifier que l'ajout du FQDN sur la carte réseau fonctionne en ouvrant l'invite de commande et saisir **nslokkup Poste Admin**

Quel est le résultat de la commande ? Pourquoi ? Quel est le nom du serveur DNS ?

Maintenant saisir **nslookup 172.16.0.50**

Quel est le résultat de la commande ? Pourquoi ?

1.7. Création d'une zone de recherche inversée

Afin de pouvoir utiliser le lien @IP nom, il faut créer une zone de recherche inversée. Comme nous venons de le voir, sans le lien la commande nslookup ne fonctionne pas.

1.7.1. Démarrer – outils d'administration – DNS – clic droit sur zone de recherche inversée – nouvelle zone – suivant – zone principale – saisir l'ID du LAN 1 à savoir **172.16.0 –** suivant – ne pas autoriser les mises à jours – suivant – terminer

1.7.2. Clic droit sur la zone de recherche inversée 192.168.1.x Subnet – nouveau pointeur – saisir la partie Identificateur Machine du poste concerné (exemple pour Poste A il s'agit de 3, valeur du dernier octet de son @IP) – parcourir – aller chercher le nom du poste correspond à l'@IP que vous venez de saisir

1.7.3. Refaire cette opération pour chacun des postes à identifier

1.7.4. Refaire l'opération 1.5 pour chaque LAN présent de votre schéma

Sur le Serveur primaire, vérifier que la zone de recherche inversée fonctionne en ouvrant l'invite de commande et saisir **nslokkup 172.16.0.50**

Quel est le résultat de la commande ? Pourquoi ? Quel est le nom du serveur DNS ?

Vérifier à l'aide de la commande **nslookup** que tous les autres postes fonctionnent.

Vérifier à l'aide de la commande **ping nom du poste** que la connectivité fonctionne entre tous les postes. Se reporter au §I-4

1.8. Création d'une zone de recherche directe à l'aide du CNAME (canonical Name) c'est-à-dire d'un alias

A quoi sert un alias (CNAME) dans DNS ?

- Sur la zone de recherche directe, faire clic droit sur votre nom de domaine à savoir **webcourses.sio–** nouveau alias – dans le nom de l'alias saisir **www.webcourses.sio** – parcourir – rechercher le serveur primaire dns – ok

- Sur le Serveur primaire, vérifier que la zone de recherche directe avec un alias fonctionne en ouvrant l'invite de commande et saisir
  nslokkup www.webcourses.sio

- Sur le Poste Admin, vérifier que la zone de recherche directe avec un alias fonctionne en ouvrant l'invite de commande et saisir
  nslokkup www.webcourses.sio

Quel est le résultat de la commande ?

2ème partie
Montrer la synchronisation de serveur
La continuité de service
La répartition de charge avec la mise en place d'un serveur DNS secondaire statique

2. 10Création d'un serveur DNS secondaire statique

Un serveur DNS secondaire est une copie en lecture seule de la zone principale standard, utilisée pour assurer la répartition de charge DNS et la tolérance aux pannes si le serveur DNS principal tombe.

Dans notre schéma, le routeur va jouer le rôle du serveur de secours en cas de non disponibilité du serveur primaire. On va donc promouvoir le routeur pour qu'il devienne un serveur secondaire du premier serveur DNS.
Le routeur va contenir une base de données DNS identique à celle du serveur primaire grâce au transfert de zone du primaire vers le secondaire.

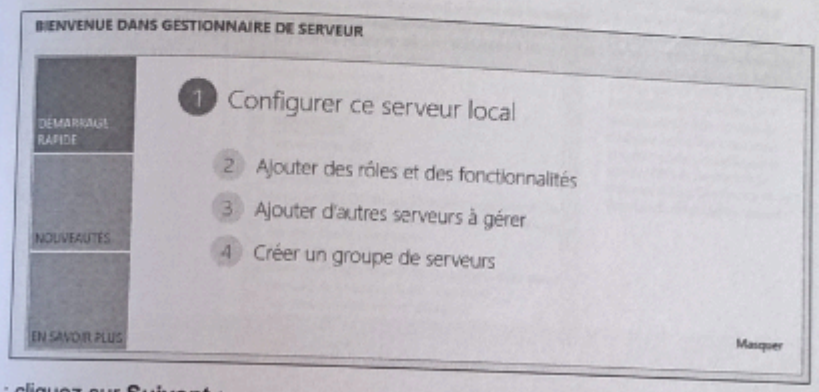
2.1. Configuration du serveur DNS secondaire statique

1. Installer et configurer le service DNS

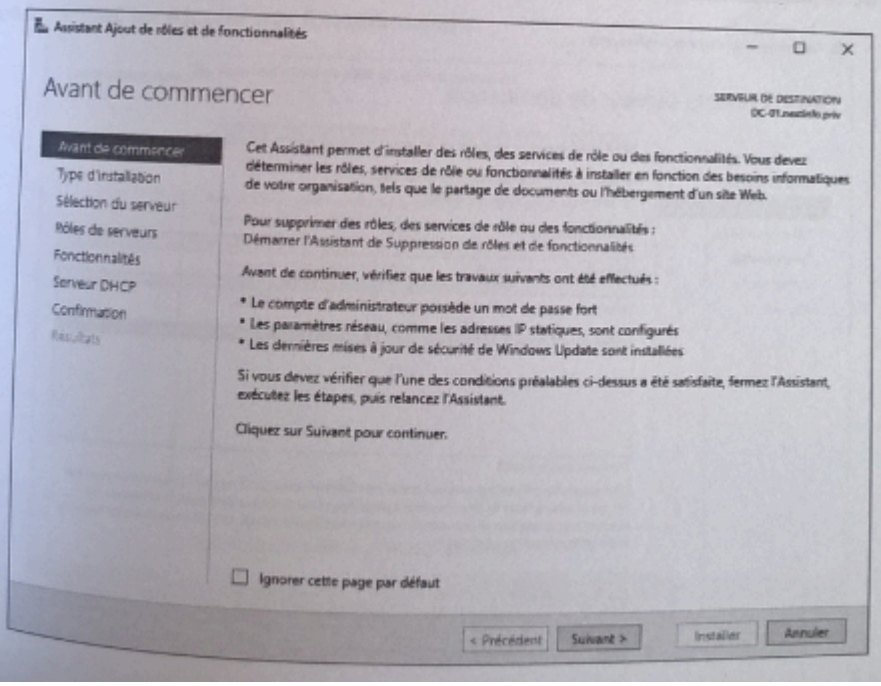
Ce TP permet d'installer et de configurer les principales options du rôle de serveur DNS. À ce stade, le domaine Nextinfo.priv n'est pas encore créé.

Installer le rôle de serveur DNS

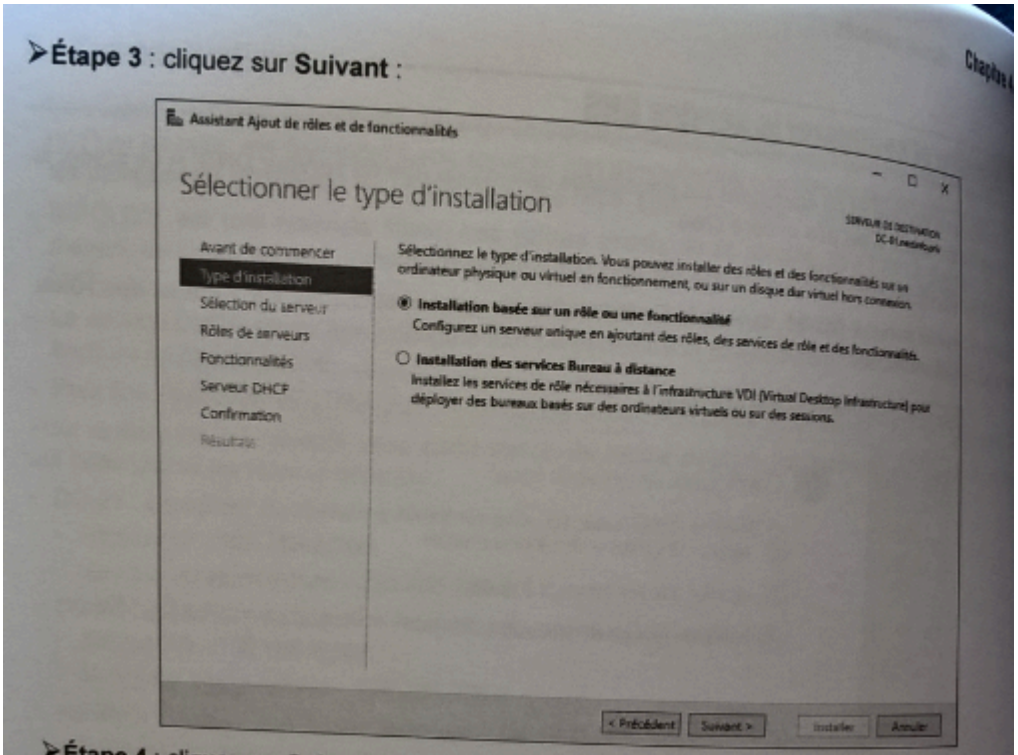
➢ **Étape 1** : sur le serveur **DC-01**, ouvrez le Gestionnaire de serveur et cliquez sur **Ajouter des rôles et des fonctionnalités**.



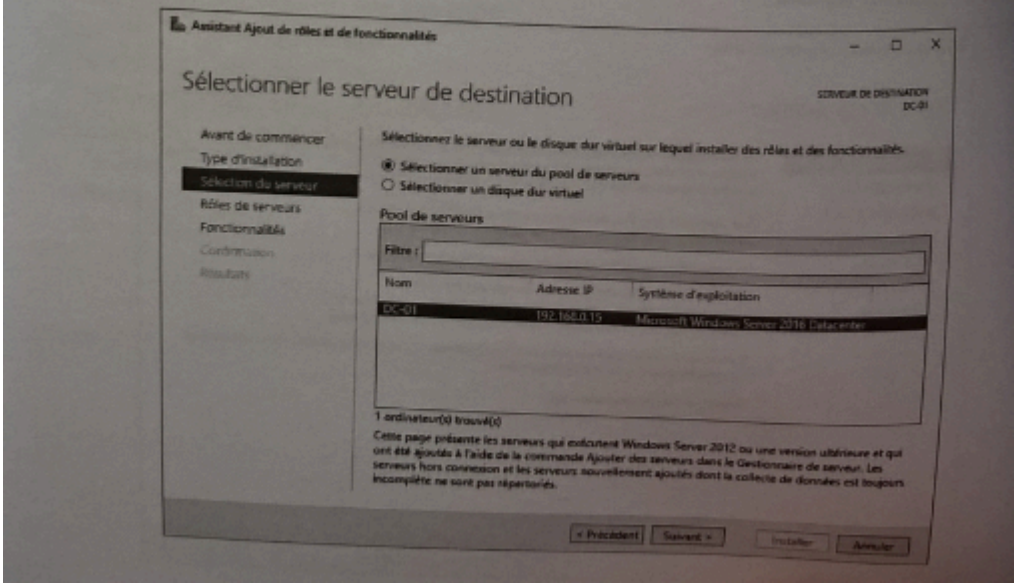
➢ **Étape 2** : cliquez sur **Suivant** :



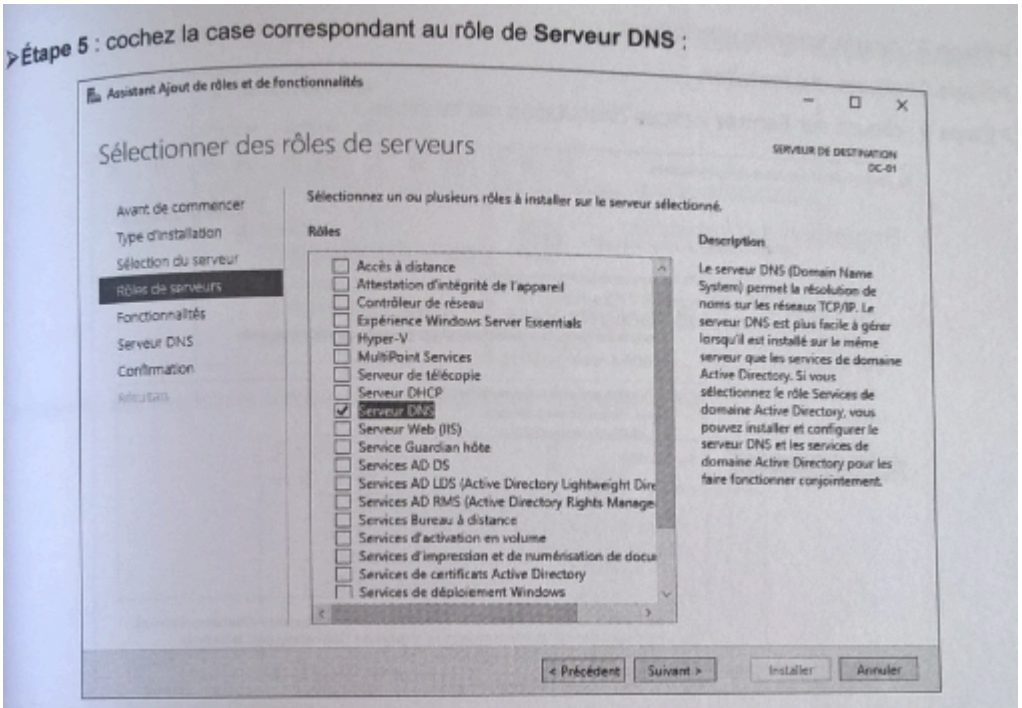
➢**Étape 3** : cliquez sur **Suivant** :



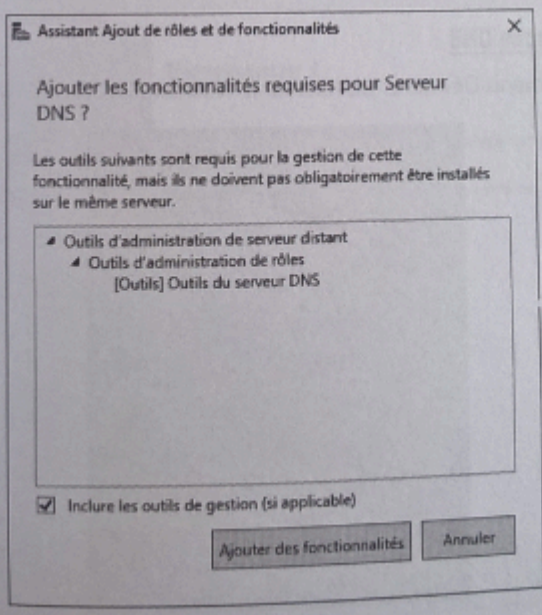
➢**Étape 4** : cliquez sur **Suivant** :



➢**Étape 5** : cochez la case correspondant au rôle de **Serveur DNS** :



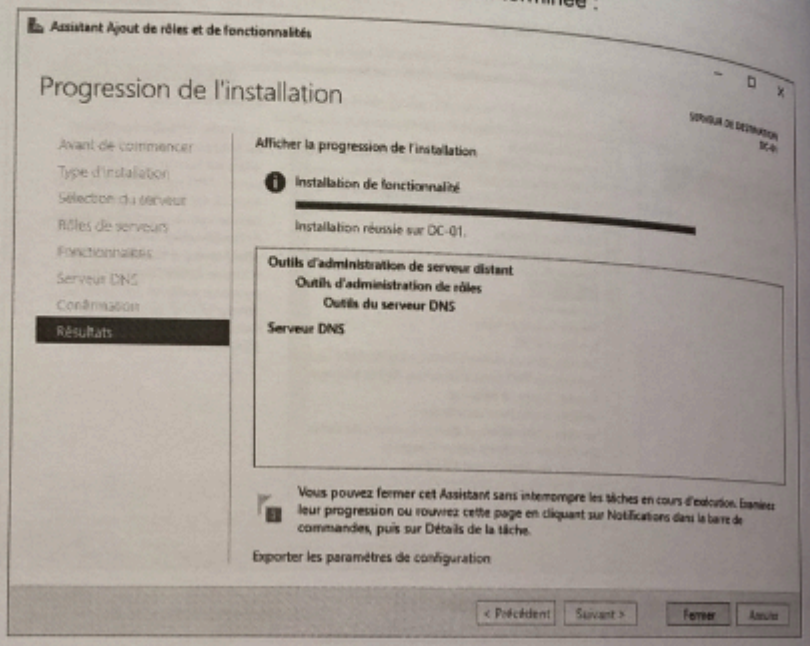
➢**Étape 6** : cliquez sur **Ajouter des fonctionnalités** :



➢**Étape 7** : cliquez trois fois sur **Suivant**.

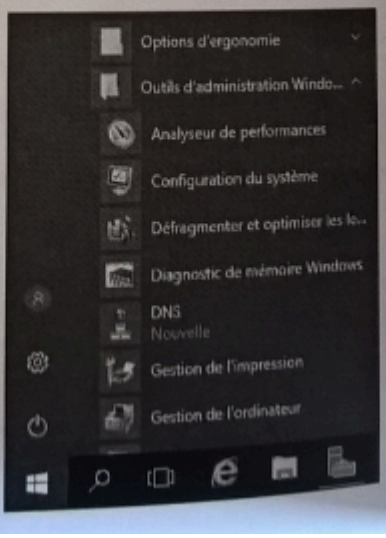
➢**Étape 8** : cliquez sur **Installer**.

➢**Étape 9** : cliquez sur **Fermer** lorsque l'installation est terminée :

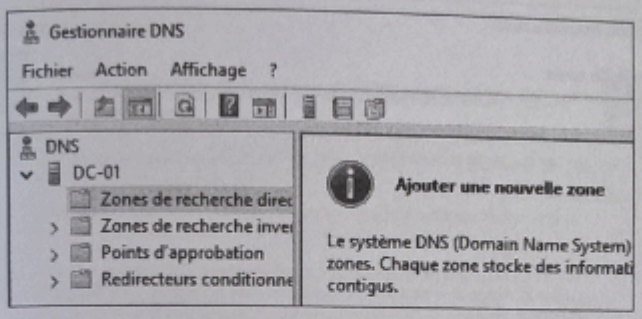


Créer des zones de recherche DNS

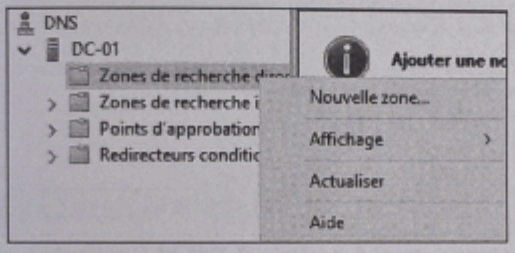
➢**Étape 1** : allez dans le menu Démarrer de Microsoft Windows Server 2016 et cliquez sur DNS :



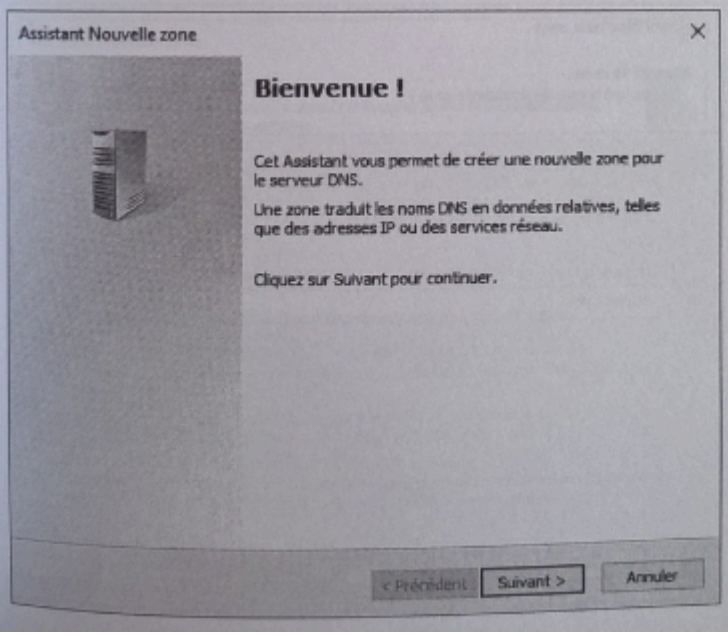
➢ **Étape 2** : développez l'arborescence de la console et sélectionnez **Zones de recherche directes** :

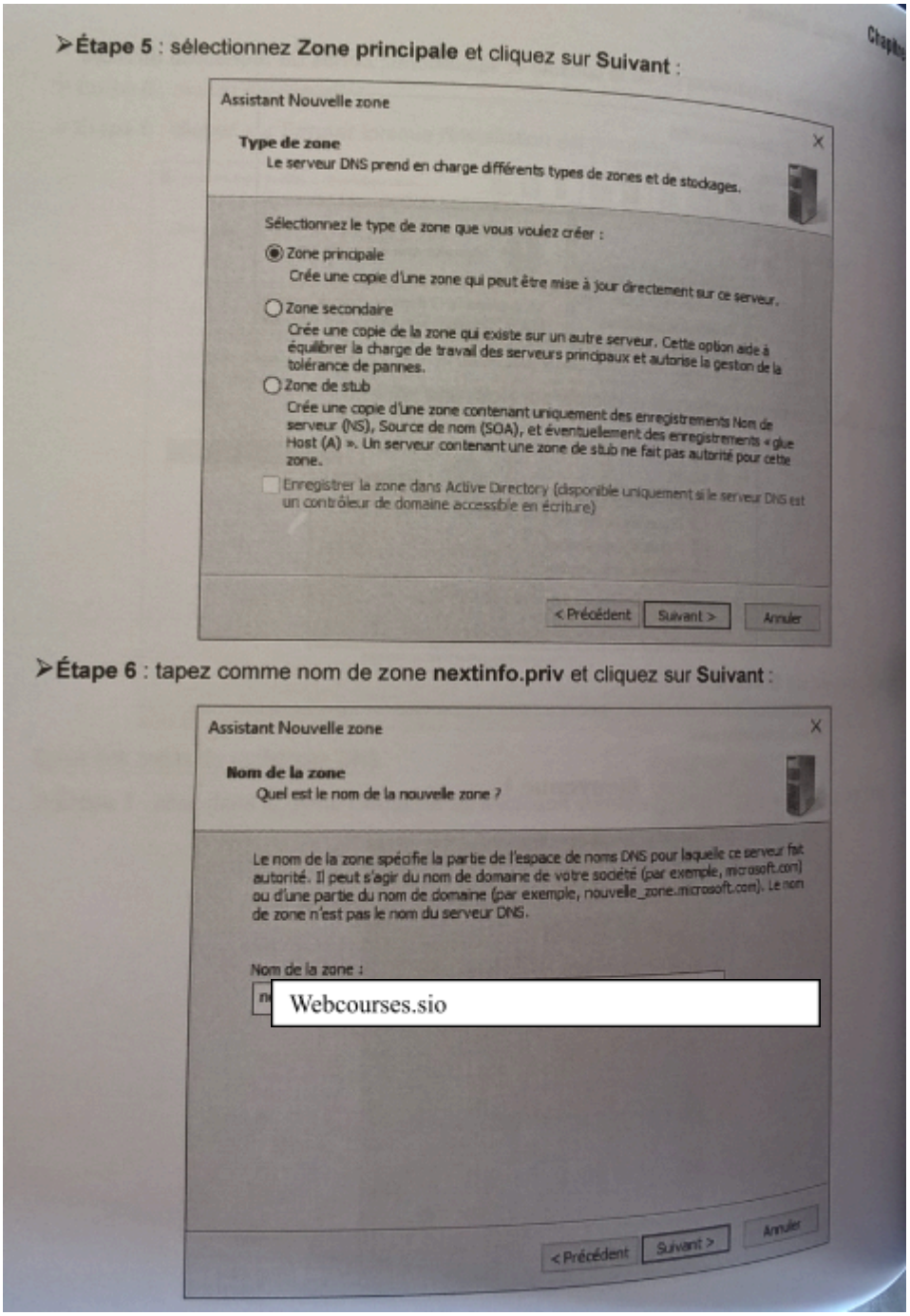


➢ **Étape 3** : affichez le menu contextuel et cliquez sur **Nouvelle zone...** :

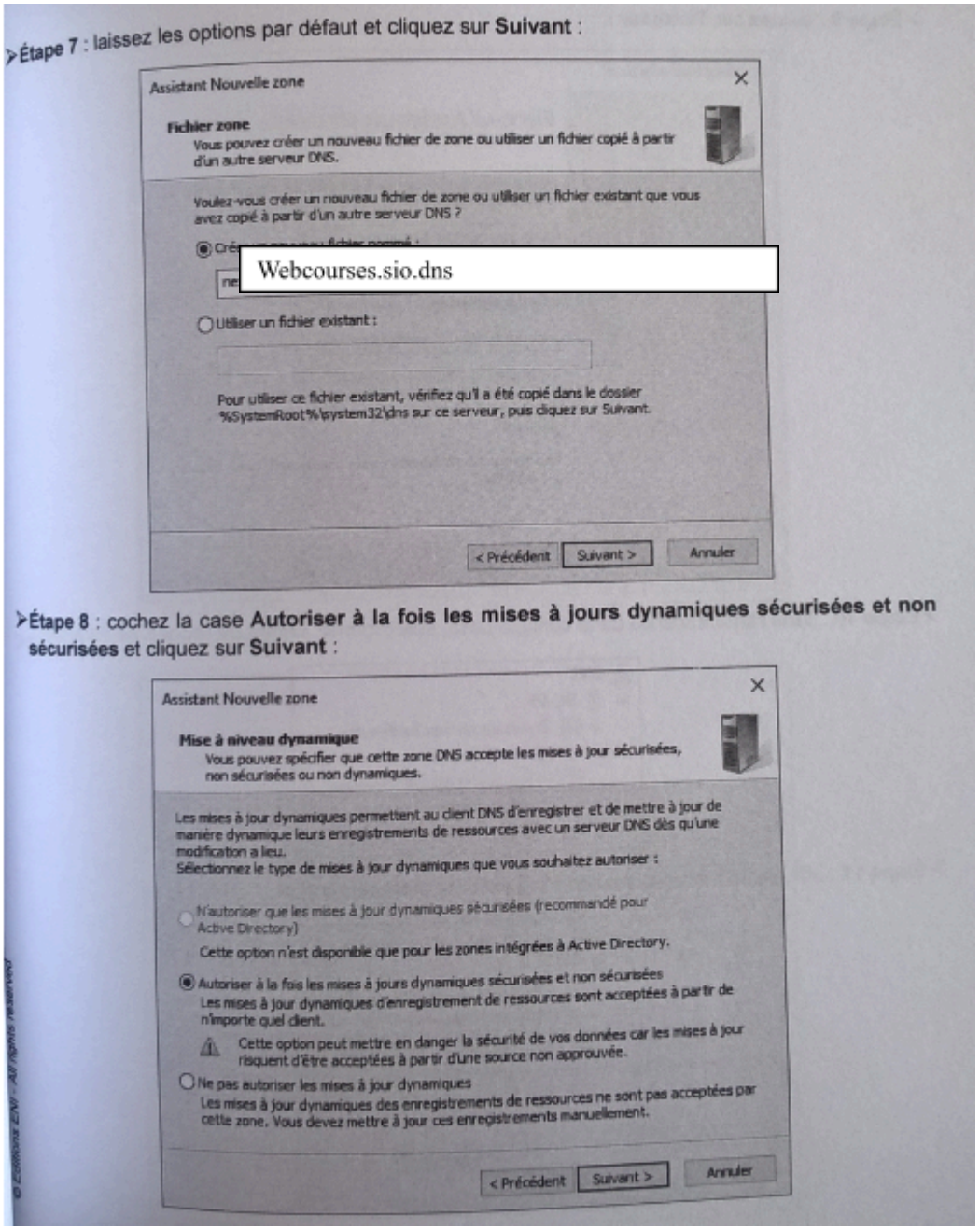


➢ **Étape 4** : cliquez sur **Suivant** :



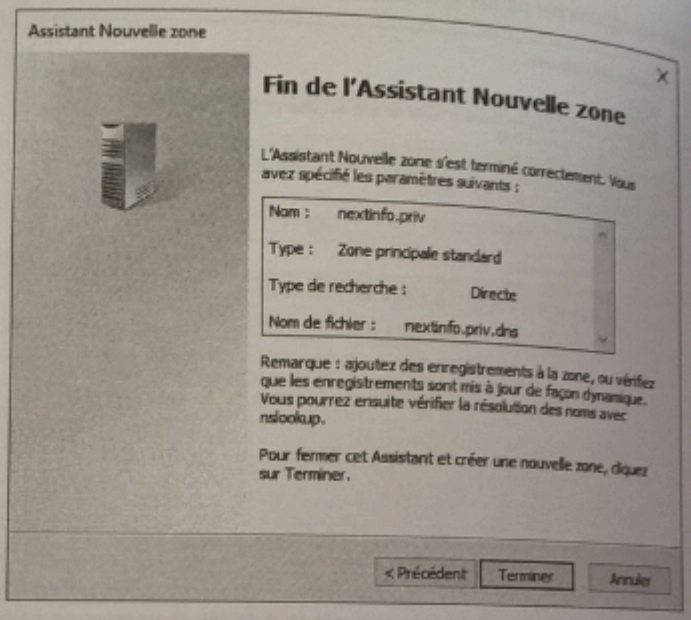

➢Étape 5 : sélectionnez Zone principale et cliquez sur Suivant :
Assistant Nouvelle zone
Type de zone
Le serveur DNS prend en charge différents types de zones et de stockages.
Sélectionnez le type de zone que vous voulez créer :
Zone principale
Crée une copie d'une zone qui peut être mise à jour directement sur ce serveur.
Zone secondaire
Crée une copie de la zone qui existe sur un autre serveur. Cette option aide à équilibrer la charge de travail des serveurs principaux et autorise la gestion de la tolérance de pannes.
Zone de stub
Crée une copie d'une zone contenant uniquement des enregistrements Nom de serveur (NS), Source de nom (SOA), et éventuellement des enregistrements « glue Host (A) ». Un serveur contenant une zone de stub ne fait pas autorité pour cette zone.
Enregistrer la zone dans Active Directory (disponible uniquement si le serveur DNS est un contrôleur de domaine accessible en écriture)
< Précédent
Suivant >
Annuler
➢Étape 6 : tapez comme nom de zone nextinfo.priv et cliquez sur Suivant :
Assistant Nouvelle zone
Nom de la zone
Quel est le nom de la nouvelle zone ?
Le nom de la zone spécifie la partie de l'espace de noms DNS pour laquelle ce serveur fait autorité. Il peut s'agir du nom de domaine de votre société (par exemple, microsoft.com) ou d'une partie du nom de domaine (par exemple, nouvelle_zone.microsoft.com). Le nom de zone n'est pas le nom du serveur DNS.
Nom de la zone :
Webcourses.sio
< Précédent
Suivant >
Annuler

➢ **Étape 7** : laissez les options par défaut et cliquez sur **Suivant** :

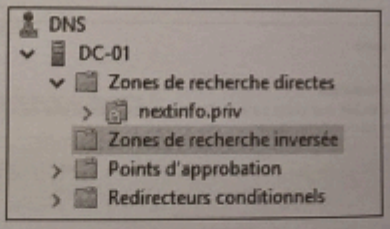


➢ **Étape 8** : cochez la case **Autoriser à la fois les mises à jours dynamiques sécurisées et non sécurisées** et cliquez sur **Suivant** :

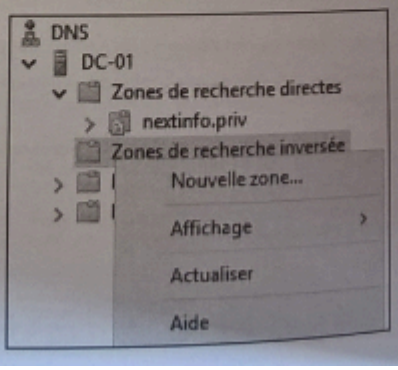
➢**Étape 9** : cliquez sur **Terminer** :



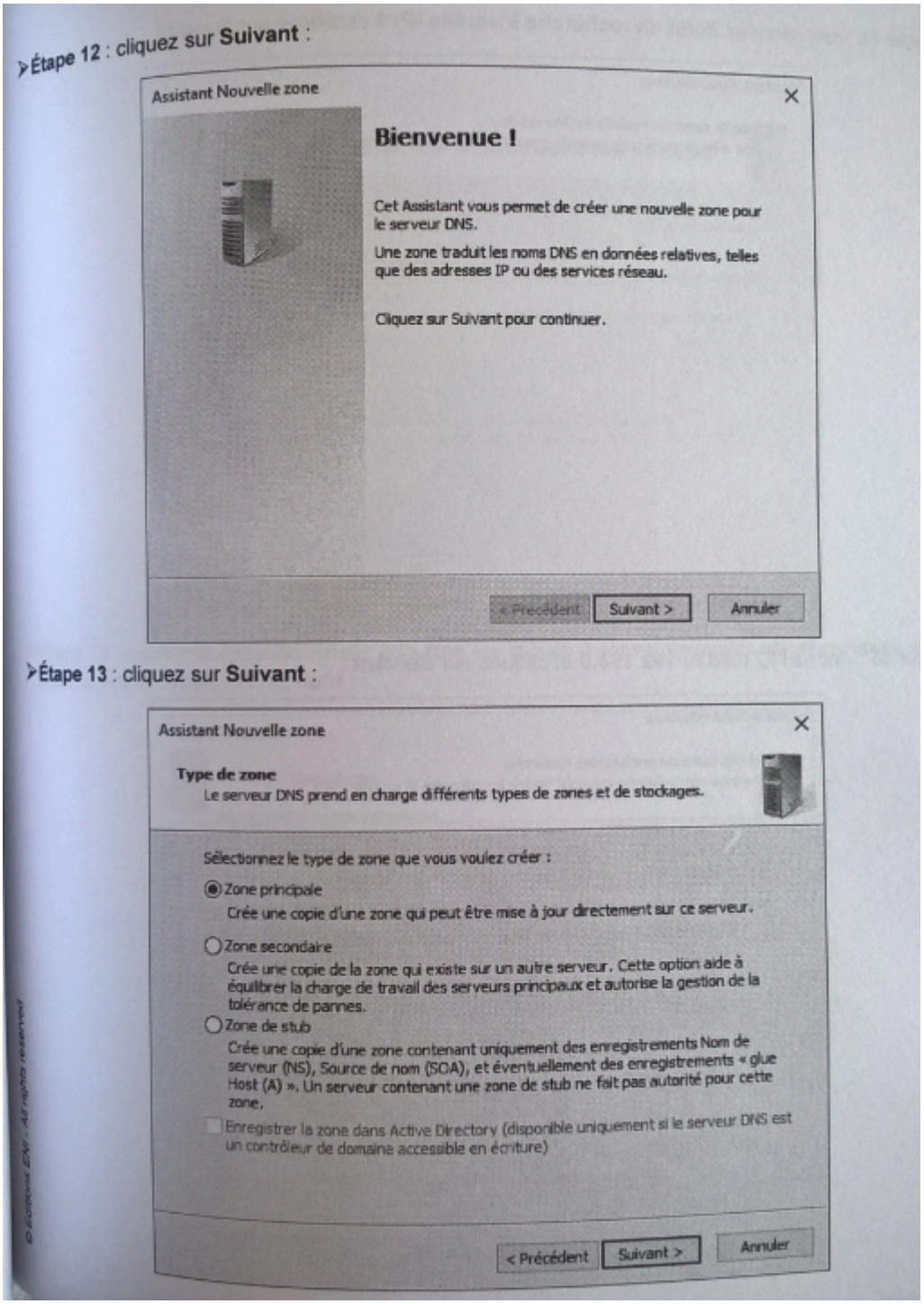
➢**Étape 10** : dans l'arborescence de la console DNS, sélectionnez **Zones de recherche inversée** :



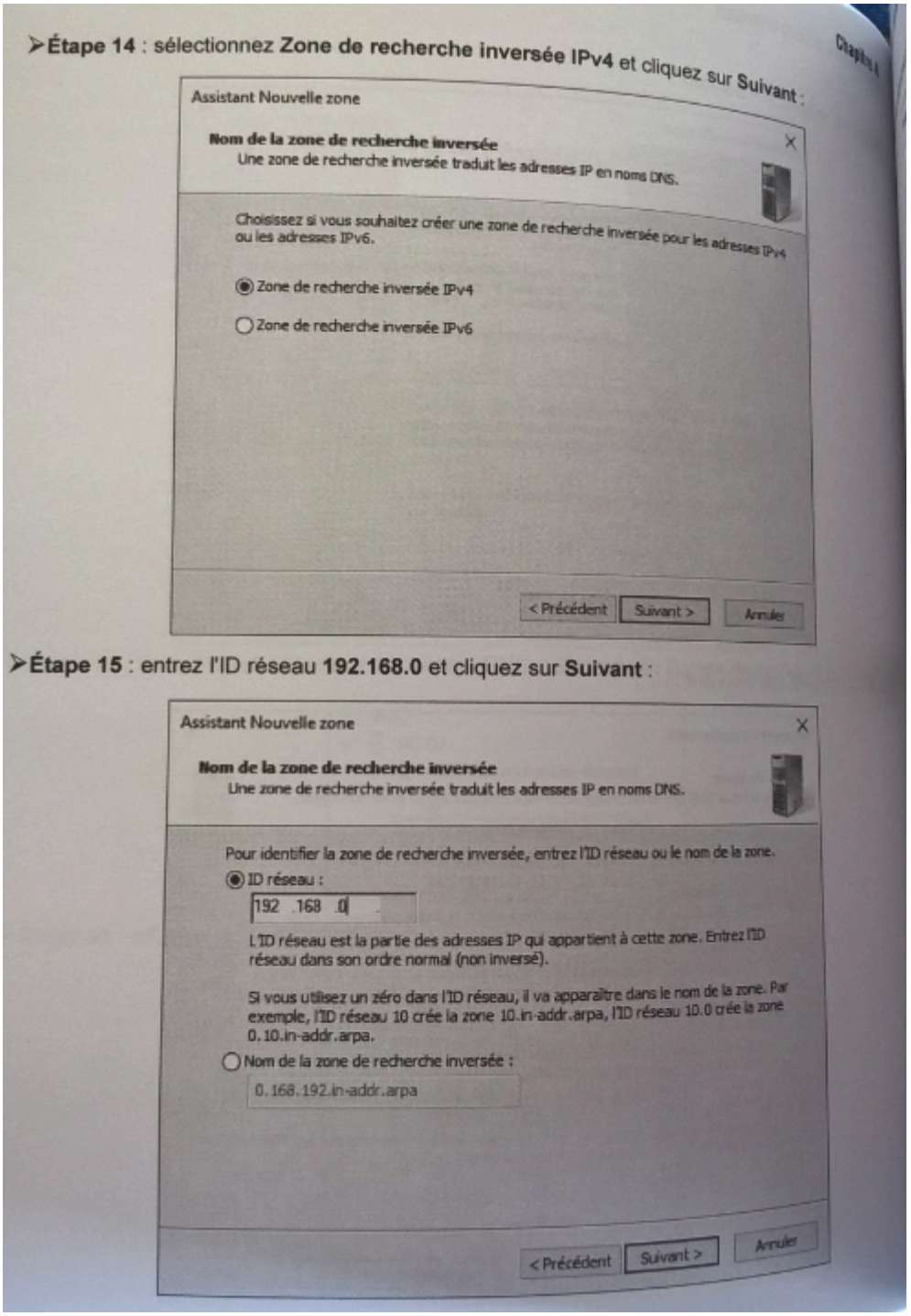
➢**Étape 11** : affichez le menu contextuel et cliquez sur **Nouvelle zone...** :



➢Étape 12 : cliquez sur **Suivant** :

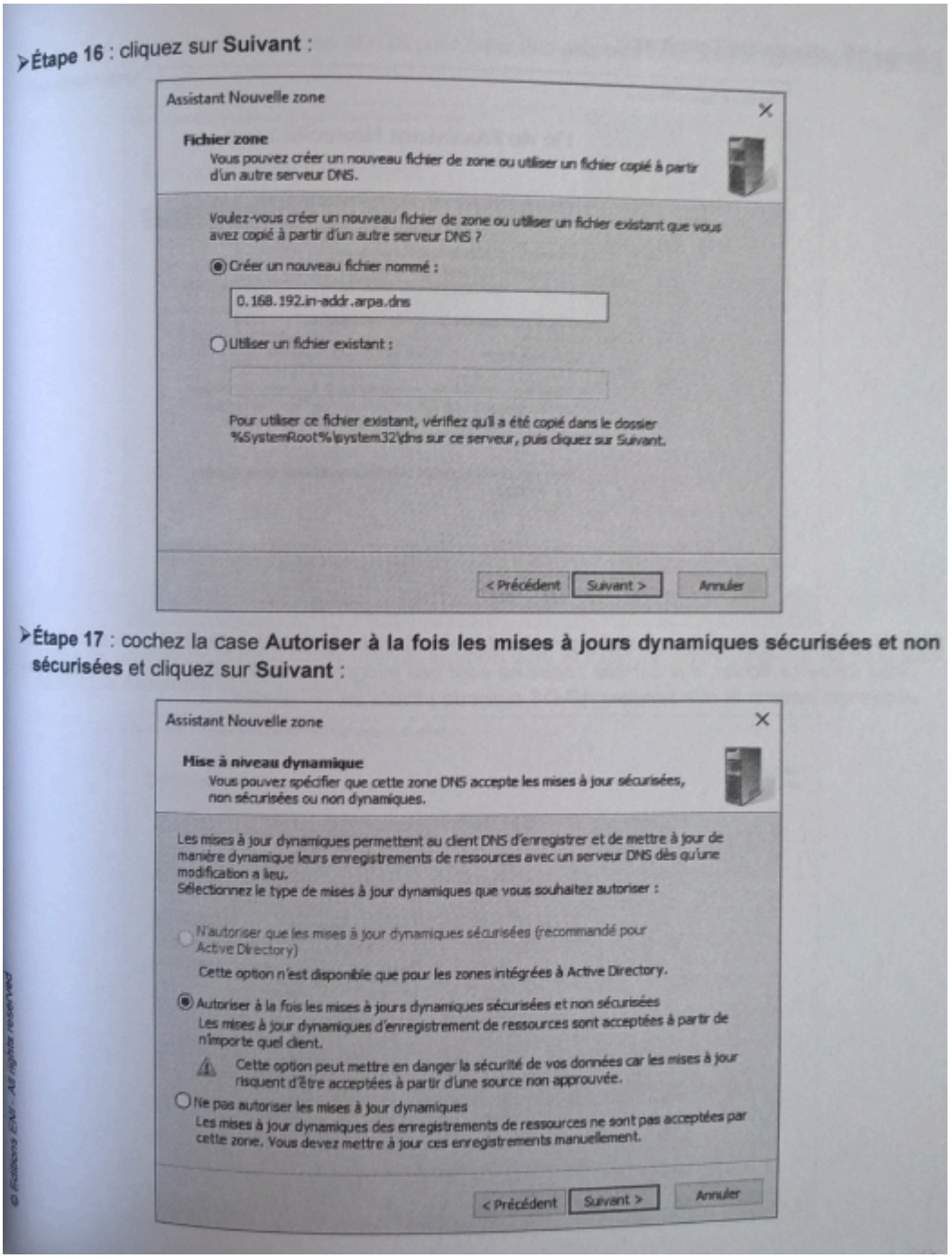


➢**Étape 14** : sélectionnez **Zone de recherche inversée IPv4** et cliquez sur **Suivant** :

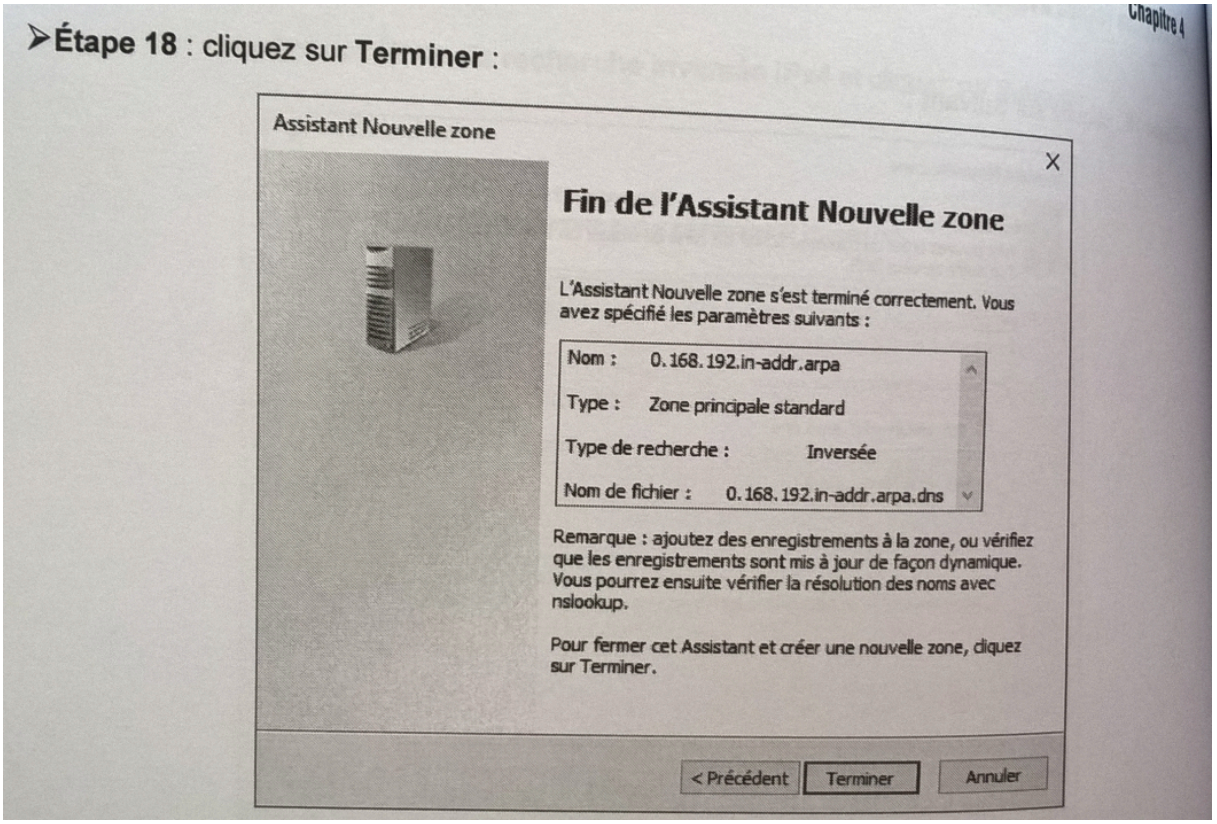


➢**Étape 15** : entrez l'ID réseau **192.168.0** et cliquez sur **Suivant** :

➢ **Étape 16** : cliquez sur **Suivant** :



➢ **Étape 17** : cochez la case **Autoriser à la fois les mises à jours dynamiques sécurisées et non sécurisées** et cliquez sur **Suivant** :


Chapitre 4
➢Étape 18 : cliquez sur Terminer :
Assistant Nouvelle zone
Fin de l'Assistant Nouvelle zone
L'Assistant Nouvelle zone s'est terminé correctement. Vous avez spécifié les paramètres suivants :
Nom : 0.168.192.in-addr.arpa
Type : Zone principale standard
Type de recherche : Inversée
Nom de fichier : 0.168.192.in-addr.arpa.dns
Remarque : ajoutez des enregistrements à la zone, ou vérifiez que les enregistrements sont mis à jour de façon dynamique. Vous pourrez ensuite vérifier la résolution des noms avec nslookup.
Pour fermer cet Assistant et créer une nouvelle zone, cliquez sur Terminer.
< Précédent
Terminer
Annuler

2.2. Créer une zone secondaire en recherche directe sur le serveur DNS secondaire

- Démarrer – outils d'administration – DNS – clic droit sur nouvelle zone – suivant – cliquer sur zone secondaire – suivant – zone de recherche directe – suivant - dans le nom de la zone indiquer **webcourses.sio –** suivant – dans l'@IP indiquer l'@IP du serveur DNS primaire à savoir **192.168.0.200** – ajouter – suivant- terminer

2.3. Configurer le serveur DNS primaire ou maître afin qu'il puisse être répliqué sur le serveur DNS secondaire

- Sur le Serveur primaire, retourner sur le service DNS – zones de recherches directes - faire clic droit sur **webcourses.sio** – propriété – cliquer sur l'onglet transfert de zone – cocher autoriser les transferts de zones et cocher uniquement vers les serveurs suivants – saisir l'@IP du serveur DNS secondaire – ajouter – appliquer - ok -

- Retourner sur le service DNS – zones de recherches directes - faire clic droit sur **webcourses.sio** – propriété – cliquer sur l'onglet source de nom (SOA) – cliquer une fois sur incrémenter – positionner les intervalles à 30 secondes – l'expiration après 1 jour – durée de vie minimale à 1 heure – ok

- Retourner sur le service DNS – zones de recherches directes - faire clic droit sur **webcourses.sio– Actualiser**

2.4. Vérification du paramétrage afin de vérifier la synchronisation des serveurs

2.4.1. Se connecter au serveur DNS secondaire et vérifier que la base de données est synchronisée avec celle du serveur primaire.

2.5. Simulation d'une panne serveur DNS

2.5.1. Pour simuler une panne serveur ou un arrêt pour maintenance nous allons faire tomber le serveur DNS primaire pour vérifier que le DNS secondaire reprenne la main

2.5.2. Revenir sur le serveur DNS primaire – clic droit sur SERVEUR PRIMAIRE – toutes les tâches – arrêter

2.5.3. Sur les postes Poste Aadin et Poste client, dans la carte réseau, modifier l'@IP du serveur DNS pour les faire pointer sur le serveur DNS secondaire.

2.5.4. Sur chacun des postes clients modifiés, ouvrir l'invite de commande :
2.5.5. taper la commande ipconfig /all pour vérifier la prise en compte de la nouvelle configuration de la carte
2.5.6. la commande nslookup nom du poste et nslookup @IP

2.6. Répartition de charge

Afin de pouvoir répartir les requêtes au niveau des serveurs primaires et secondaires, il est intéressant de répartir les clients sur les différents serveurs.

2.7. Rajouter, dans le sous-réseau 192.172.16.0/24, 2 postes clients supplémentaires.
2.8. Configurer ces postes comme il se doit.
2.9. Pour les postes de ce sous-réseau, mettre la configuration suivante :
DNS primaire : 172.16.0.100
DNS secondaire : 192.168.0.200

2.10. Rajouter, dans le sous-réseau 192.168.0.0/24, 2 postes clients supplémentaires.
2.11. Configurer ces postes comme il se doit.
2.12. Pour les postes de ce sous-réseau, mettre la configuration suivante :
DNS primaire : 172.16.0.100
DNS secondaire : 192.168.0.200

2.13. ouvrir Wireshark sur les deux serveurs et les postes clients et lancer les demandes de captures
2.14. Demander les résolutions d'adresse pour chacun des postes

2.15. Observer la distribution des requêtes

3ème partie Cibler l'intérêt d'un DNS dynamique et évolutif Pour la maintenance

Contexte

Comme nous venons de le voir, pour passer d'un serveur DNS primaire à un serveur DNS secondaire, il faut changer l'@IP manuellement sur chacun des postes clients.
De plus, si un serveur DNS est associé à un serveur DHCP sur un réseau, il se peut qu'en changeant le nom d'un poste, ou une @IP, le mappage ne fonctionne plus si l'on est en statique.
Dans le cas d'un parc informatique important, cela devient vite ingérable.
La solution consiste donc à transformer le DNS statique en un DNS dynamique et évolutif.

3. Configuration du serveur DNS primaire

- Redémarrer le serveur primaire– clic droit sur SERVEUR PRIMAIRE – toutes les tâches – démarrer

- Clic droit sur **webcourses.sio–** propriétés – sur l'onglet général, dans le menu **mises à jour dynamiques** choisir l'option **non sécurisés et sécurisés –** appliquer – ok

- Sur le Serveur primaire, aller démarrer – poste de travail – clic droit sur poste de travail – propriété – nom de l'ordinateur – modifier – autres – dans la zone suffixes DNS principal de cet ordinateur saisir **webcourses.sio–** appliquer – ok

- Arrêter et Redémarrer le Serveur primaire

3.1. Configuration des postes clients

- Aller dans la carte réseau – propriété – avancé - DNS – cocher utiliser le service DNS de cette connexion pour l'enregistrement DNS – vérifier que la zone « **ajouter ces suffixes DNS** » est bien cochée et que la valeur **webcourses.sio** est bien saisie dans la zone suffixe DNS pour cette connexion – ok – positionner 172.16.0.100 comme @IP pour le serveur DNS préféré et 192.168.0.200 dans le serveur DNS auxiliaire – changer l'@IP avec 172.16.0.27 pour Poste Admin et 192.168.10.45 pour Poste client

- Sur le Poste Admin et le poste cleint, aller dans démarrer – poste de travail – clic droit sur poste de travail – propriété – nom de l'ordinateur – modifier – autres – dans la zone suffixes DNS principal de cet ordinateur saisir web**courses.sio–** appliquer – ok

- Arrêter et Redémarrer les postes Poste Admin et Poste client

- Ouvrir l'invite de commande et faire ipconfig /all pour vérifier la prise en compte de la nouvelle configuration de la carte

- Afin de prendre en compte la nouvelle configuration des cartes réseau, sur l'invite de commande de chacun des postes clients, faire ipconfig /registerdns

3.2. Vérification du paramétrage

- Aller sur le Serveur primaire – clic droit sur web**courses.sio-** actualiser
- Vous devez voir apparaître votre nouvelle configuration d'@IP
- Aller sur le Serveur secondaire - clic droit sur web**courses.sio-** actualiser
- Vous devez voir apparaître votre nouvelle configuration d'@IP

- Sur le Serveur primaire, supprimer de votre base de données les postes Poste Admin et Poste client
- Faire actualiser et vérifier que la mise à jour a été prise en compte
- Sur le Serveur secondaire, clic droit sur web**courses.sio-** actualiser
- Vérifier que la mise à jour a été prise en compte par copie

Arrêter les postes Poste Admin et Poste client puis les redémarrer

Sur le serveur DNS primaire et secondaire, faire actualiser et vérifier que la base s'est mise à jour dynamiquement.

4ème partie
Montrer l'intérêt de contrôler le trafic DNS à travers La mise en place d'une Délégation et d'une redirection

4. Redirection

4.1. Domaine webcourses.sio

Nous allons considérez que le domaine **webcourses.sio,** sur le Serveur primaire ayant comme @IP 192.168.2.2, sera le domaine enfant.
Nous rappelons aussi que la zone **webcourses.sio** contient entre autre le mappage des postes Poste client **webcourses.sio** et Serveur contrôleur de domaine. **webcourses.sio**

De manière à créer un domaine parent sur le serveur secondaire, il faut d'abord supprimer la zone secondaire **webcourses.sio** sur ce serveur secondaire**.**

4.1.1. Création d'un domaine parent appelé courses.sio sur le serveur secondaire

4.1.2. Création d'une zone de recherche directe

Démarrer – Outils d'administration – DNS – clic droit sur Zone de recherche directe - Nouvelle zone – suivant - Zone principale – Saisir courses.sio– suivant – ne pas autoriser les mises à jour – suivant – terminer

4.1.3. Créer une zone de recherche Inversée

Démarrer – Outils d'administration – DNS – clic droit sur Zone de recherche Inversée – Nouvelle zone – suivant - Zone principale – ID réseau 192.168.1 Suivant - Ne pas autoriser les mises à jour – suivant – terminer

4.1.4. Création des mappages

Clic droit sur la zone **courses.sio– nouvel hôte** – saisir le nom du poste client et son adresse d'IP **192.168.10.50** – ajouter un hôte – cocher l'option créer un pointeur d'enregistrement PTR - terminé
Pensez à actualiser les modifications.

4.1.5. la résolution des noms

4.1.6. Sur le poste B, ouvrir une fenêtre de DOS, puis saisir **nslookup Poste client**

Quel est le résultat de la commande ? Pourquoi ?

Recommencer l'opération mais en saisissant le nom FQDN du poste B

Quel est le résultat de la commande ?

4.1.7. la résolution inversée à l'aide de la commande **nslookup 192.168.10.50**

Quel est le résultat de la commande ? Pourquoi ?

4.1.8. L'ajoute la suffixe dans la propriété TCP/IP sur le poste client

Panneau de configuration – connexion réseau – clic droit sur carte réseau – Propriété – Protocole Internet - Propriété – Avancé – DNS – Ajouter ces suffixe DNS – Saisir **courses.sio**– dans Suffixe DNS pour cette connexion - Saisir **courses.sio**
Ok – ok – terminé

Faites la résolution des noms à l'aide de la commande **nslookup 192.168.10.50** sur le poste client

Quel est le résultat de la commande ? Pourquoi ?

Quel est le nom du serveur DNS ? _____

4.1.9. Remédier s'il le faut

4.2. Délégation

4.2.1. Sur le poste client, vous essayez de résoudre **nslookup Poste Admin.webcourses.sio**

Quel est le résultat de la commande ? Pourquoi ?

Afin que le serveur DNS du client **Poste client** puisse interroger le serveur d'autorité de la zone **webcourses.sio** qui est le domaine enfant de **courses.sio,** il est nécessaire de créer une **délégation** à partir de la zone **courses.sio**.

Pour cela, sur le serveur secondaire, il faut aller dans :

Démarrer – Outils d'administration – DNS – clic droit sur Zone de recherche directe – nouvelle délégation – suivant **–** saisir **bts** dans domaine délégué – suivant – Ajouter le nom du serveur **Serveur Primaire.webcourses.sio en faisant parcourir (**l'**@**IP correspondante se place automatiquement) – suivant – terminer – actualisation.

4.2.2. Sur le poste B, vous essayez de résoudre à nouveau le nom **Poste Admin.webcourses.sio**

Quel est le résultat de la commande ? Pourquoi ?

4.2.3. Sur le Poste A, vous essayez de résoudre le nom **Poste client.courses.sio**

Quel est le résultat de la commande ? Pourquoi ?

Afin que le serveur DNS du client **Poste Admin** puisse interroger le serveur d'autorité de la zone **courses.sio** qui est le domaine parent de **webstgab.local**, il faut créer une redirection à partir du serveur DNS de la zone **webcourses.sio** sur le Serveur primaire**.**

4.2.4. Sur le Serveur primaire faire :

Clic droit sur serveur DNS - propriété - redirecteur – nouveau – saisir le nom du domaine parent **courses.sio**– saisir l'adresse IP du serveur DNS parent **172.16.0.100** - Ajouter – ne pas cocher l'option **ne pas utiliser la récursivité pour ce domaine** – appliquer - ok

4.2.5. Recommencer le Poste client de résolution de nom avec **Poste client.courses.sio**

Quel est le résultat de la commande ? Pourquoi ?

Mission 6 Documenter le service DNS

Compétences	Reprendre toutes les compétences relatives aux différentes missions
Objectifs	Documenter DNS
Vocabulaire à connaître	
Évaluation	Compte-rendu à rendre pour évaluation sommative coefficient 2 Compte-rendu est à poser dans votre PFC Épreuve E4 certificative

Page de garde

4. **L'entête de chaque page doit contenir les informations suivantes :**
   8. Nom de l'établissement
   9. Titre complet de l'activité
   10. La version du document

5. **Le pied de chaque page doit contenir les informations suivantes :**
   11. L'auteur / les auteurs
   12. Numéro de page
   13. Date

6. **Au centre de la page**
   14. Donner l'objectif principal de l'activité

Sommaire ou table des matières

2. **Automatiser** votre sommaire

Introduction

2. **Présenter**
   2.1. le contexte sur lequel vous travaillez (Description de la ligue de marathon)
   2.2. Description de son logo (celui que vous avez choisi sur votre site) représentation, symbole, lien Internet si vous l'avez récupéré sur une bibliothèque d'images

Déroulé de la mission 5

1. **Donner** le schéma réseau global associé au contexte des missions 5
2. **Préciser** les contraintes liées aux Prérequis si nécessaires
1. **Notifier** les points de vigilance de chaque mission
2. **Expliquer** les points de blocage et les solutions apportées
3. **Montrer** à l'aide d'une copie écran les résultats obtenus après les mises en place des missions

Analyse de l'activité

4. **Spécifier** les difficultés rencontrées au cours des différentes phases de mise en place
5. **Mentionner** les apports professionnels acquis à travers cette expérience
6. **Préciser** les apports personnels acquis à travers cette expérience

Mission 7 Installer et paramétrer un service DHCP

Compétences	
Objectif principal	**Gérer** un service DHCP
Objectifs intermédiaires	**Installer** et configurer le service DHCP **Montrer** le rôle de l'agent relais
Vocabulaire à connaître	
Évaluation	Épreuve E4 certificative

Votre mission

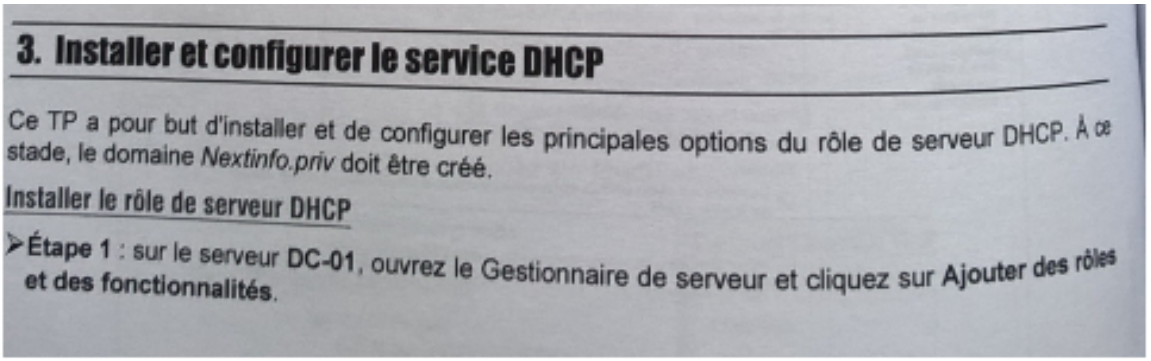
Installer et **paramétrer** le service DHCP

Information utile

Poste administrateur : par DHCP
Serveur DHCP primaire : 172.16.0.100/24
Nom de la machine srvaddns
un poste client : par DHCP

Guide d'installation

1. Démarrer le service



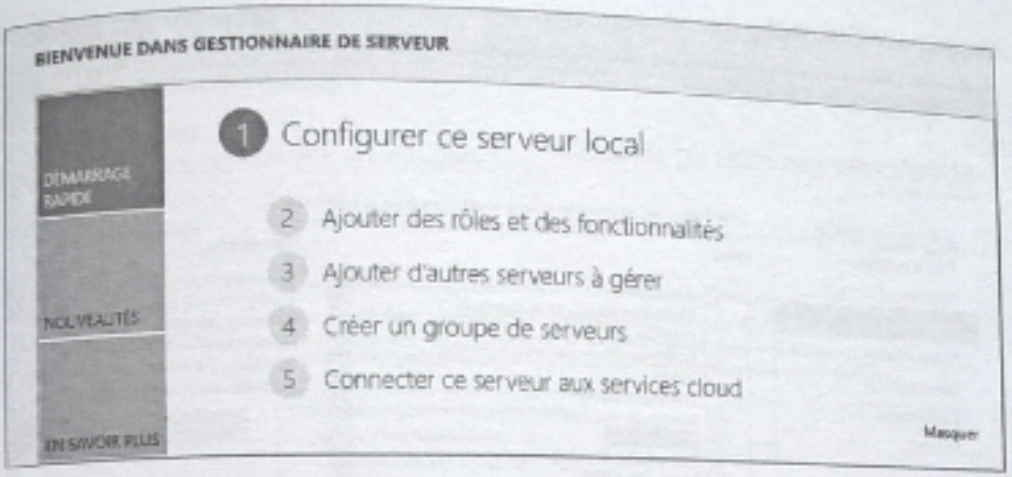
3. Installer et configurer le service DHCP

Ce TP a pour but d'installer et de configurer les principales options du rôle de serveur DHCP. À ce stade, le domaine *Nextinfo.priv* doit être créé.

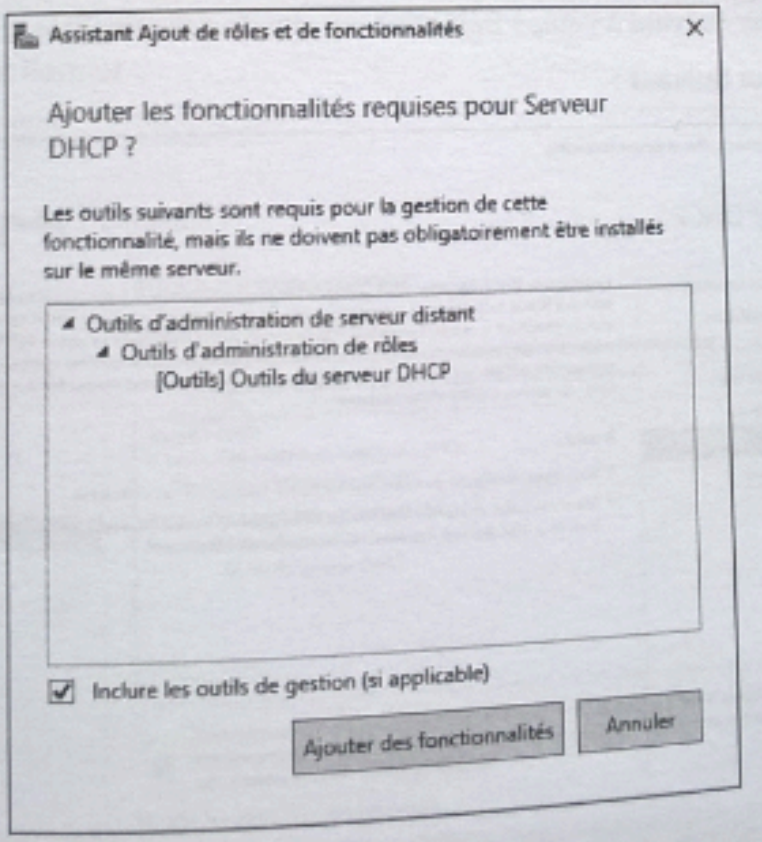
Installer le rôle de serveur DHCP

➢ **Étape 1** : sur le serveur **DC-01**, ouvrez le Gestionnaire de serveur et cliquez sur **Ajouter des rôles et des fonctionnalités**.

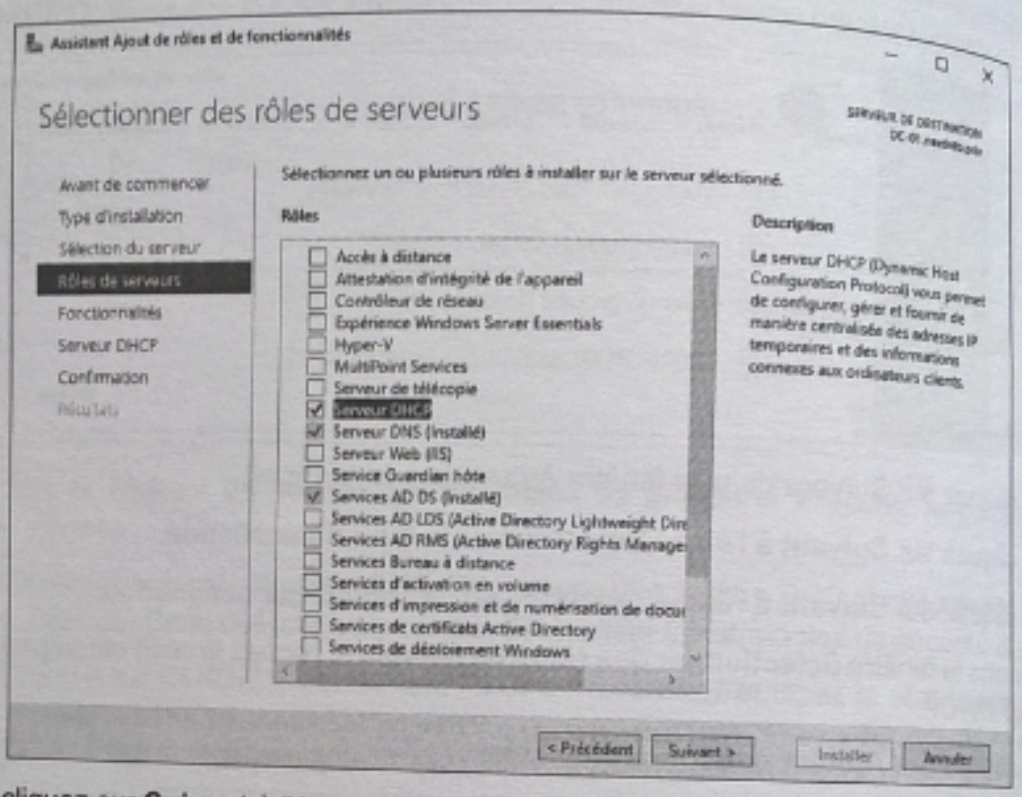
Remplacer dc-01 par srvaddns



- **Étape 2** : cliquez sur **Suivant** dans la fenêtre **Avant de commencer**.
- **Étape 3** : cliquez sur **Suivant** à l'étape **Sélectionner le type d'installation**.
- **Étape 4** : cliquez sur **Suivant** à l'étape **Sélectionner le serveur de destination**.
- **Étape 5** : dans la fenêtre **Sélectionner des rôles de serveurs**, cochez la case correspondant au rôle de **Serveur DHCP**.
- **Étape 6** : cliquez sur **Ajouter des fonctionnalités** :

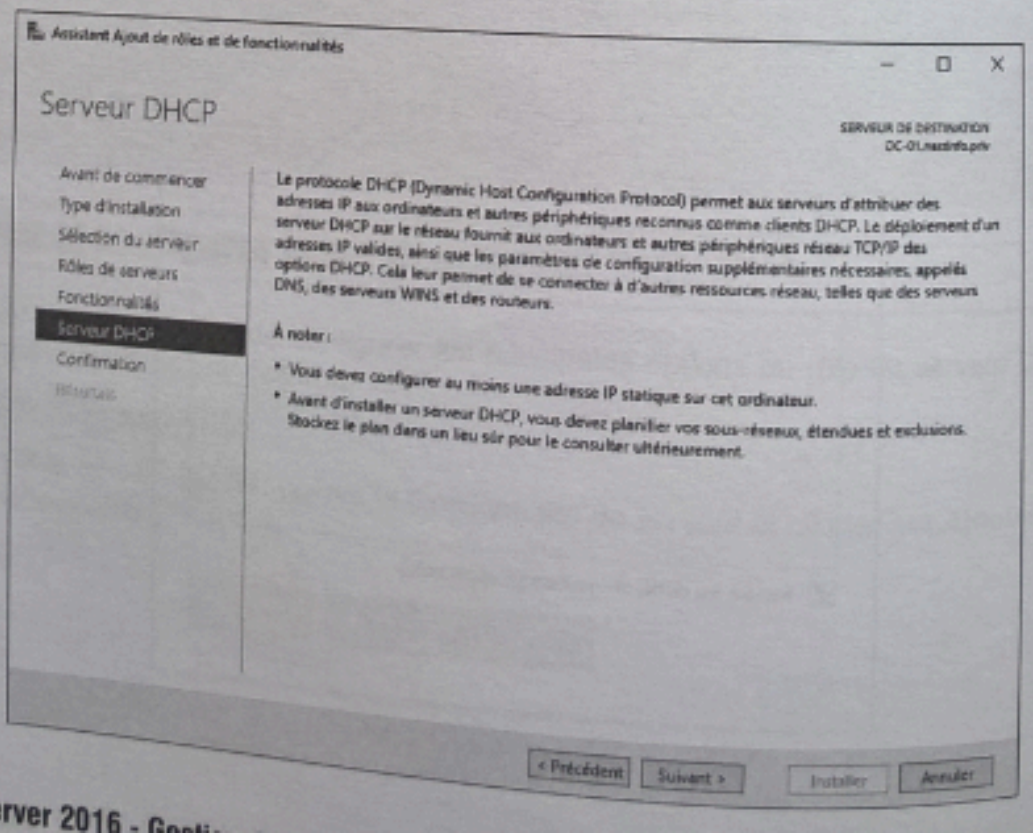


➢ **Étape 7** : cliquez sur **Suivant** :



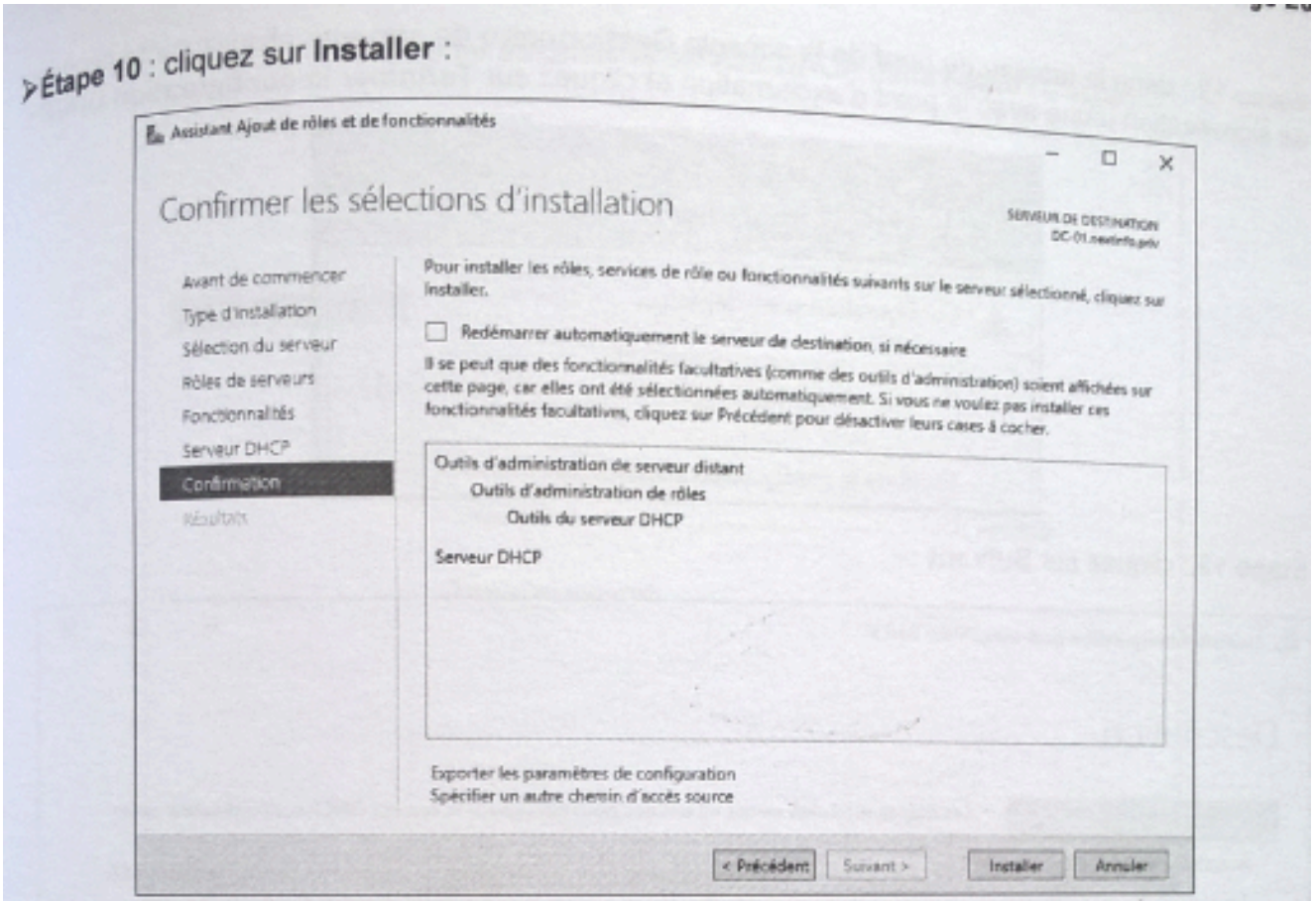
➢ **Étape 8** : cliquez sur **Suivant** à l'étape **Sélectionner des fonctionnalités**.

➢ **Étape 9** : cliquez sur **Suivant** :

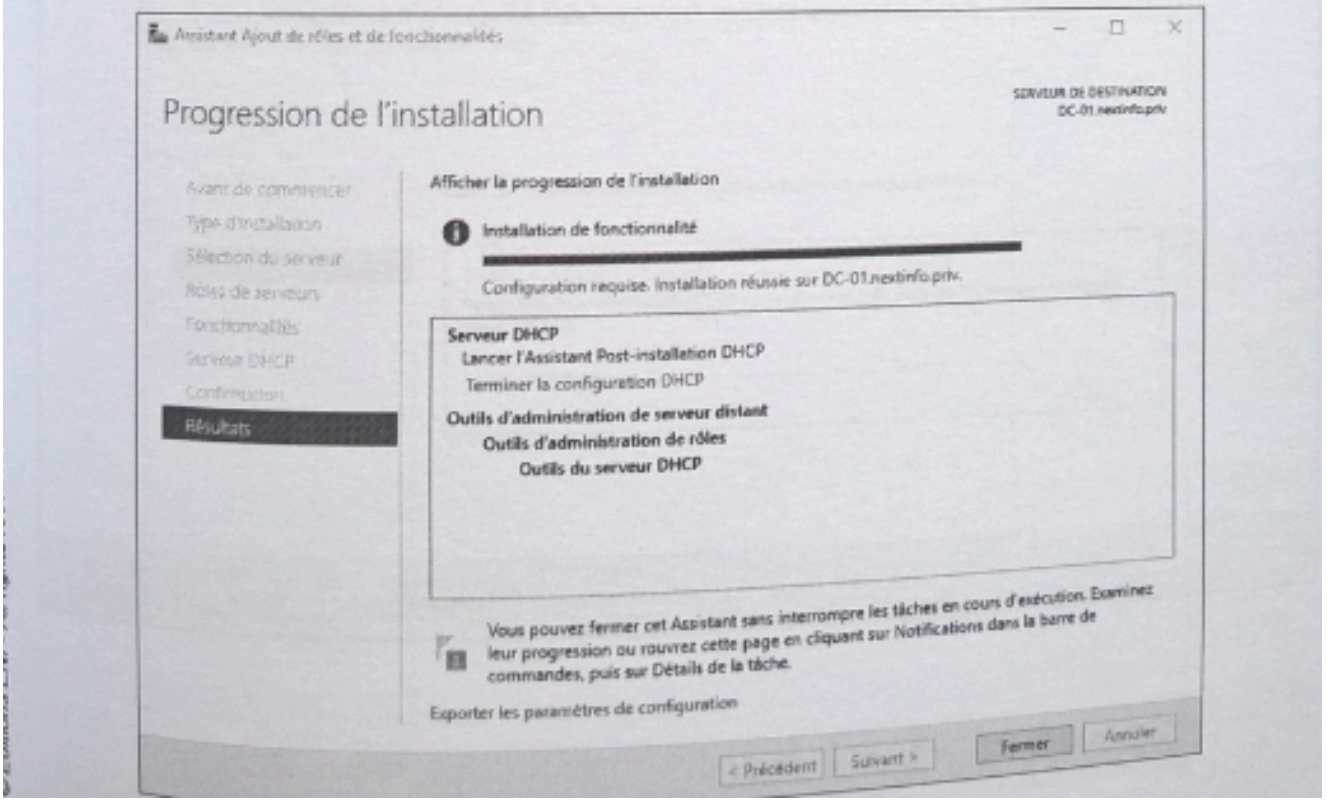


Windows Server 2016 - Confi...

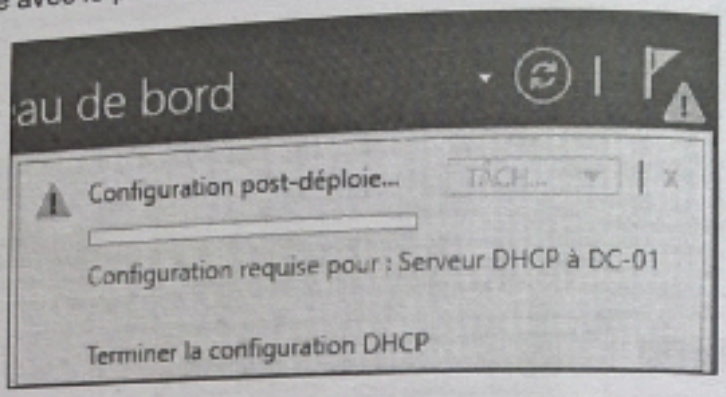
➢ **Étape 10** : cliquez sur **Installer** :



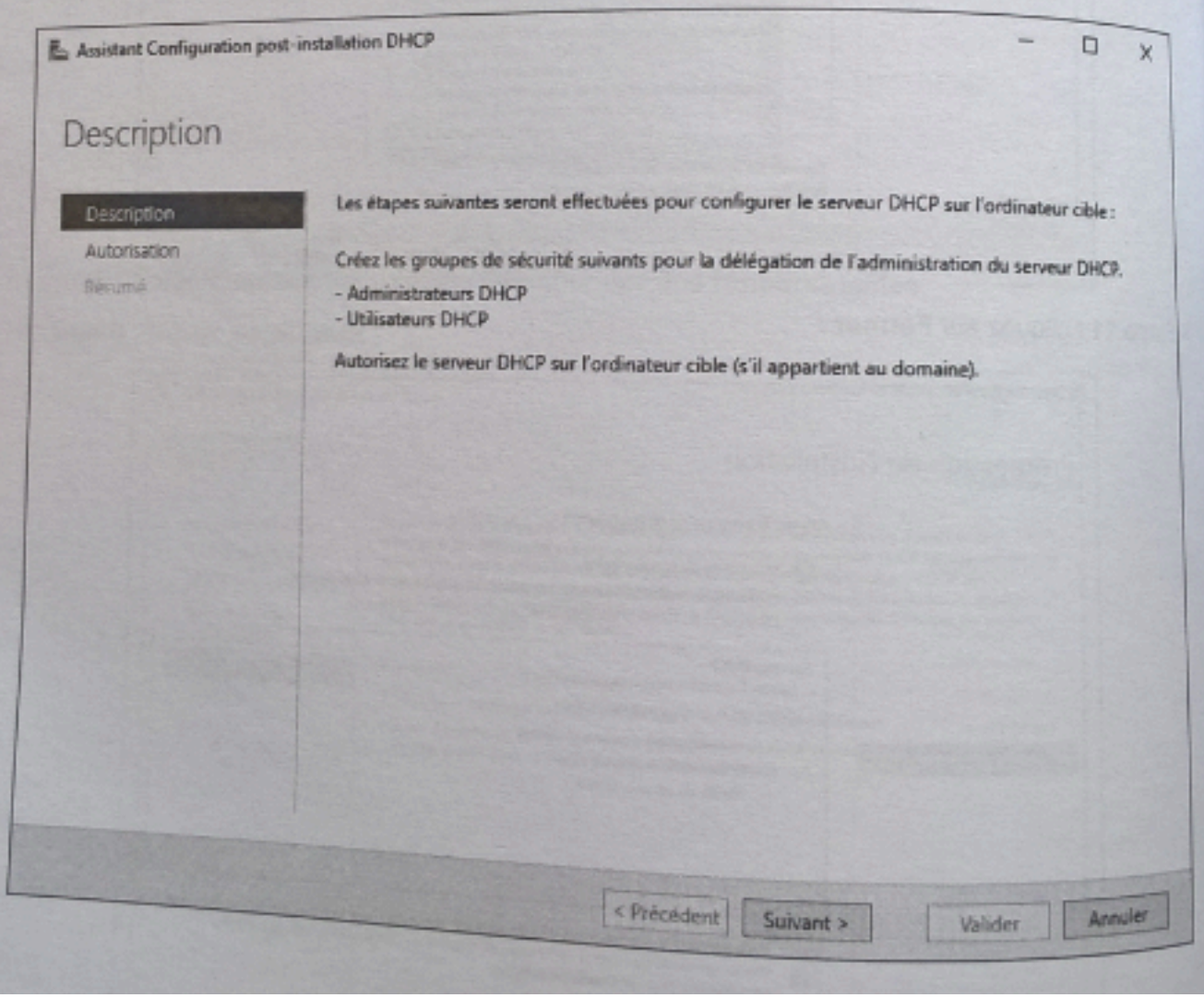
➢ **Étape 11** : cliquez sur **Fermer** :



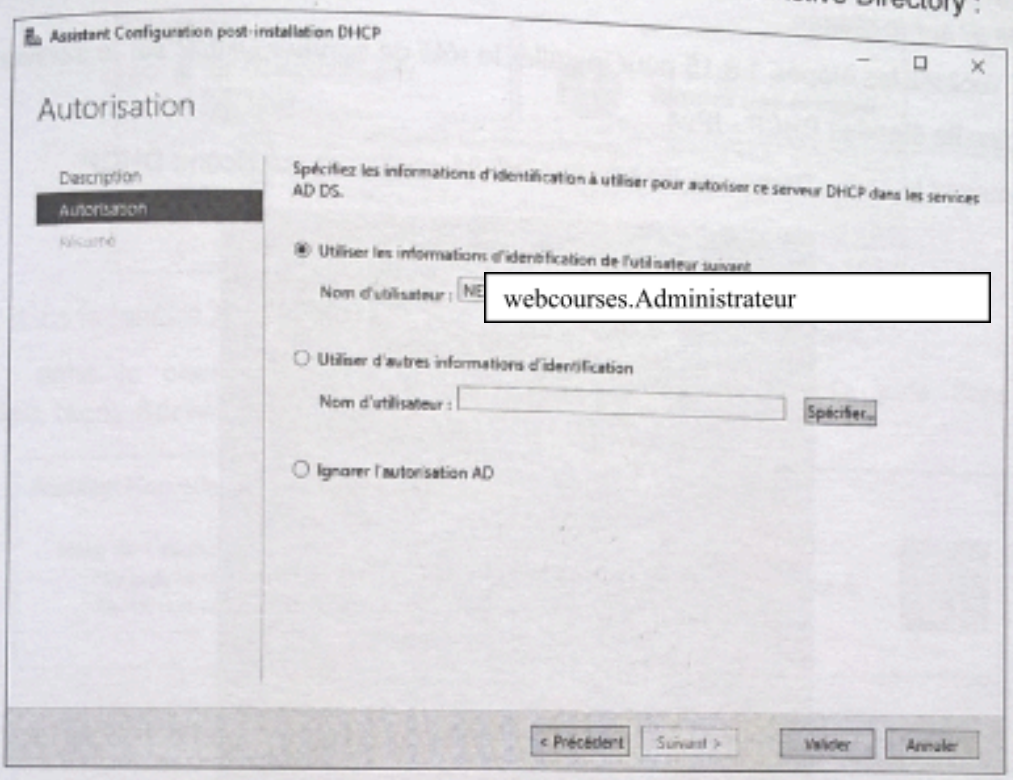
➢ **Étape 12** : dans le tableau de bord de la console **Gestionnaire de serveur**, cliquez sur le panneau de signalisation jaune avec le point d'exclamation et cliquez sur **Terminer la configuration DHCP** :



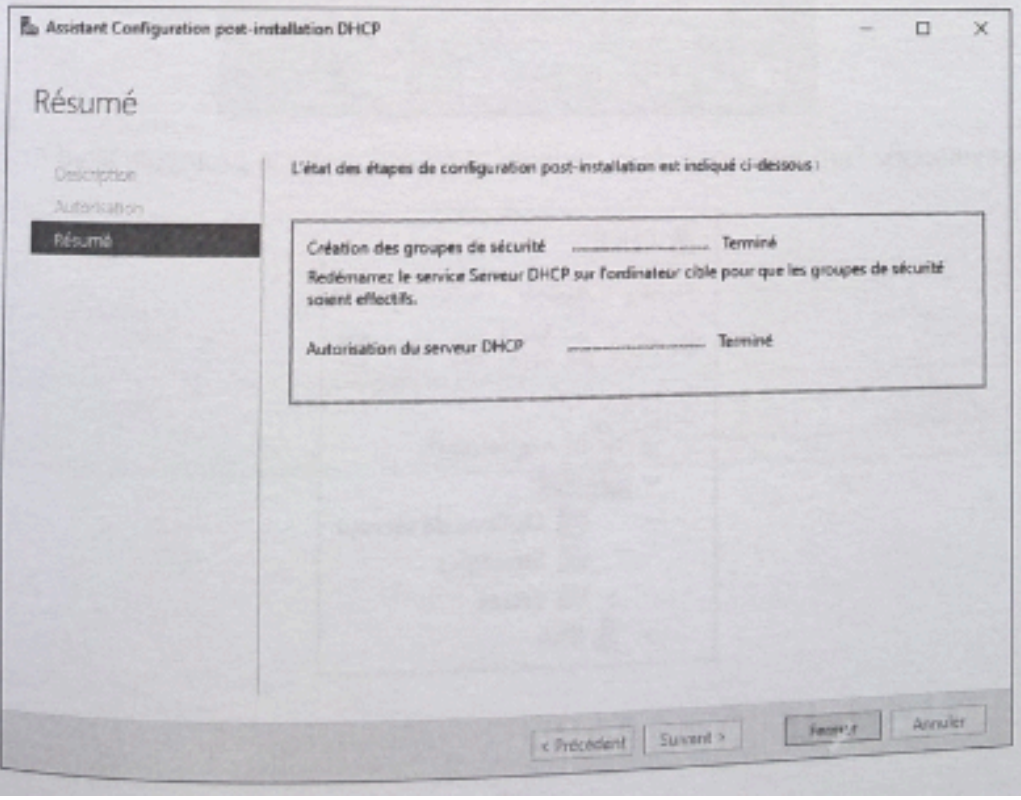
➢ **Étape 13** : cliquez sur **Suivant** :



➢**Étape 14** : cliquez sur **Valider** pour autoriser le serveur DHCP dans Active Directory :



➢**Étape 15** : cliquez sur **Fermer** :



2. Configuration du service

3. Configuration d'une étendue : ATTENTION une étendue / réseau

Clic droit sur serveur DHCP – nouvelle étendue – suivant – remplir les champs demandés – suivant – remplir les champs plage IP et le masque du réseau (exemple : plage d'@ IP de 192.168.10.1 à 192.168.10.50 (correspondant au vélo) avec un masque par défaut à 255.255.255.0 car il s'agit d'une classe C) – exclure les @ IP s'il y a lieu (par exemple l'@ IP d'une imprimante ou d'un serveur) – **pour notre activité mettre le bail à 2 mn** – suivant – cocher OUI je veux configurer

Ces options maintenant – suivant – saisir l'@ IP de la passerelle correspondant au LAN sur lequel on travaille – faire suivant jusqu'à obtenir le bouton terminer – actualiser

4. Demander une @ IP dynamique pour un poste client

A FAIRE SUR CHACUN DES POSTES CLIENTS

Il faut passer une @IP fixe en IP dynamique. Pour se faire aller dans :

a) Propriété du protocole internet TCP/IP – propriété – générale cocher l'option obtenir une @ IP automatiquement.

b) Ouvrir l'invite de commande et taper :

Ipconfig /release pour résilier le bail existant ou l'initialiser

Ipconfig /renew pour demander une @ IP dynamique via le serveur DHCP

Ipconfig /all pour vérifier la configuration de la carte réseau (@ IP – masque – passerelle)

c) Vérifier via la commande PING la connectivité globale de l'ensemble du réseau.

5. Ajouter l'agent de relais

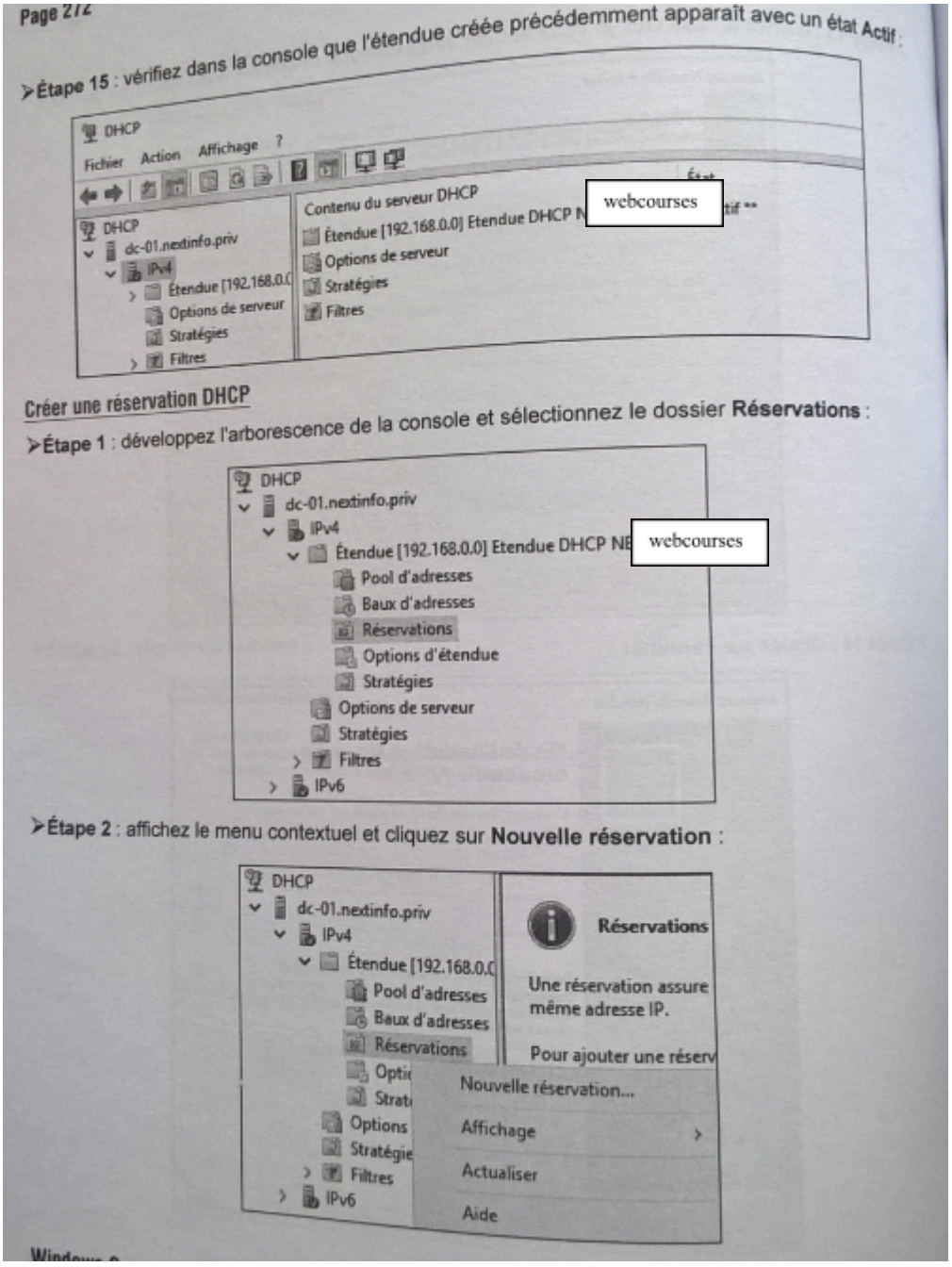
Pour se faire aller dans :

Démarrer – outils d'administration - Routage et accès distant – clic droit – ajouter un serveur – cet ordinateur - OK
Cliquer sur serveur local – routage IP – clic droit sur Général – nouveau protocole de routage – Agent de relais DHCP – OK

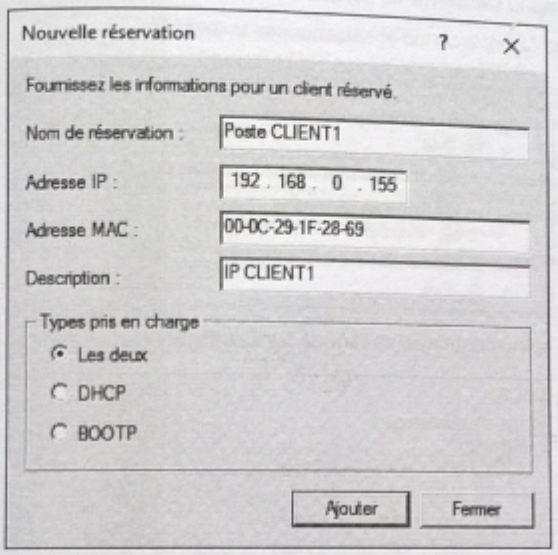
6. Configuration de l'agent de Relais

Clic droit sur Agent de Relais – nouvelle interface – choisir l'étendue se trouvant en dehors du Lan du serveur DHCP –

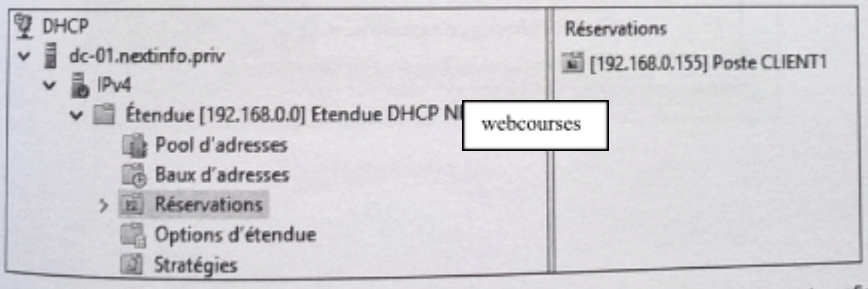
Clic droit sur Agent de Relais – propriétés – donner l'@ IP fixe du serveur DHCP qui devra desservir les @ IP.
Attention : s'il y a plusieurs serveurs DHCP possibles, rentrer toutes les @ IP des serveurs (cas de backup par exemple).



➢ **Étape 3** : tapez le nom de réservation **Poste CLIENT1**, l'adresse IP **192.168.0.155**, l'adresse MAC correspondante à la carte réseau de votre machine virtuelle CLIENT1 et la description **IP CLIENT1** puis cliquez sur **Ajouter**, puis sur **Fermer** :



➢ **Étape 4** : vérifiez que la réservation d'adresse IP pour le poste CLIENT1 apparaît :



➢ **Étape 5** : connectez-vous sur le poste **CLIENT1** et assurez-vous que la carte réseau est configurée pour recevoir une adresse IP automatiquement. Tapez ensuite la commande `ipconfig /renew`.

➢ **Étape 6** : tapez la commande `ipconfig`, et vérifiez que l'adresse IP est bien **192.168.0.155**.

Mission 8 Installer et configurer la haute disponibilité du service DHCP

Compétences	
Objectif principal	**Installer** et **configurer** la haute disponibilité du service DHCP
Objectifs intermédiaires	**Installer** la haute disponibilité du service DHCP **Configurer** la haute disponibilité du service DHCP
Vocabulaire à connaître	
Évaluation	Épreuve E4 certificative

Votre mission

Installer et **configurer** la haute disponibilité du service DHCP

Information utile

Poste administrateur : par DHCP
Serveur DHCP primaire : 172.16.0.100/24
Nom de la machine srvaddns
Serveur DHCP secondaire : 192.168.0.200/24 installer DHCP
Nom de la machine srvdns
un poste client : par DHCP

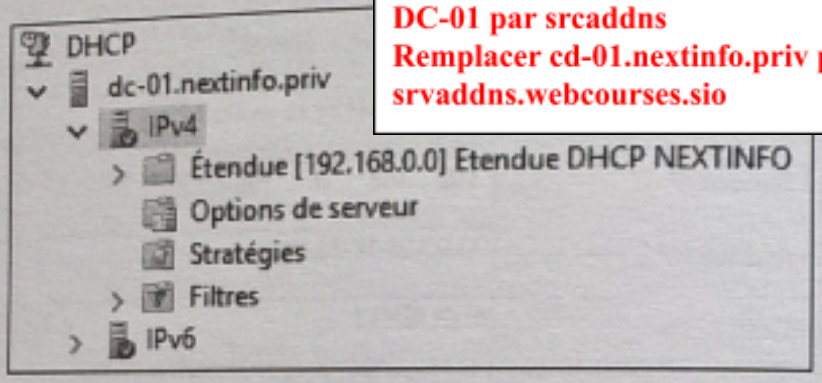
Guide d'installation

4. Installer et configurer la haute disponibilité du service DHCP

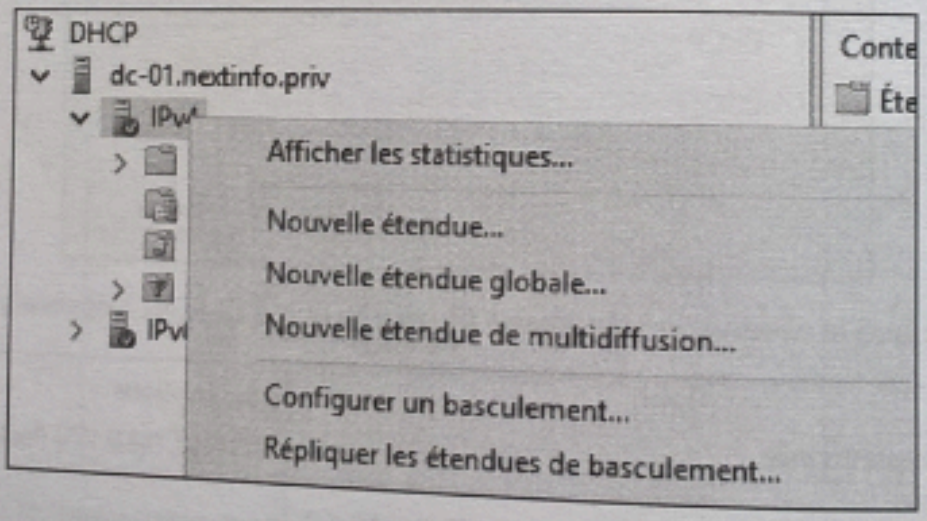
➢ **Étape 1** : ouvrez le menu **Démarrer** du serveur **DC-01** et cliquez sur l'icône **DHCP**.

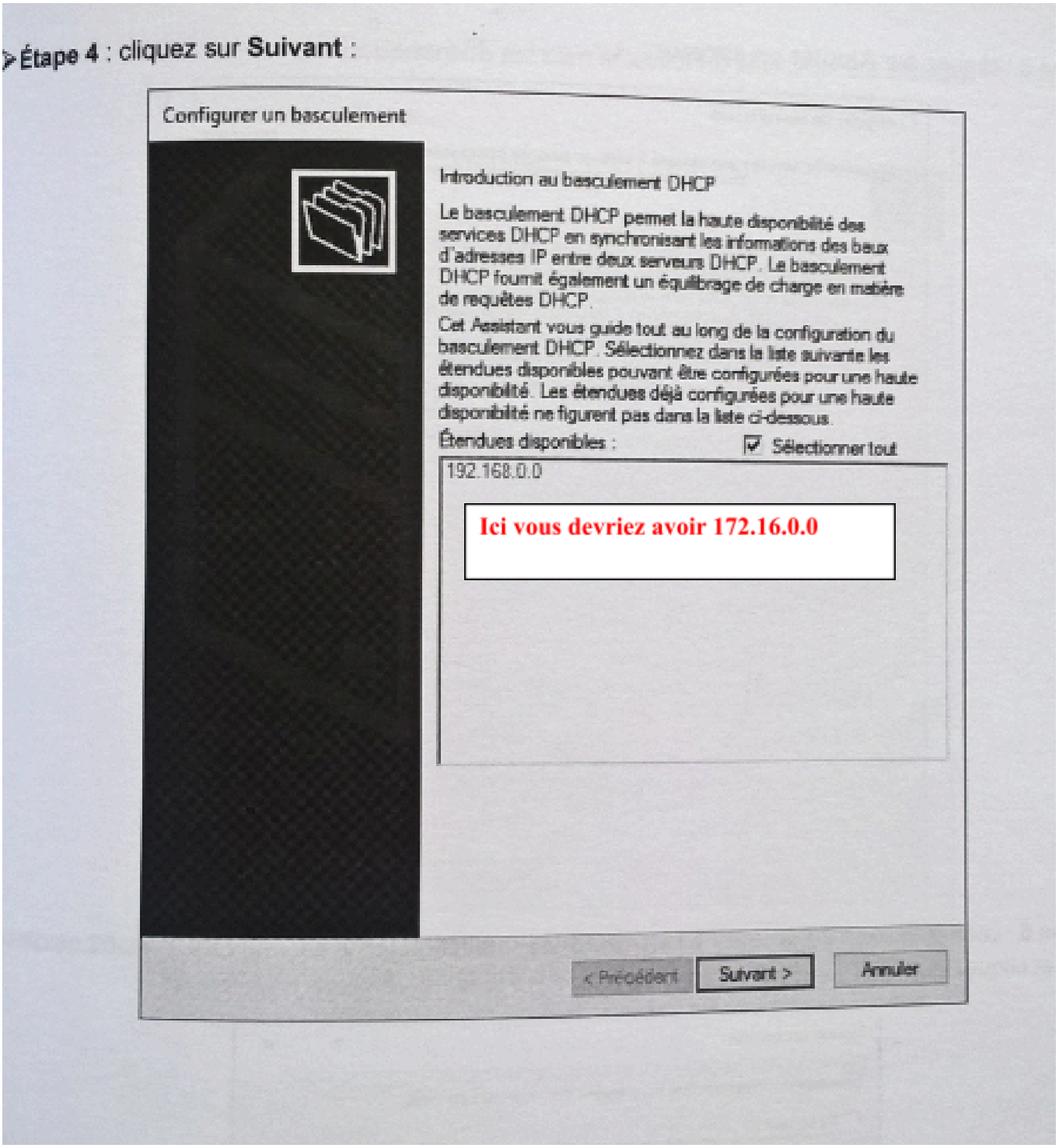
➢ **Étape 2** : développez l'arborescence et sélectionnez le protocole **IPv4** :

DC-01 par srcaddns
Remplacer cd-01.nextinfo.priv par srvaddns.webcourses.sio

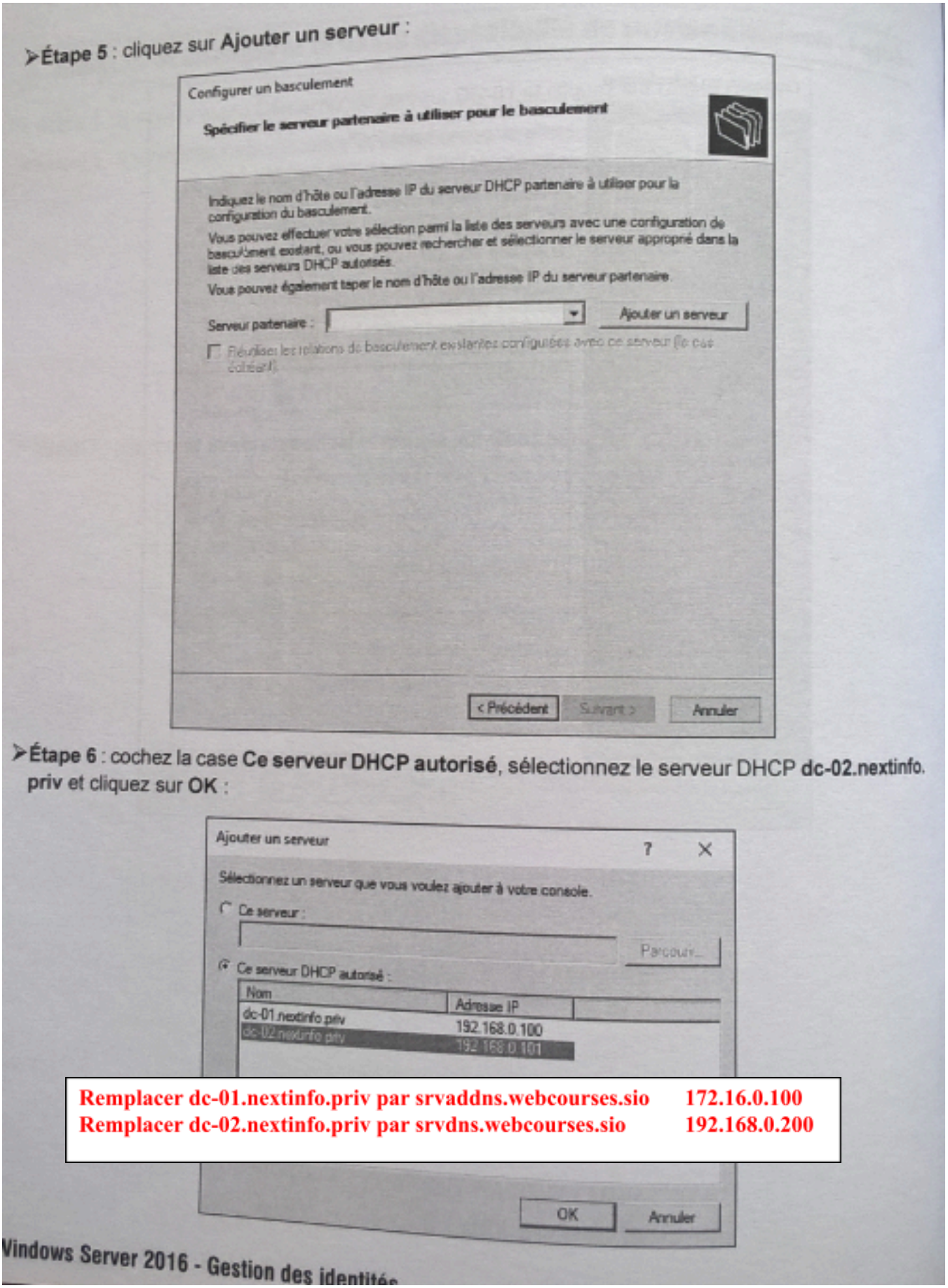


➢ **Étape 3** : affichez le menu contextuel et cliquez sur **Configurer un basculement...**.




Étape 4 : cliquez sur Suivant :
Configurer un basculement
Introduction au basculement DHCP
Le basculement DHCP permet la haute disponibilité des services DHCP en synchronisant les informations des baux d'adresses IP entre deux serveurs DHCP. Le basculement DHCP fournit également un équilibrage de charge en matière de requêtes DHCP.
Cet Assistant vous guide tout au long de la configuration du basculement DHCP. Sélectionnez dans la liste suivante les étendues disponibles pouvant être configurées pour une haute disponibilité. Les étendues déjà configurées pour une haute disponibilité ne figurent pas dans la liste ci-dessous.
Étendues disponibles :
Sélectionner tout
192.168.0.0
Ici vous devriez avoir 172.16.0.0
< Précédent
Suivant >
Annuler

➢ **Étape 5** : cliquez sur **Ajouter un serveur** :

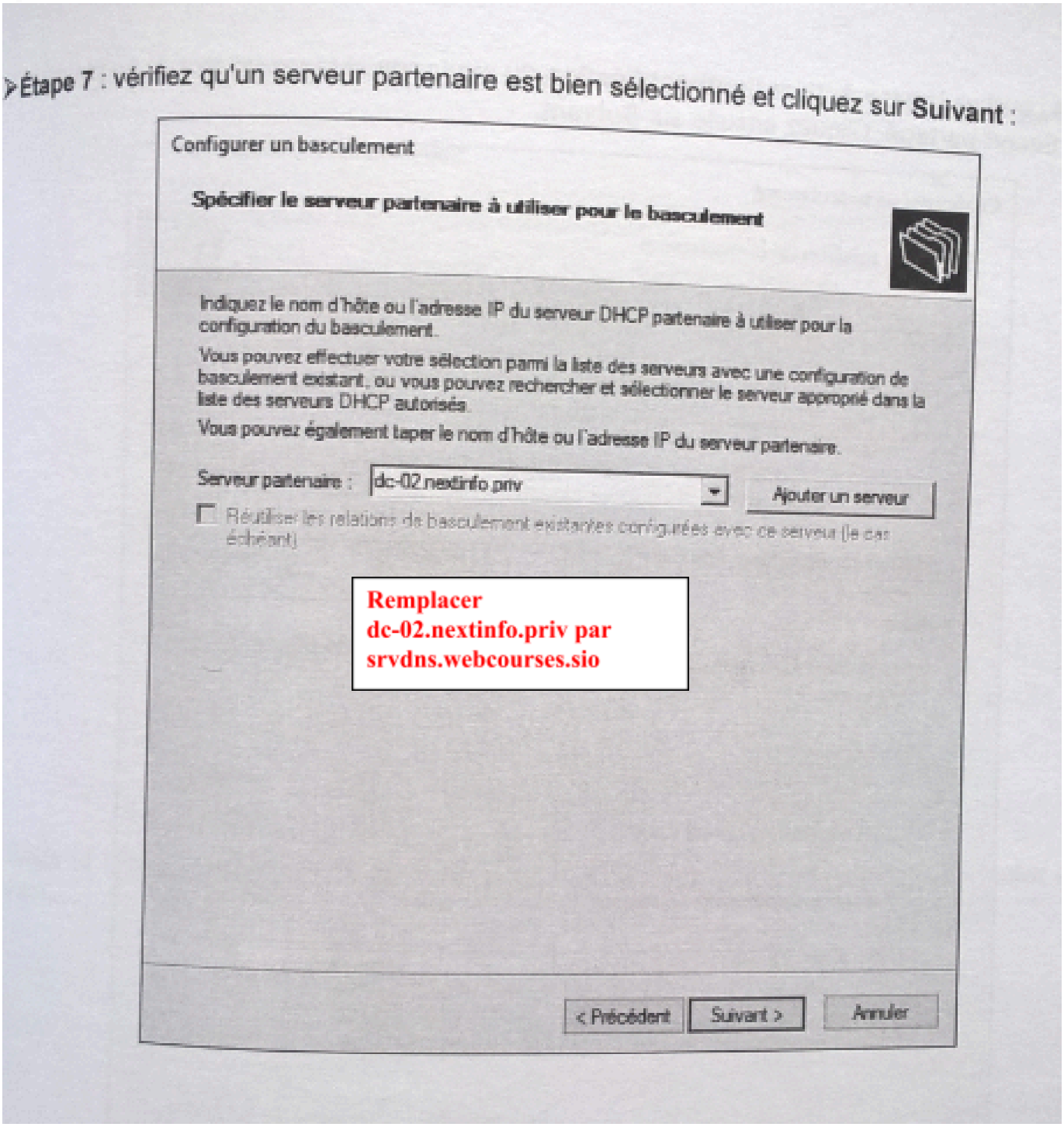


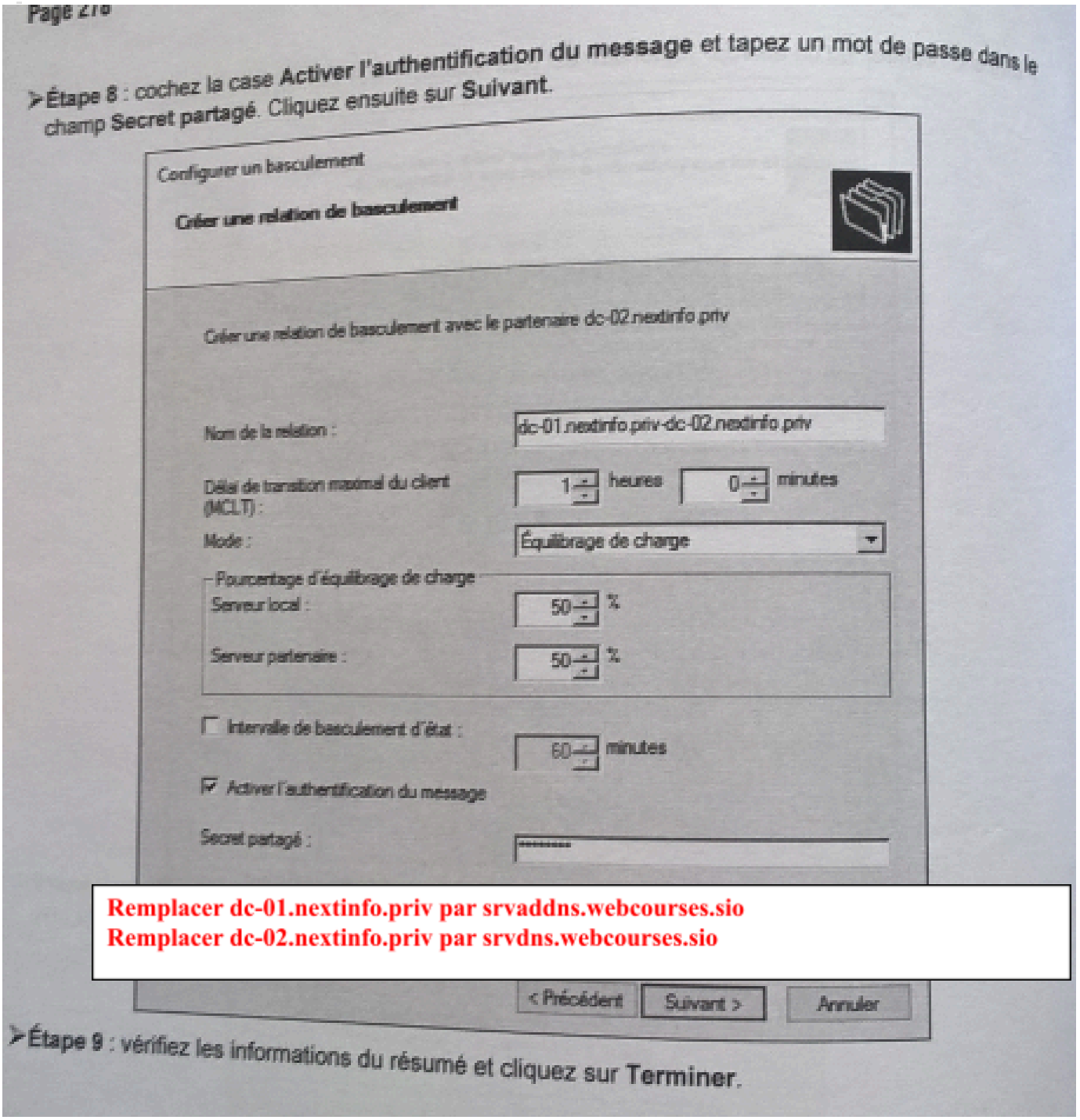
➢ **Étape 6** : cochez la case **Ce serveur DHCP autorisé**, sélectionnez le serveur DHCP **dc-02.nextinfo.priv** et cliquez sur **OK** :

Remplacer dc-01.nextinfo.priv par srvaddns.webcourses.sio 172.16.0.100
Remplacer dc-02.nextinfo.priv par srvdns.webcourses.sio 192.168.0.200

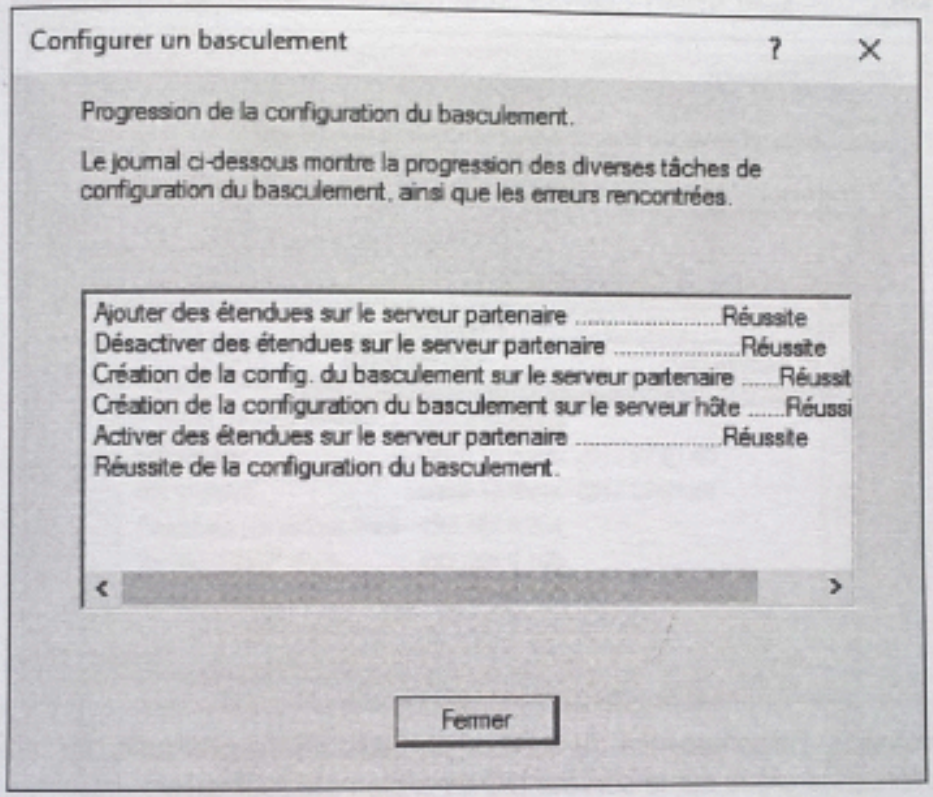
Windows Server 2016 - Gestion des identités

Étape 7 : vérifiez qu'un serveur partenaire est bien sélectionné et cliquez sur **Suivant** :

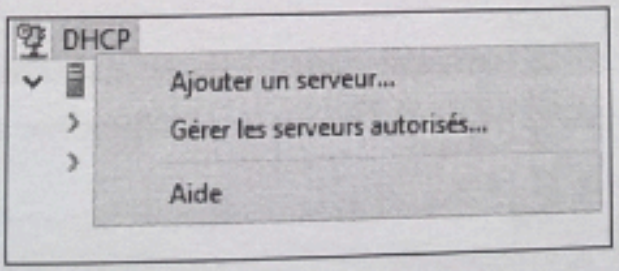



Page 270
➢Étape 8 : cochez la case Activer l'authentification du message et tapez un mot de passe dans le champ Secret partagé. Cliquez ensuite sur Suivant.
Configurer un basculement
Créer une relation de basculement
Créer une relation de basculement avec le partenaire dc-02.nextinfo.priv
Nom de la relation :
dc-01.nextinfo.priv-dc-02.nextinfo.priv
Délai de transition maximal du client (MCLT) :
1 heures
0 minutes
Mode :
Équilibrage de charge
Pourcentage d'équilibrage de charge
Serveur local :
50 %
Serveur partenaire :
50 %
Intervalle de basculement d'état :
60 minutes
Activer l'authentification du message
Secret partagé :
Remplacer dc-01.nextinfo.priv par srvaddns.webcourses.sio
Remplacer dc-02.nextinfo.priv par srvdns.webcourses.sio
< Précédent
Suivant >
Annuler
➢Étape 9 : vérifiez les informations du résumé et cliquez sur Terminer.

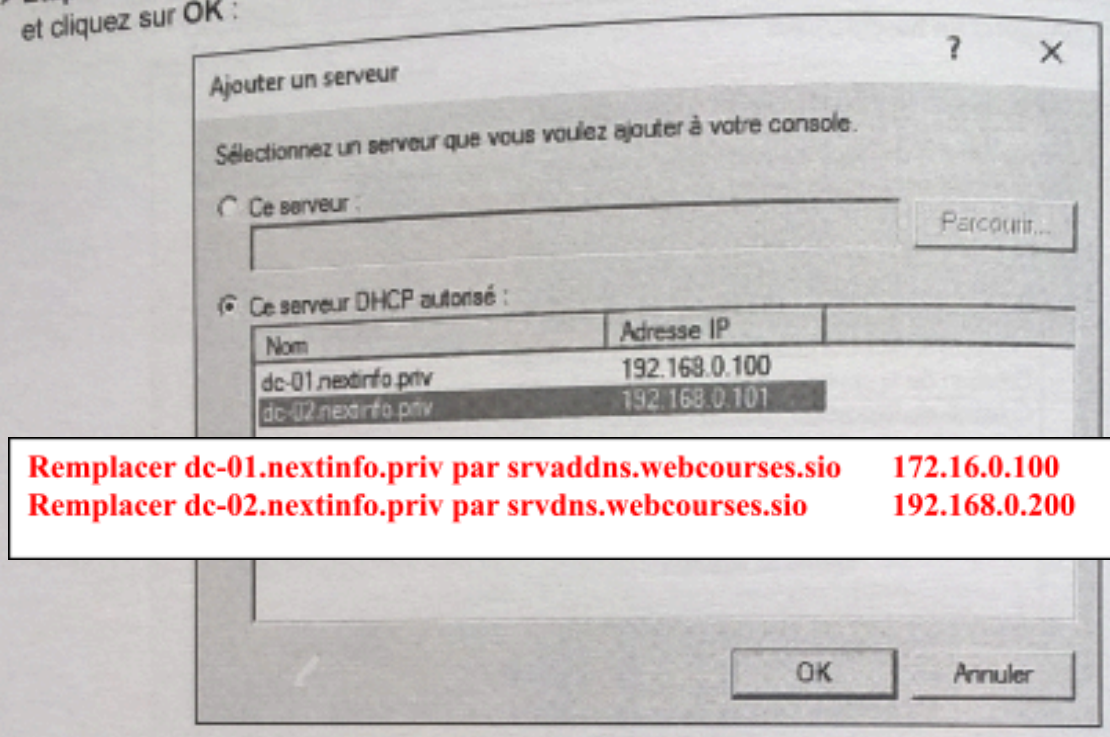
➢ **Étape 10** : assurez-vous de la réussite de chaque étape du basculement, puis cliquez sur **Fermer** :



➢ **Étape 11** : dans l'arborescence de la console, sélectionnez DHCP et cliquez sur **Ajouter un serveur...** :

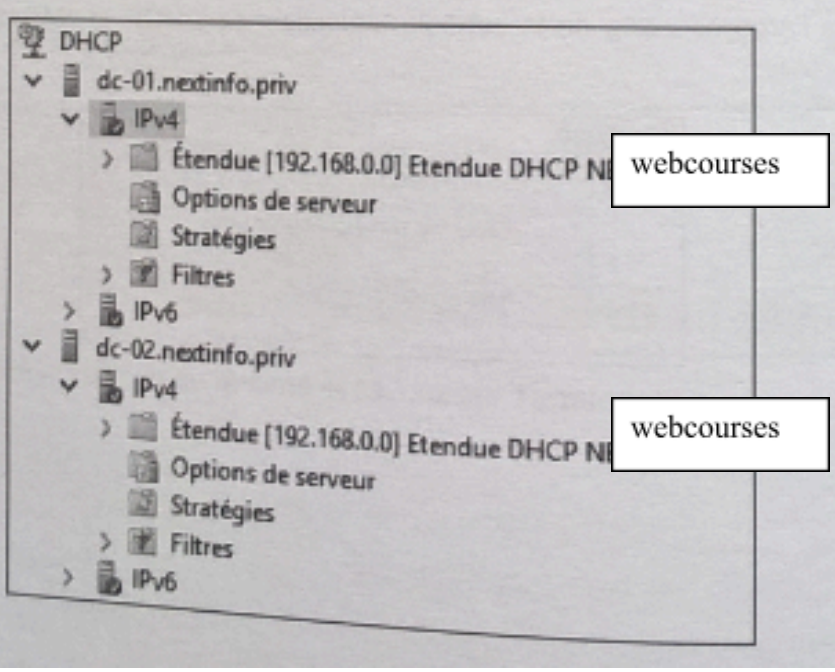


➢ **Étape 12** : cochez la case **Ce serveur DHCP autorisé**, sélectionnez le serveur **dc-02.nextinfo.priv** et cliquez sur **OK** :



Remplacer dc-01.nextinfo.priv par srvaddns.webcourses.sio 172.16.0.100
Remplacer dc-02.nextinfo.priv par srvdns.webcourses.sio 192.168.0.200

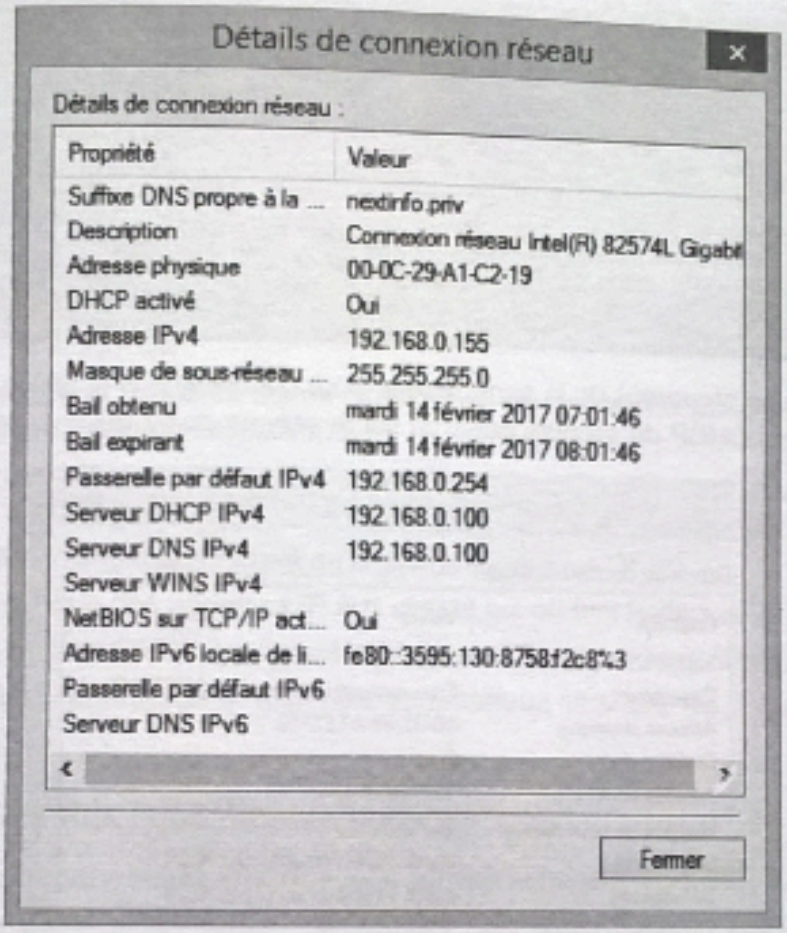
➢ **Étape 13** : développez l'arborescence du serveur **dc-02.nextinfo.priv** jusqu'au protocole **IPv4** afin de vérifier que l'étendue créée sur le serveur **DC-01** a bien été répliquée :



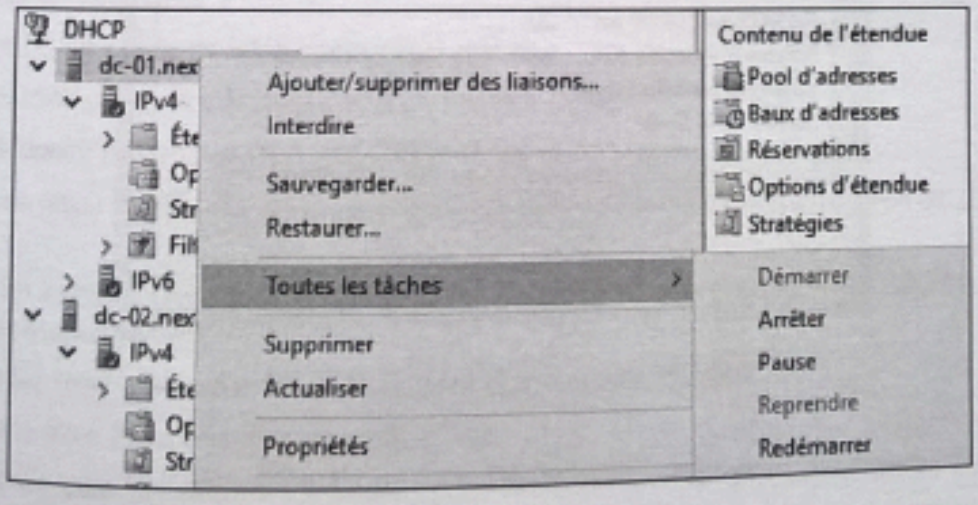
webcourses

webcourses

➢ **Étape 14** : ouvrez une session sur le poste **CLIENT1**, puis affichez les détails de connexion de la carte réseau. Identifiez et mémorisez l'adresse IP du **serveur DHCP IPv4** :



➢ **Étape 15** : basculez sur le serveur **DC-01**, puis dans la console DHCP, arrêtez le service sur le serveur **dc-01.nextinfo.priv** :

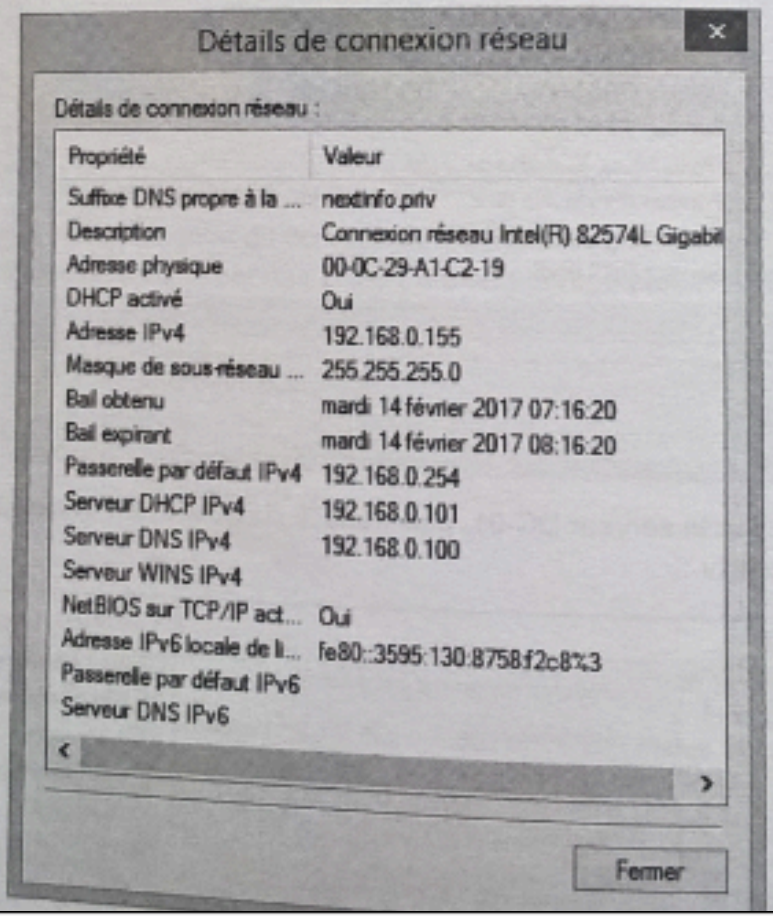


Remplacer DC_01 par srvaddns
Remplacer dc-01.nextinfo.priv par srvaddns.webcourses.sio

➢ **Étape 16** : basculez de nouveau sur le poste **CLIENT1** et exécutez consécutivement les commandes DOS suivantes **ipconfig /release** puis **ipconfig /renew**.

```
C:\Users\Administrateur.NEXTINFO>ipconfig /renew

Configuration IP de Windows

Carte Ethernet Ethernet0 :

   Suffixe DNS propre à la connexion. . . : nextinfo.priv
   Adresse IPv6 de liaison locale. . . . .: fe80::3595:130:8758:f2c8%3
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.0.155
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 192.168.0.254

C:\Users\Administrateur.NEXTINFO>
```

➢ **Étape 17** : affichez les propriétés de la carte réseau pour constater que le serveur DHCP IPv4 a bien basculé sur le serveur DHCP de secours hébergé sur le serveur dc-02.nextinfo.priv (192.168.0.101) :



Remplacer dc-02.nextinfo.priv par srvdns.webcourses.sio 192.168.0.200

Mission 9 Documenter DHCP et sa haute disponibilité

Compétences	Reprendre toutes les compétences relatives aux différentes missions
Objectifs	Documenter DHCP
Vocabulaire à connaître	
Évaluation	Compte-rendu à rendre pour évaluation sommative coefficient 2 Compte-rendu est à poser dans votre PFC Épreuve E4 certificative

Page de garde

7. **L'entête de chaque page doit contenir les informations suivantes :**
   15. Nom de l'établissement
   16. Titre complet de l'activité
   17. La version du document

8. **Le pied de chaque page doit contenir les informations suivantes :**
   18. L'auteur / les auteurs
   19. Numéro de page
   20. Date

9. **Au centre de la page**
   21. Donner l'objectif principal de l'activité

Sommaire ou table des matières

3. **Automatiser** votre sommaire

Introduction

3. **Présenter**
   3.1. le contexte sur lequel vous travaillez (Description de l'association Web courses)
   3.2. Description de son logo (celui que vous avez choisi sur votre site) représentation, symbole, lien Internet si vous l'avez récupéré sur une bibliothèque d'images

Déroulé de la mission 7

3. **Donner** le schéma réseau global associé au contexte des missions 1 à 7
4. **Préciser** les contraintes liées aux Prérequis si nécessaires
4. **Notifier** les points de vigilance de chaque mission
5. **Expliquer** les points de blocage et les solutions apportées

6. **Montrer** à l'aide d'une copie écran les résultats obtenus après les mises en place des missions

Analyse de l'activité

7. **Spécifier** les difficultés rencontrées au cours des différentes phases de mise en place
8. **Mentionner** les apports professionnels acquis à travers cette expérience
9. **Préciser** les apports personnels acquis à travers cette expérience

Mission 10 Cybersécurité Gestion des certificats avec AD CS

Compétences	
Objectif principal	**Gérer** les certificats avec AD CS
Objectifs intermédiaires	**Installer** une CA autonome **Installer** une CA d'entreprise **Activer** une CA émettrice **Publier** un certificat via des GPO **Configurer** l'interface Web **Demander** un certificat
Vocabulaire à connaître	
Evaluation	Epreuve E4

Votre mission

Mettre en place des certificats AD CS

Informations utiles

Du contrôleur de domaine : 172.16.0.100/24
Un nouveau serveur autorité de certification racine : 172.16.0.150/24
Nom de la machine : srvcaracine
L'autorité de certification émettrice : le serveur IIS web : 172.16.0.151/24
Nom de la machine : srvcaiis
Passerelle : 172.16.0.254/24
Un poste client

Guide d'installation

1. Installer une CA autonome

Ce TP permet d'installer le rôle de serveur AD CS en tant [illegible] de certification autonome sur le serveur C[illegible]n situé sur le domaine Nextin[illegible] dans un groupe de travail nommé Workgroup. Cette CA doit être la racine de la hiérarchie afin de construire un modèle à deux couches de notre infrastructure à clés publiques.

racine

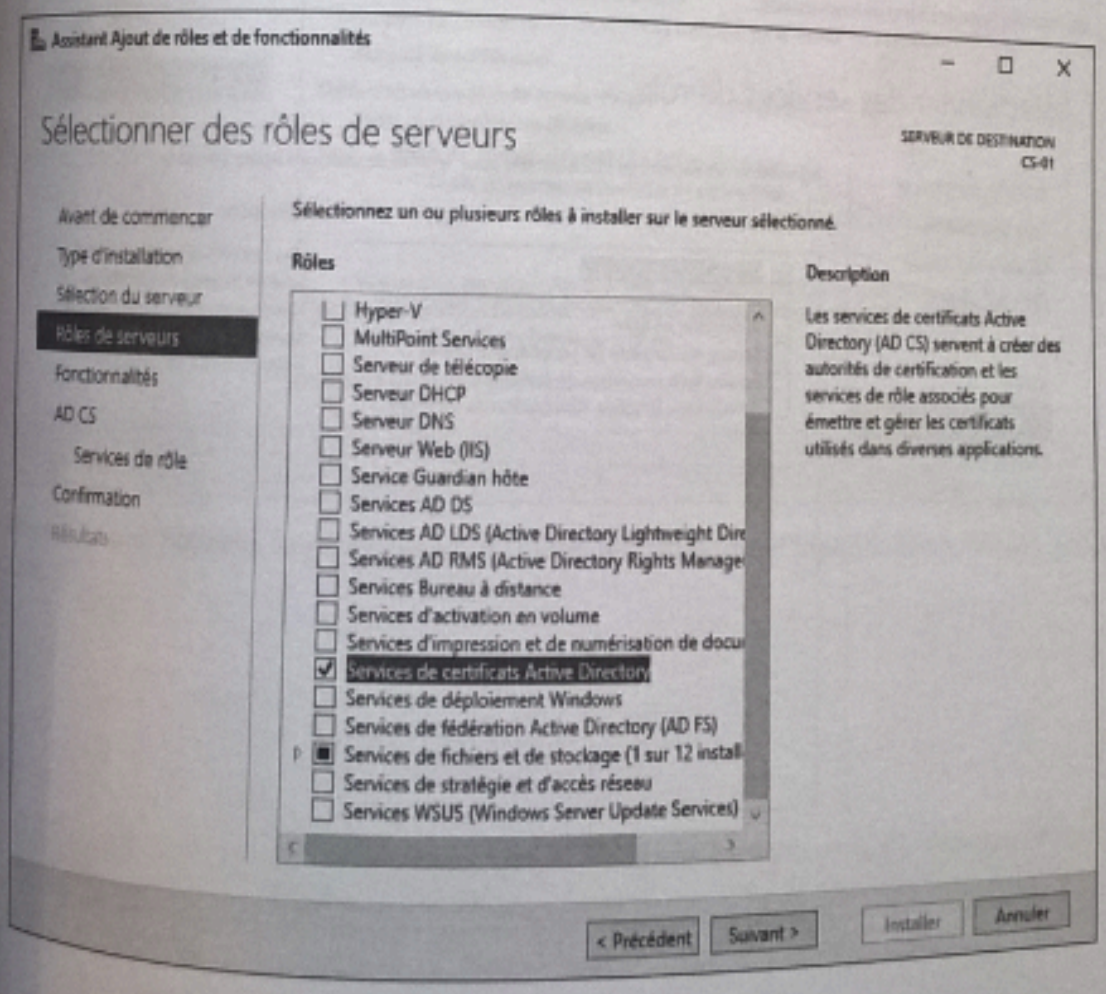
Webcourses.sio

racine

➢ **Étape 1** : ouvrez une session sur le serveur CS-[illegible] avec les identifiants d'administration, puis dans le **Gestionnaire de serveur**, cliquez sur **Ajouter des rôles et des fonctionnalités**.

➢ **Étape 2** : cliquez sur **Suivant** pour passer les pages **Avant de commencer**, **Sélectionner le type d'installation** et **Sélectionner le serveur de destination**.

➢ **Étape 3** : à l'écran **Sélectionner des rôles de serveurs**, cochez la case correspondant au rôle **Services de certificats Active Directory**, puis cliquez sur le bouton **Ajouter des fonctionnalités**. Cliquez ensuite sur **Suivant** :



➢ **Étape 4** : dans la fenêtre **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.

➢ **Étape 5** : dans la fenêtre **Services de certificats Active Directory**, cliquez sur **Suivant**.

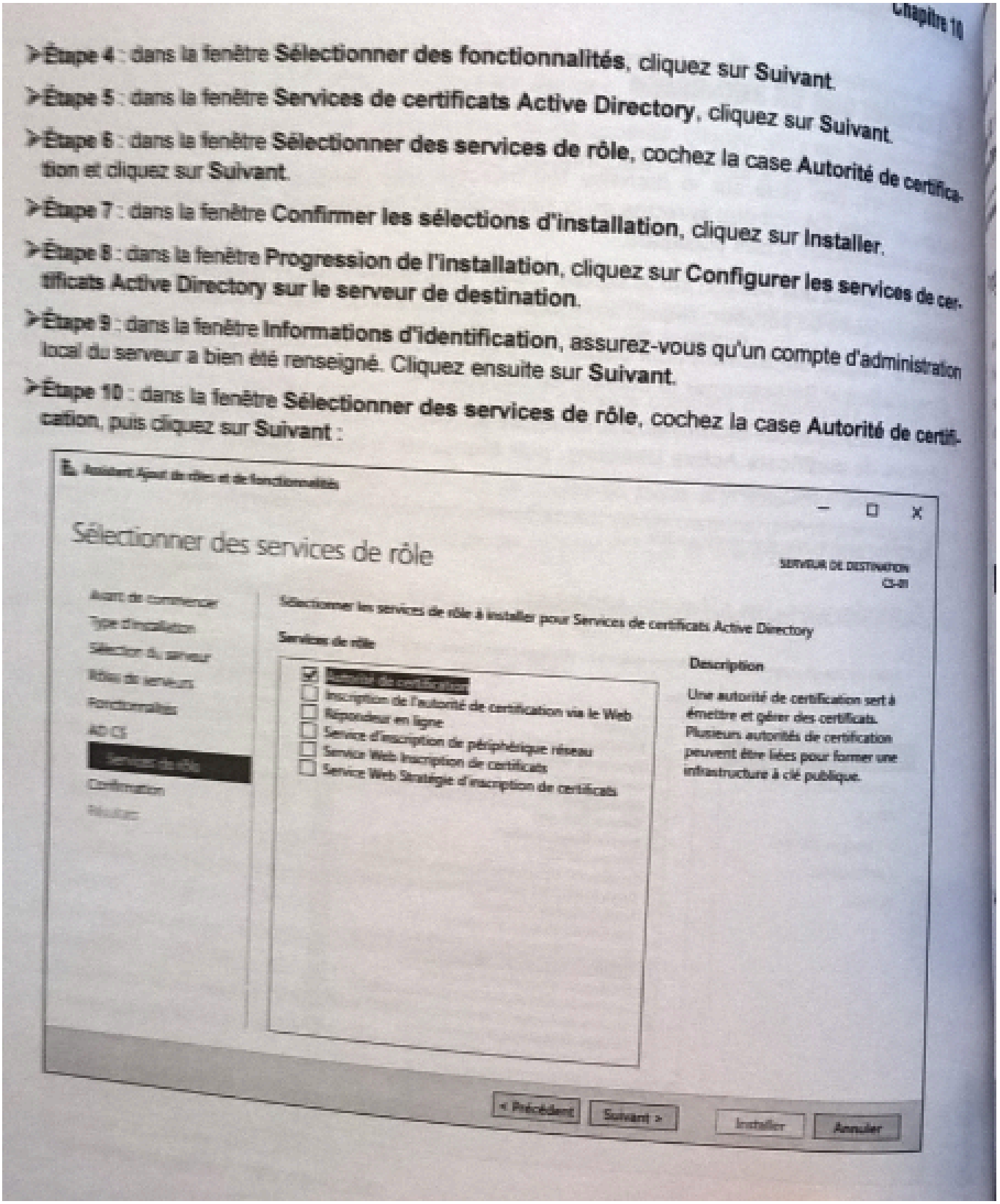
➢ **Étape 6** : dans la fenêtre **Sélectionner des services de rôle**, cochez la case **Autorité de certification** et cliquez sur **Suivant**.

➢ **Étape 7** : dans la fenêtre **Confirmer les sélections d'installation**, cliquez sur **Installer**.

➢ **Étape 8** : dans la fenêtre **Progression de l'installation**, cliquez sur **Configurer les services de certificats Active Directory sur le serveur de destination**.

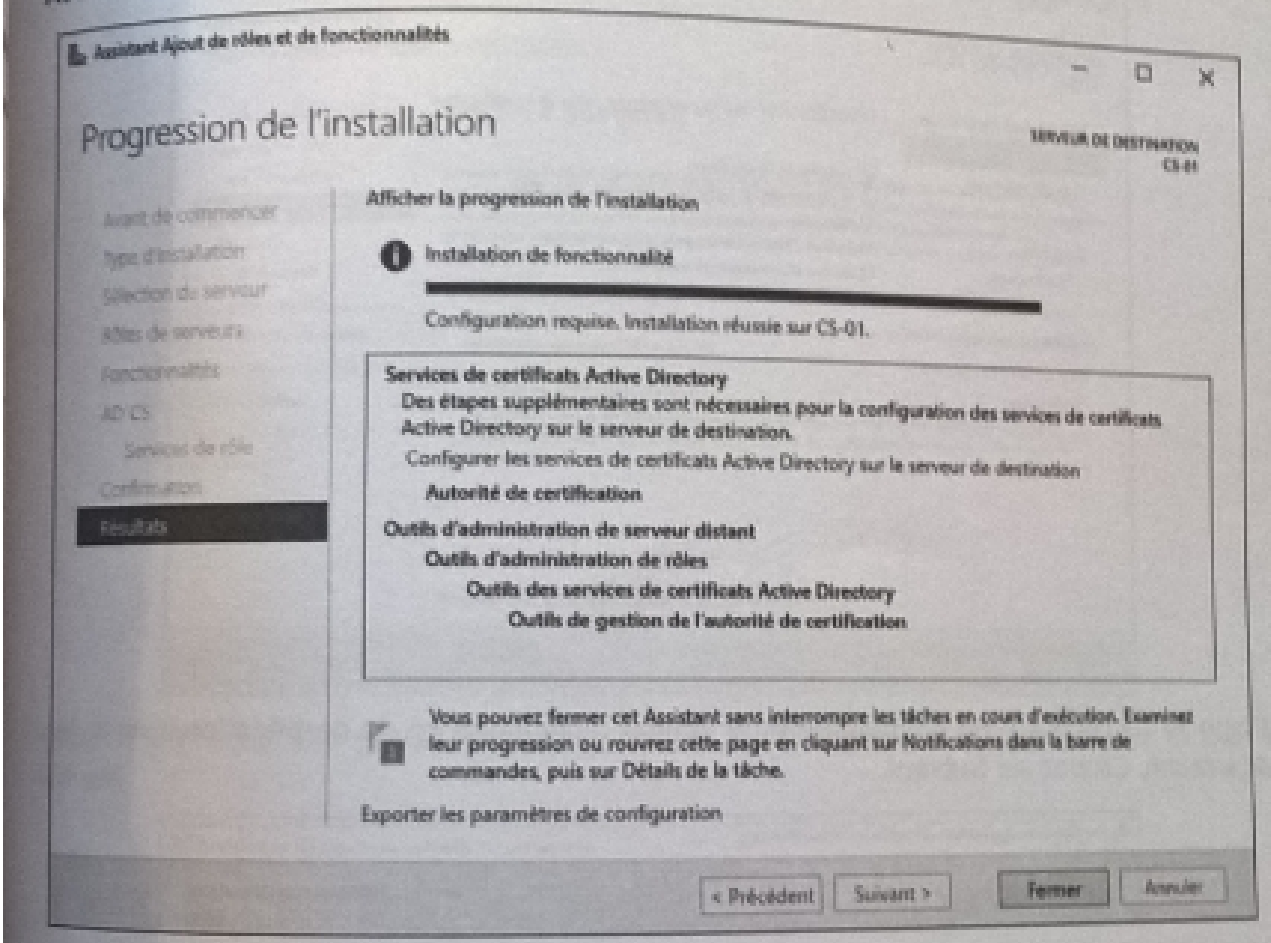
➢ **Étape 9** : dans la fenêtre **Informations d'identification**, assurez-vous qu'un compte d'administration local du serveur a bien été renseigné. Cliquez ensuite sur **Suivant**.

➢ **Étape 10** : dans la fenêtre **Sélectionner des services de rôle**, cochez la case **Autorité de certification**, puis cliquez sur **Suivant** :



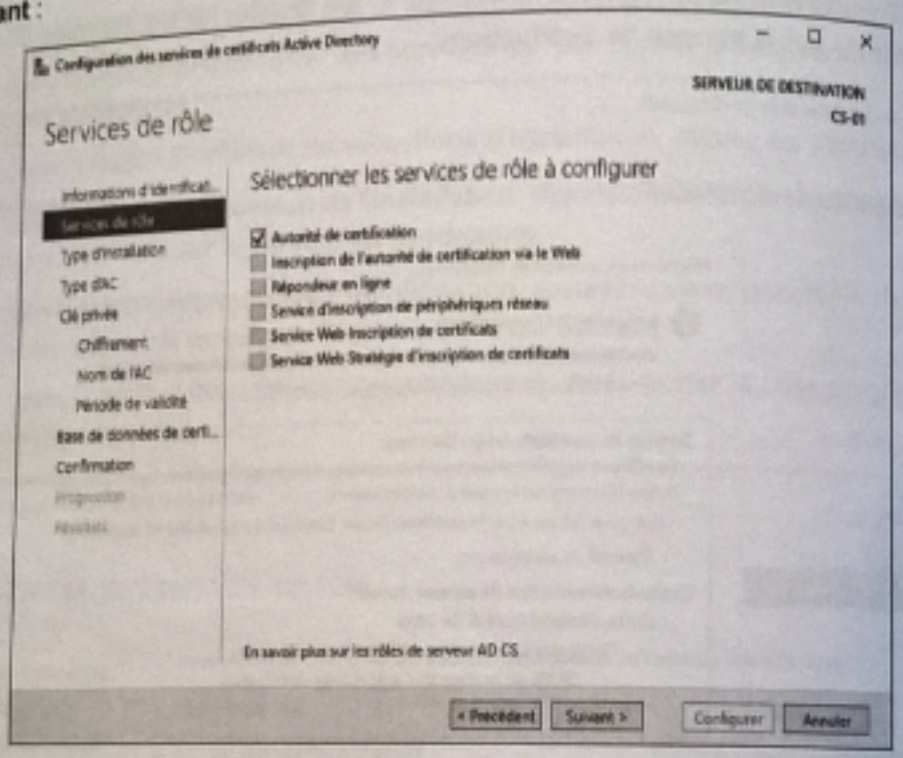
➢Étape 11 : à l'écran de **Confirmation**, cliquez sur **Installer**.

➢Étape 12 : une fois l'installation achevée, cliquez sur le lien **Configurer les services de certificats Active Directory sur le serveur de destination** :

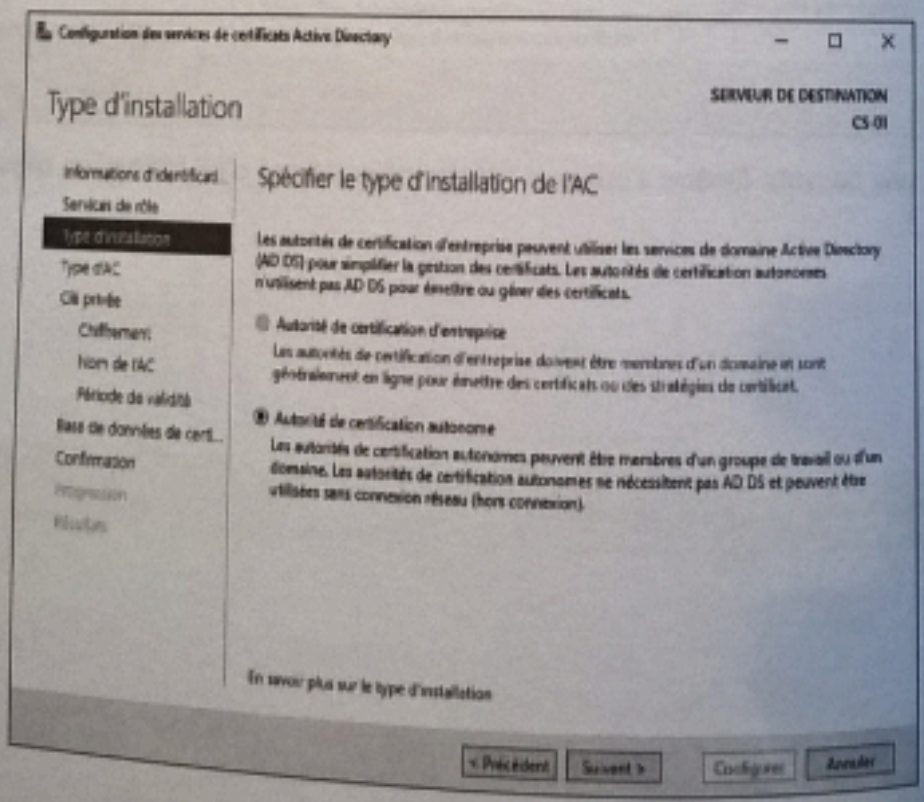


➢Étape 13 : une nouvelle fenêtre s'ouvre, à l'étape **Informations d'identification**, cliquez sur **Suivant**.

➢ **Étape 14** : dans la fenêtre **Services de rôle**, cochez la case **Autorité de certification**, puis cliquez sur **Suivant** :

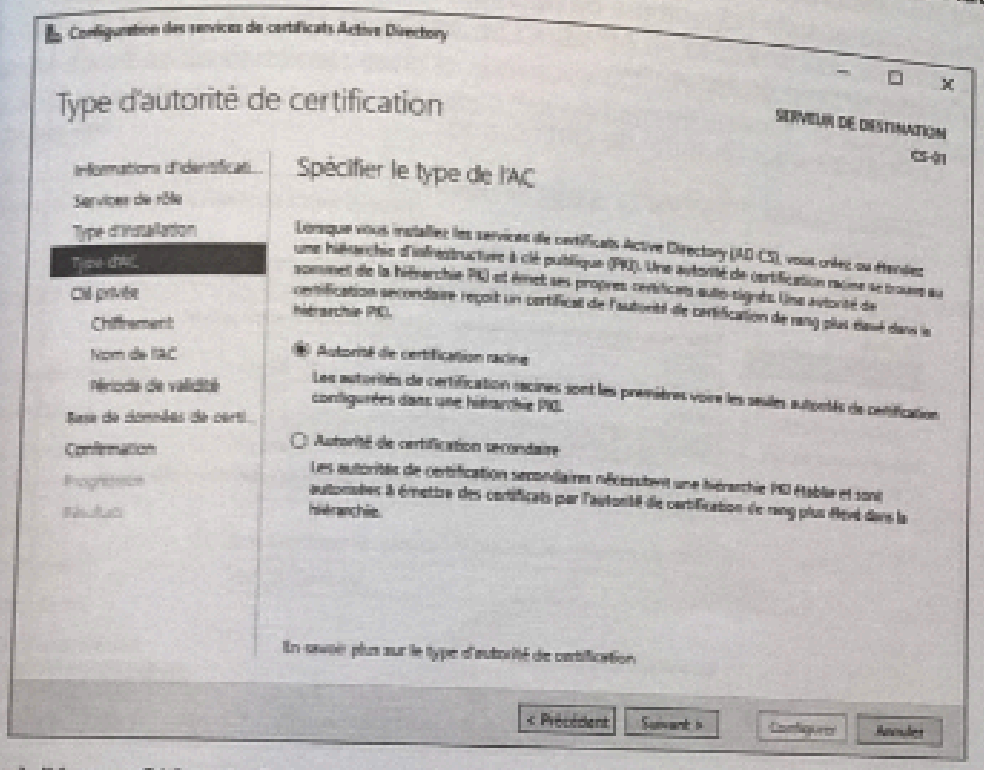


➢ **Étape 15** : à l'écran **Type d'installation**, le bouton radio **Autorité de certification autonome** est déjà coché. Cliquez sur **Suivant**.

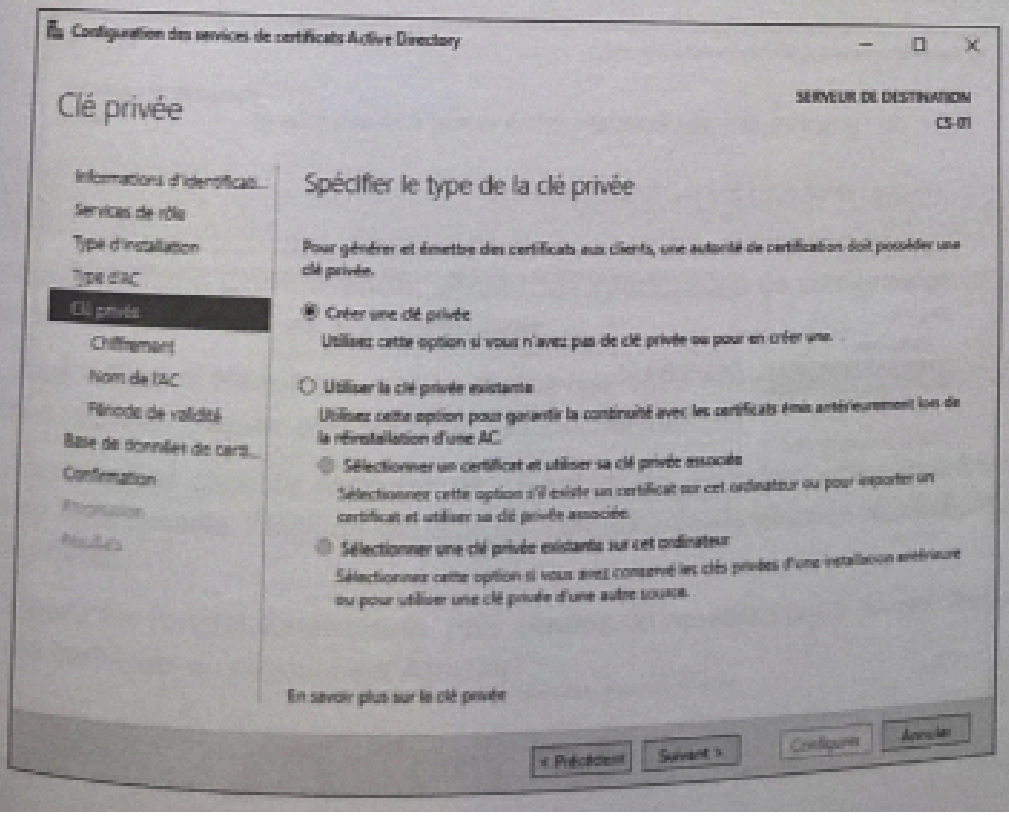


Windows Server 2016 - Gestion des

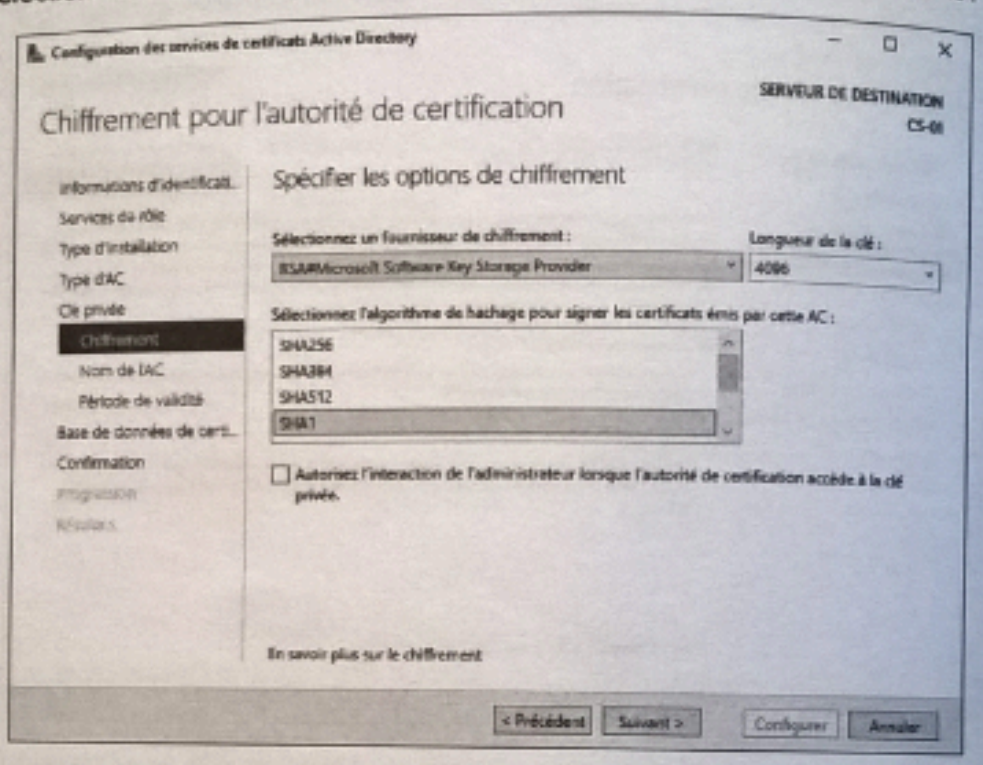
➢ **Étape 16** : dans la fenêtre **Type d'autorité de certification**, cochez le bouton radio **Autorité de certification racine**, puis cliquez sur **Suivant** :



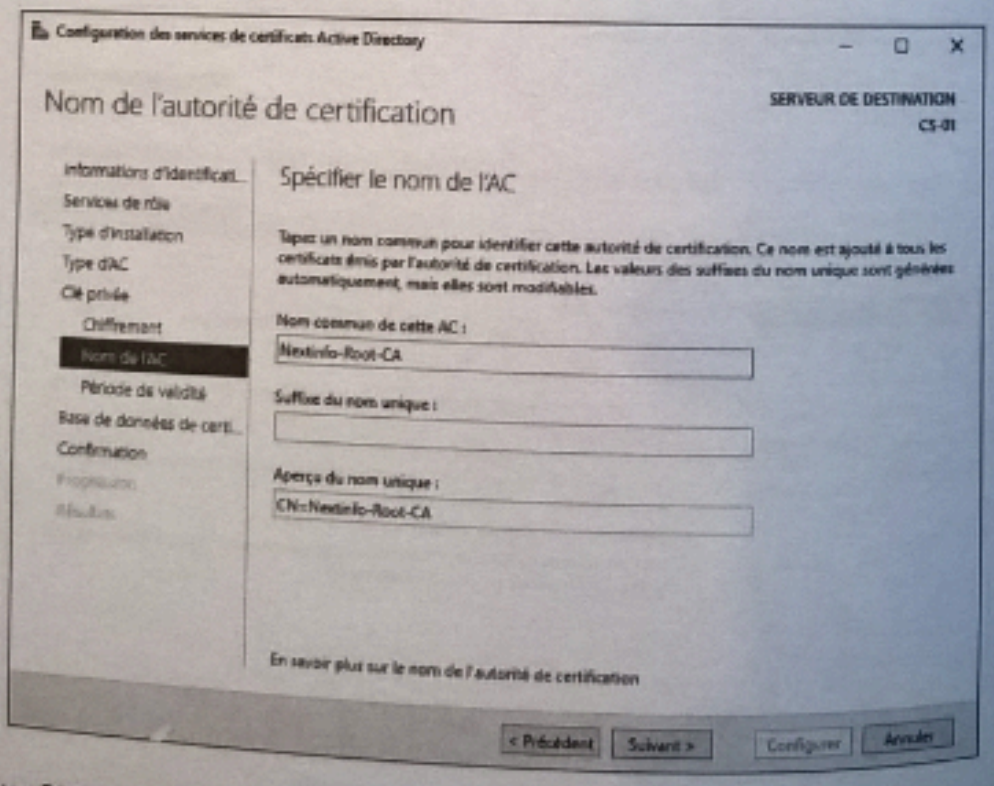
➢ **Étape 17** : à l'écran **Clé privée**, cochez le bouton radio **Créer une clé privée**, puis cliquez sur **Suivant** :



➢**Étape 18** : dans la fenêtre **Chiffrement pour l'autorité de certification**, sélectionnez le fournisseur de chiffrement **RSA#Microsoft Software Key Storage Provider**, puis indiquez une longueur de clé de *4096*. Sélectionnez ensuite l'algorithme de hachage **SHA1** et cliquez sur **Suivant** :



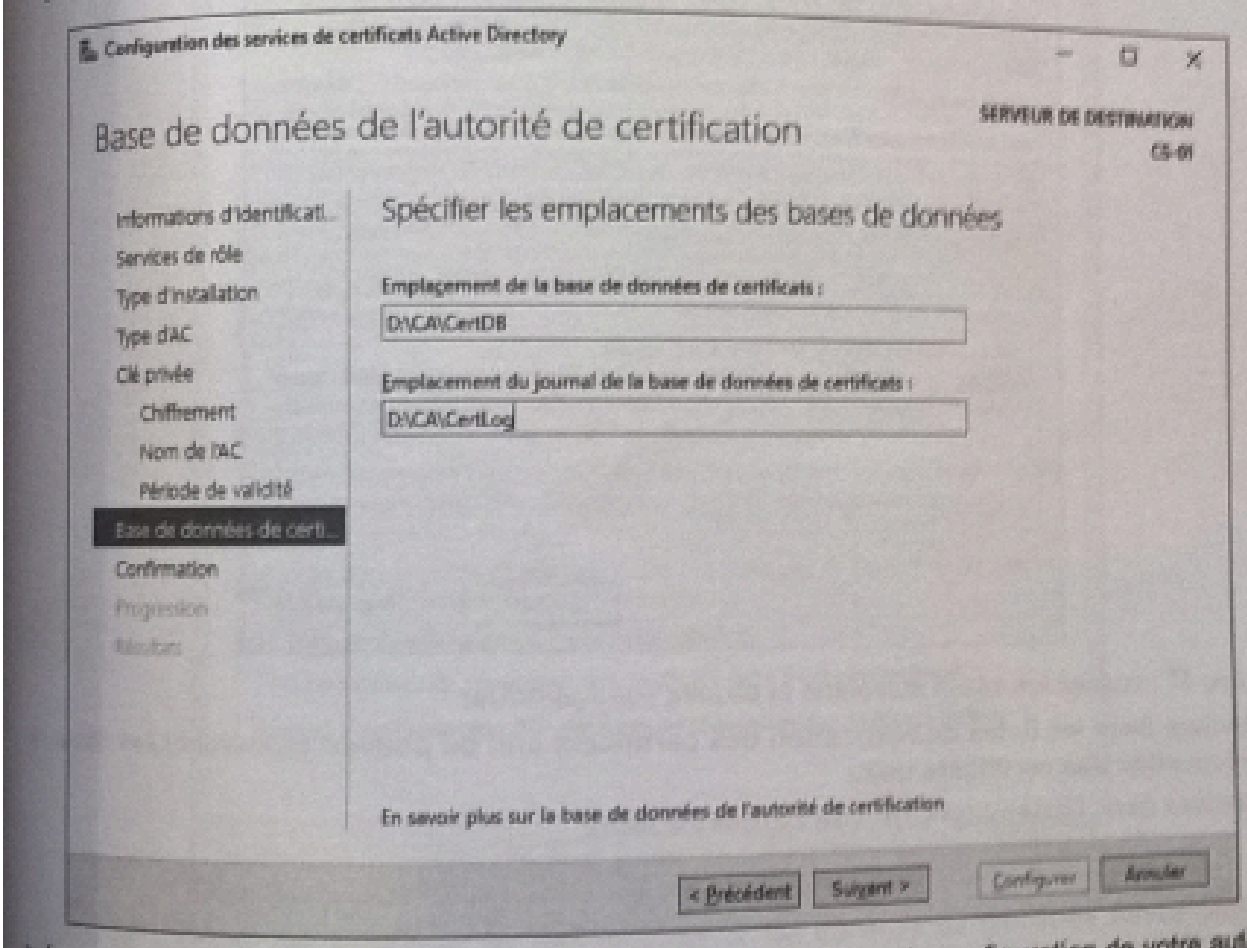
➢**Étape 19** : dans la fenêtre **Nom de l'autorité de certification**, tapez *Nextinfo-Root-CA* dans le champ **Nom commun de cette AC**, puis cliquez sur **Suivant** :



Windows Server 2016 - Gestion des identité...

➢ **Étape 20** : à l'écran **Période de validité**, indiquez *10 Années* pour spécifier la date d'expiration de l'autorité de certification, puis cliquez sur **Suivant**.

➢ **Étape 21** : dans la fenêtre **Base de données de l'autorité de certification**, spécifiez l'emplacement de la base de données de certificats dans le répertoire *D:\CA\CertDB*, puis spécifiez l'emplacement du journal de la base de données de certificats à l'emplacement suivant : *D:\CA\CertLog*. Cliquez ensuite sur **Suivant**.



➢ **Étape 22** : dans la fenêtre **Confirmation**, vérifiez les informations de configuration de votre autorité de certification racine, puis cliquez sur **Configurer**.

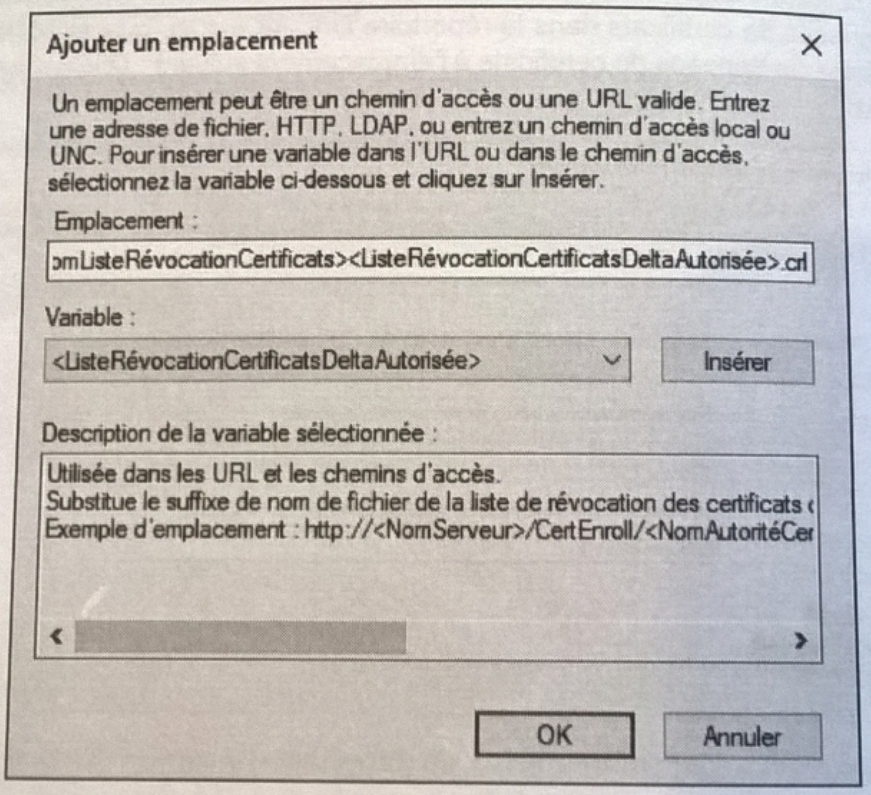
➢ **Étape 23** : dans le fenêtre **Résultats**, assurez-vous que votre autorité de certification affiche un état **Configuration réussie**. Cliquez ensuite deux fois sur **Fermer**.

➢ **Étape 24** : démarrez la console **Autorité de certification** dans les outils d'administration. Dans l'arborescence de la console, faites un clic droit sur l'autorité de certification **Nextinfo-Root-CA** et cliquez sur **Propriétés**.

➢ **Étape 25** : cliquez sur l'onglet **Extensions**, puis ajoutez un nouveau point de distribution de liste de révocation des certificats en cliquant sur **Ajouter**.

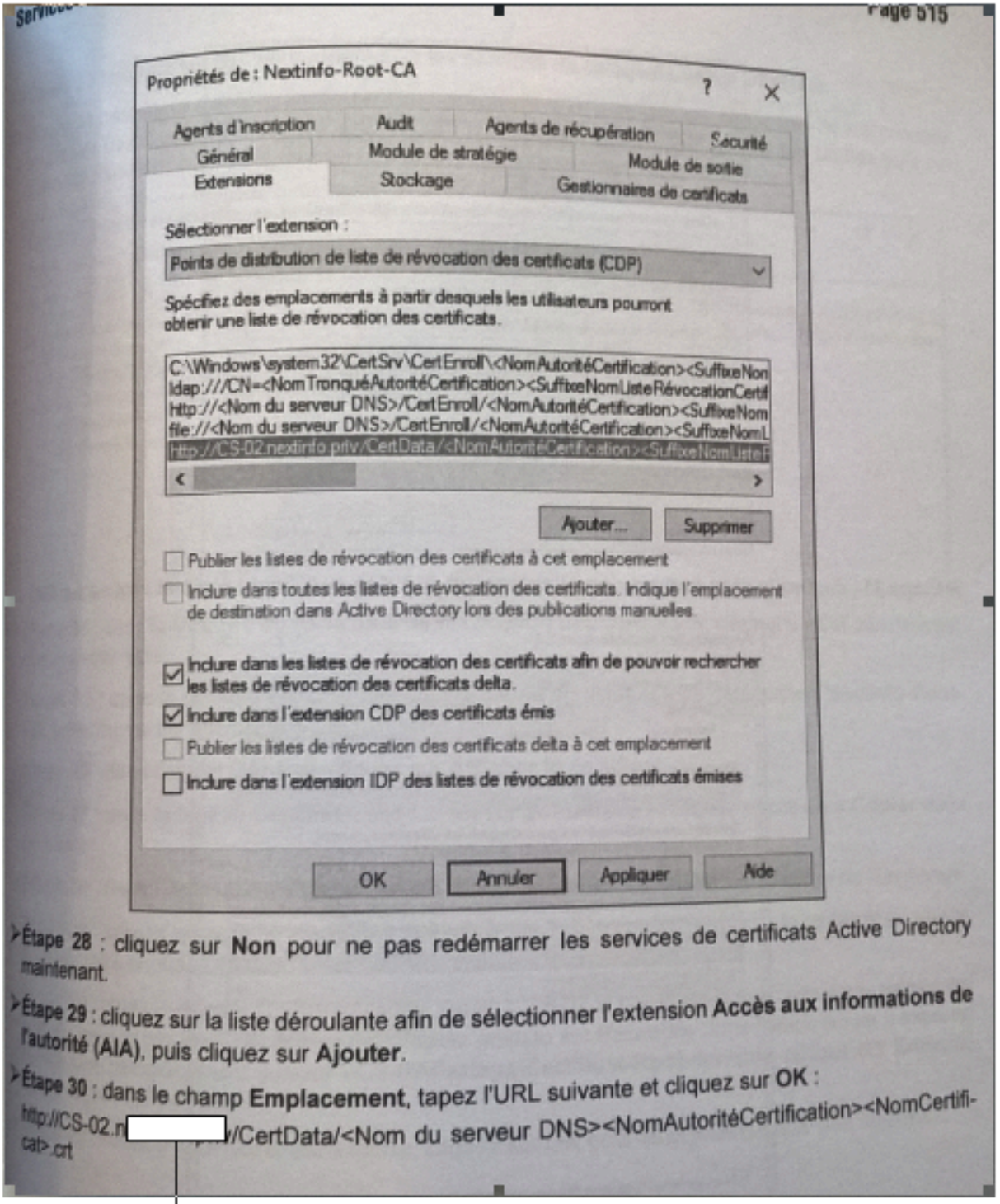
➢ **Étape 26** : dans le champ **Emplacement**, tapez l'URL suivante et cliquez sur **OK** :

http://CS-02.nextinfo.priv/CertData/<NomAutoritéCertification><SuffixeNomListeRévocationCertificats><ListeRévocationCertificatsDeltaAutorisée>.crl



➢ **Étape 27** : cochez les cases suivantes et cliquez sur **Appliquer** :

- **Inclure dans les listes de révocation des certificats afin de pouvoir rechercher les listes de révocation des certificats delta**
- **Inclure dans l'extension CDP des certificats émis**



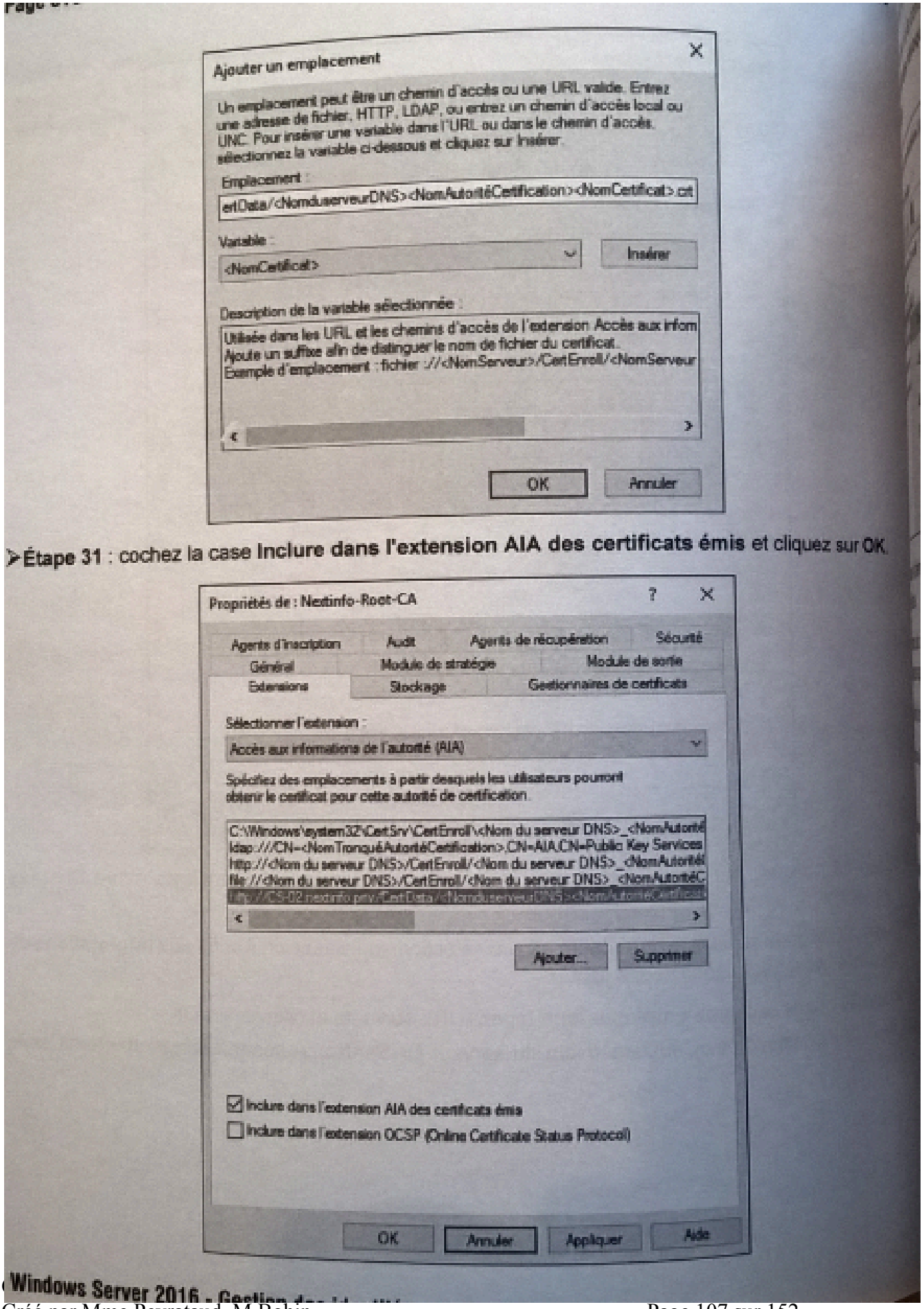
➢ Étape 28 : cliquez sur **Non** pour ne pas redémarrer les services de certificats Active Directory maintenant.

➢ Étape 29 : cliquez sur la liste déroulante afin de sélectionner l'extension **Accès aux informations de l'autorité (AIA)**, puis cliquez sur **Ajouter**.

➢ Étape 30 : dans le champ **Emplacement**, tapez l'URL suivante et cliquez sur **OK** :

http://CS-02.n[redacted]/CertData/<Nom du serveur DNS><NomAutoritéCertification><NomCertificat>.crt

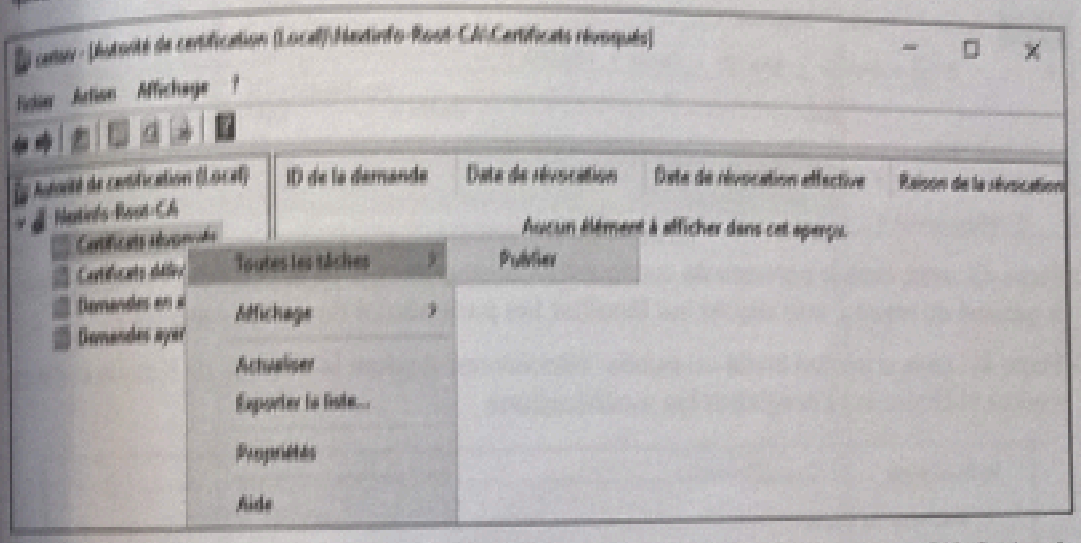
Webcourses.sio



➢ **Étape 31** : cochez la case **Inclure dans l'extension AIA des certificats émis** et cliquez sur **OK**

➢Étape 32 : cliquez sur **Oui** pour redémarrer les services de certificats Active Directory.

➢Étape 33 : de retour à la console de gestion **certsrv**, développez l'arborescence afin de sélectionner le dossier **Certificats révoqués**. Faites un clic droit dessus, cliquez sur **Toutes les tâches** puis cliquez sur **Publier** :



➢Étape 34 : dans la fenêtre **Publier la liste de révocation des certificats**, cliquez sur **OK** afin de créer une nouvelle liste.

➢Étape 35 : dans la console **certsrv**, faites un clic droit sur l'autorité de certification **Nextinfo-Root-CA**, puis cliquez sur **Propriétés**.

➢Étape 36 : dans l'onglet **Général**, cliquez sur **Afficher le certificat**.

➢Étape 37 : dans la fenêtre **Certificat**, cliquez sur l'onglet **Détails** et cliquez ensuite sur **Copier dans un fichier**.

➢Étape 38 : dans l'**Assistant Exportation du certificat**, cliquez sur **Suivant** à l'écran de bienvenue.

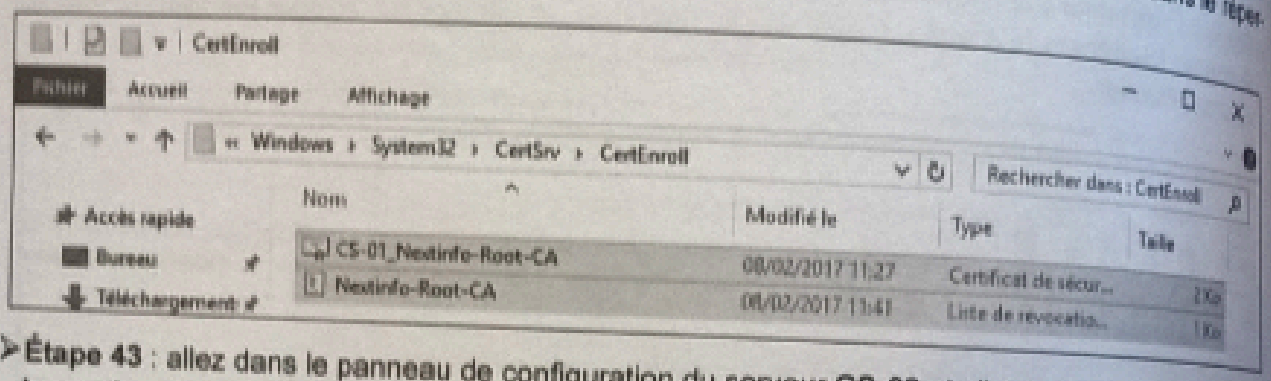
➢Étape 39 : laissez les options par défaut et cliquez sur **Suivant** afin d'exporter le certificat au format X.509 binaire encodé DER.

➢Étape 40 : créez le dossier *C:\Partage* sur le serveur **CS-02** et partagez-le avec des droits de lecture/écriture pour le groupe **Tout le monde**. Cliquez ensuite sur **Parcourir** dans l'étape fichier à exporter et indiquez l'emplacement suivant **\\CS-02\Partage\Certificat-Root.cer**, puis cliquez sur **Enregistrer**, **Suivant** et **Terminer**.

➢Étape 41 : lorsque le certificat est exporté, cliquez sur **OK** pour fermer l'ensemble des fenêtres.

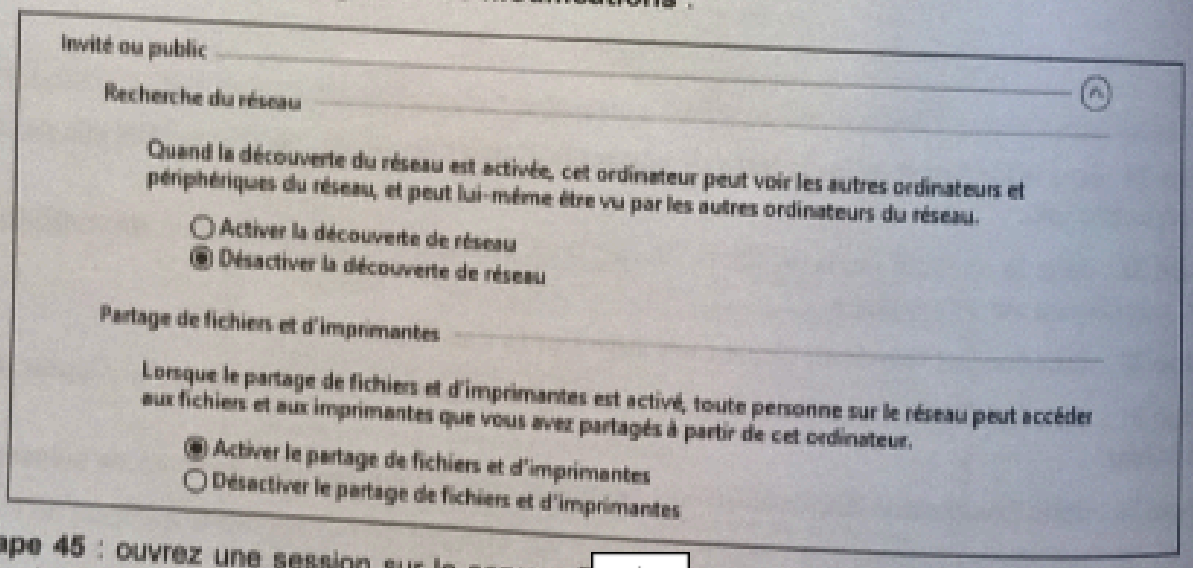
REMPLACER CS-01 par srvcaiis

➢ **Étape 42** : partagez le répertoire C:\windows\system32\CertSrv\CertEnrol puis naviguez dans le répertoire *C:\Partage* sur le serveur CS-02, afin d'y copier les deux fichiers présents dans le répertoire ci-dessous :



➢ **Étape 43** : allez dans le panneau de configuration du serveur **CS-02** et cliquez sur **Afficher l'état et la gestion du réseau**, puis cliquez sur **Modifier les paramètres de partage avancés**.

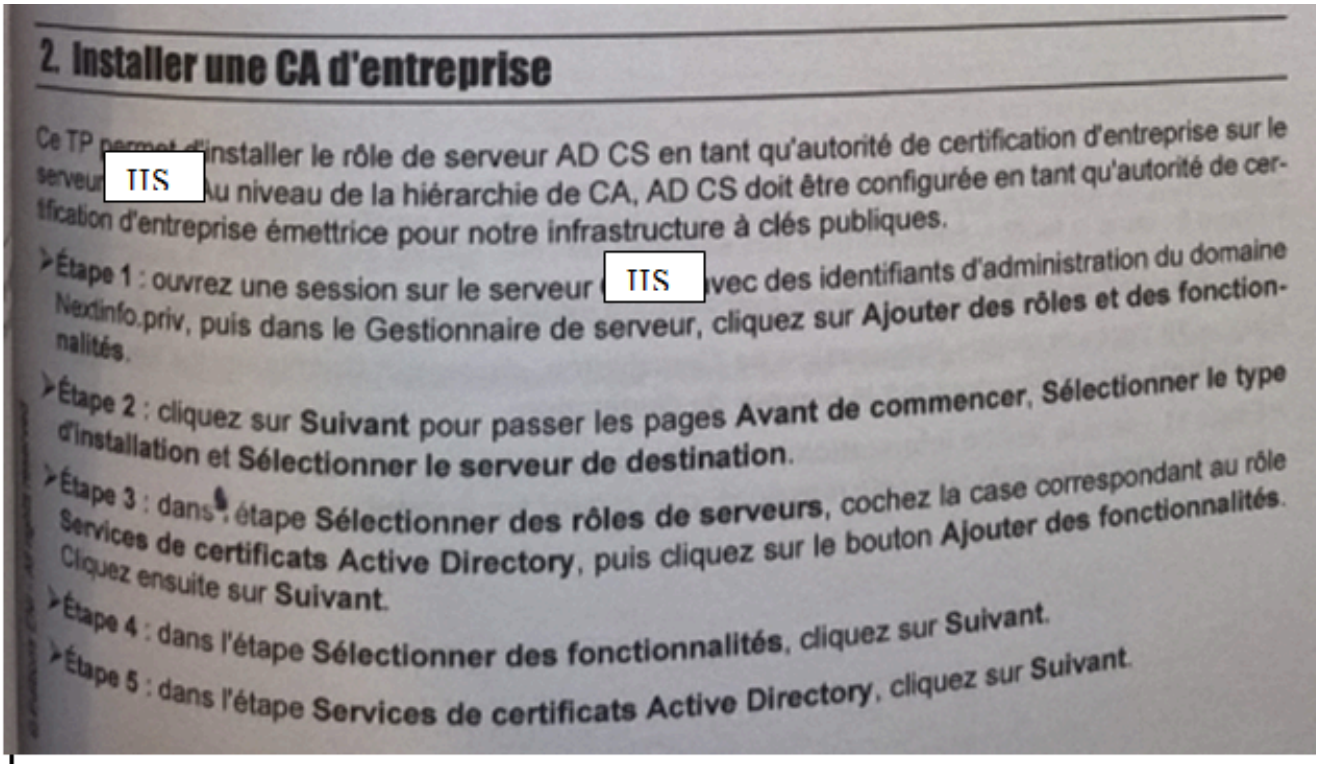
➢ **Étape 44** : dans la section **Invité ou public**, sélectionnez **Activer le partage de fichiers et d'imprimantes** et cliquez sur **Enregistrer les modifications** :



➢ **Étape 45** : ouvrez une session sur le serveur D racine vec des privilèges d'administration dans le domaine Nextinfo.priv. Démarrez la console de gestion DNS et créez l'hôte A suivant dans la zone de recherche directe Nextinfo.priv :

Nom : C srvcaracine

Adresse IP : 172.16.0.150

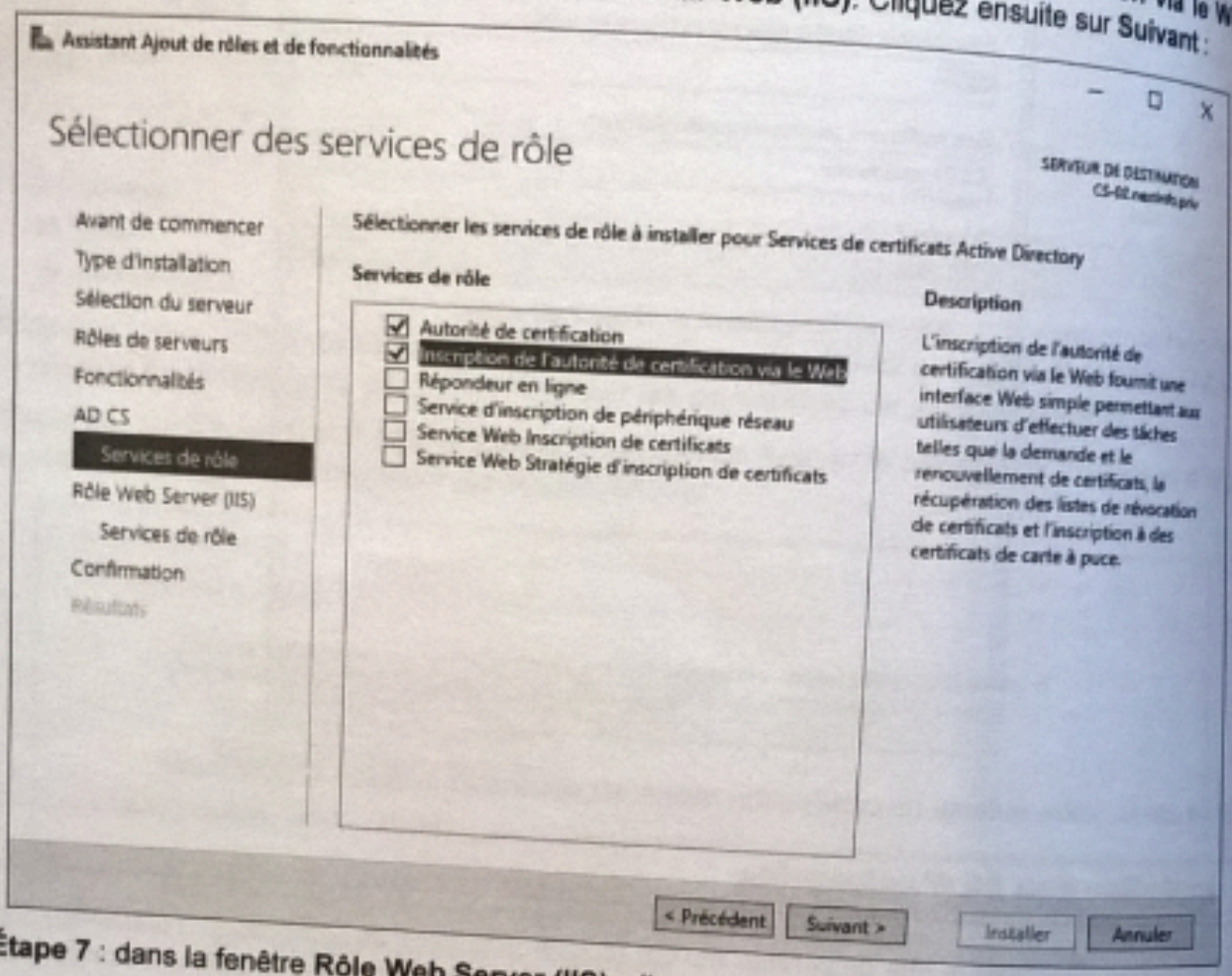


2. Installer une CA d'entreprise

Ce TP permet d'installer le rôle de serveur AD CS en tant qu'autorité de certification d'entreprise sur le serveur [illegible] au niveau de la hiérarchie de CA, AD CS doit être configurée en tant qu'autorité de certification d'entreprise émettrice pour notre infrastructure à clés publiques.

- **Étape 1** : ouvrez une session sur le serveur [illegible] avec des identifiants d'administration du domaine Nextinfo.priv, puis dans le Gestionnaire de serveur, cliquez sur **Ajouter des rôles et des fonctionnalités**.
- **Étape 2** : cliquez sur **Suivant** pour passer les pages **Avant de commencer**, **Sélectionner le type d'installation** et **Sélectionner le serveur de destination**.
- **Étape 3** : dans l'étape **Sélectionner des rôles de serveurs**, cochez la case correspondant au rôle **Services de certificats Active Directory**, puis cliquez sur le bouton **Ajouter des fonctionnalités**. Cliquez ensuite sur **Suivant**.
- **Étape 4** : dans l'étape **Sélectionner des fonctionnalités**, cliquez sur **Suivant**.
- **Étape 5** : dans l'étape **Services de certificats Active Directory**, cliquez sur **Suivant**.

➢ **Étape 6** : dans la fenêtre **Sélectionner des services de rôle**, cochez la case **Autorité de certification**, puis **Inscription de l'autorité de certification via le Web** et cliquez sur **Ajouter des fonctionnalités**. Le fait d'ajouter le service de rôle **Inscription de l'autorité de certification via le Web**, l'assistant propose alors l'installation du rôle **serveur Web (IIS)**. Cliquez ensuite sur **Suivant** :



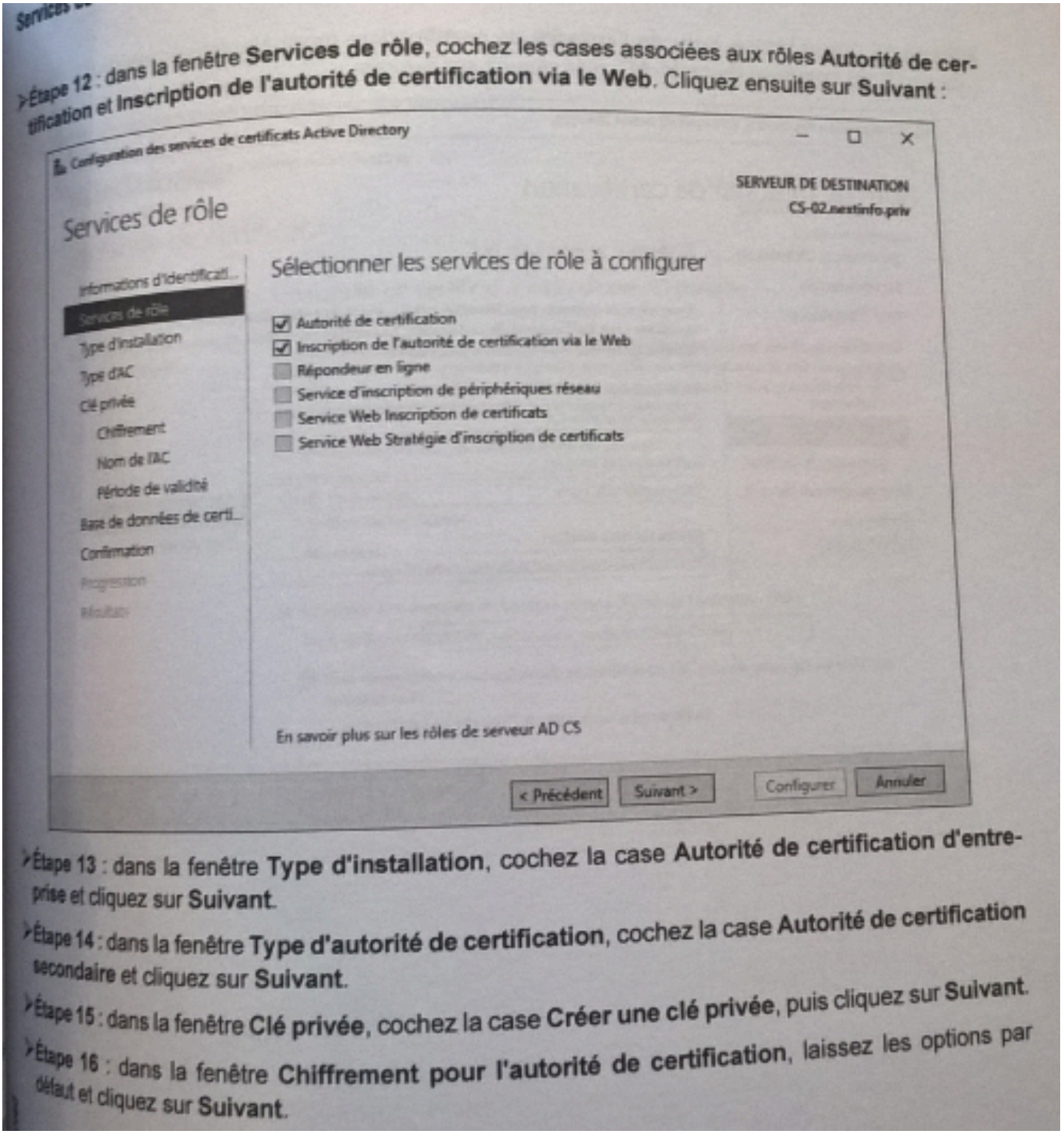
➢ **Étape 7** : dans la fenêtre **Rôle Web Server (IIS)**, cliquez sur **Suivant**.

➢ **Étape 8** : dans la fenêtre **Sélectionner des services de rôle**, cliquez sur **Suivant**.

➢ **Étape 9** : dans la fenêtre **Confirmer les sélections d'installation**, cliquez sur **Installer**.

➢ **Étape 10** : dans la fenêtre **Progression de l'installation**, cliquez sur **Configurer les services de certificats Active Directory sur le serveur de destination**.

➢ **Étape 11** : dans la fenêtre **Informations d'identification**, assurez-vous qu'un compte d'administration du domaine Nextinfo.priv a été renseigné, puis cliquez sur **Suivant**.



➢Étape 12 : dans la fenêtre **Services de rôle**, cochez les cases associées aux rôles **Autorité de certification** et **Inscription de l'autorité de certification via le Web**. Cliquez ensuite sur **Suivant** :

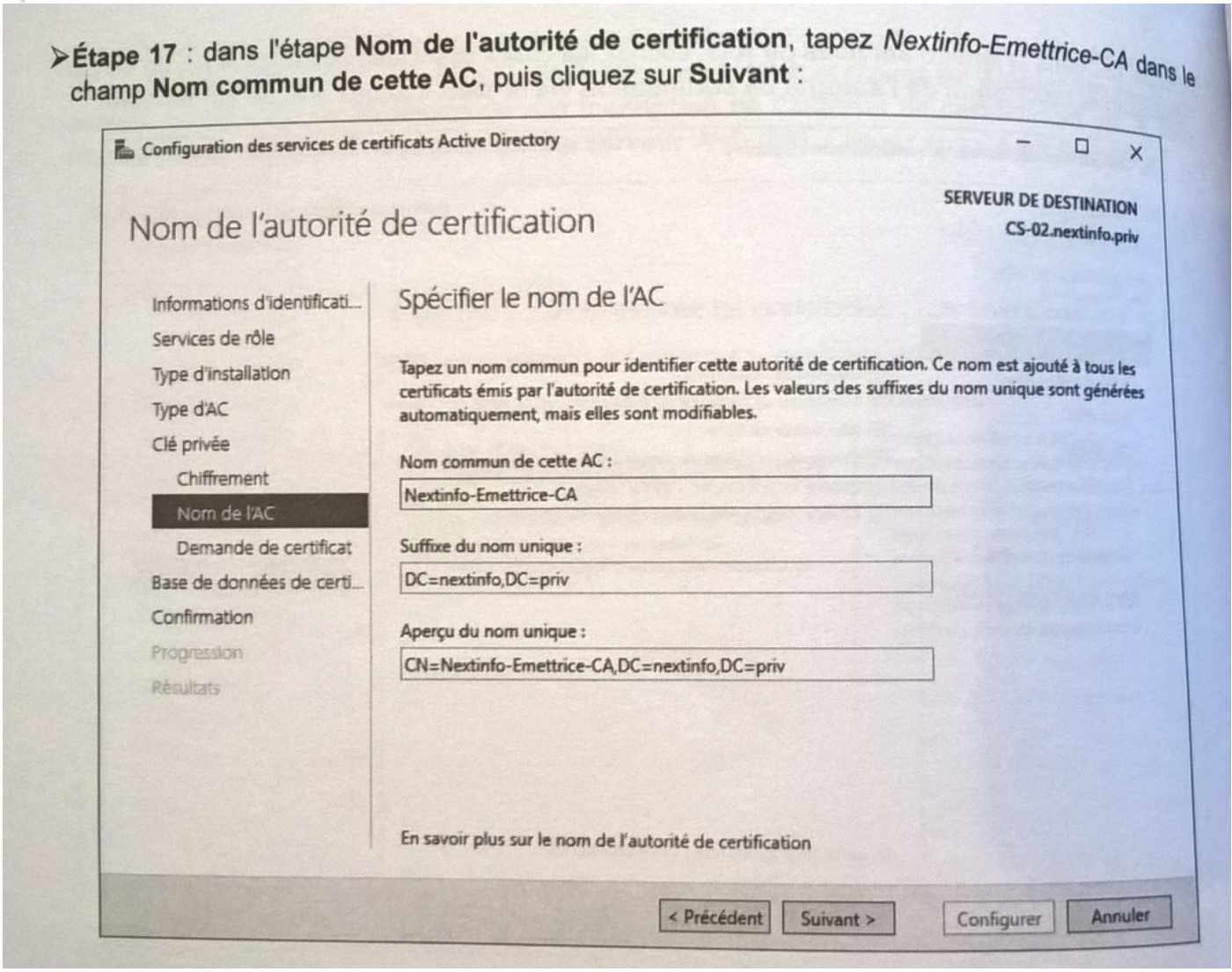
➢Étape 13 : dans la fenêtre **Type d'installation**, cochez la case **Autorité de certification d'entreprise** et cliquez sur **Suivant**.

➢Étape 14 : dans la fenêtre **Type d'autorité de certification**, cochez la case **Autorité de certification secondaire** et cliquez sur **Suivant**.

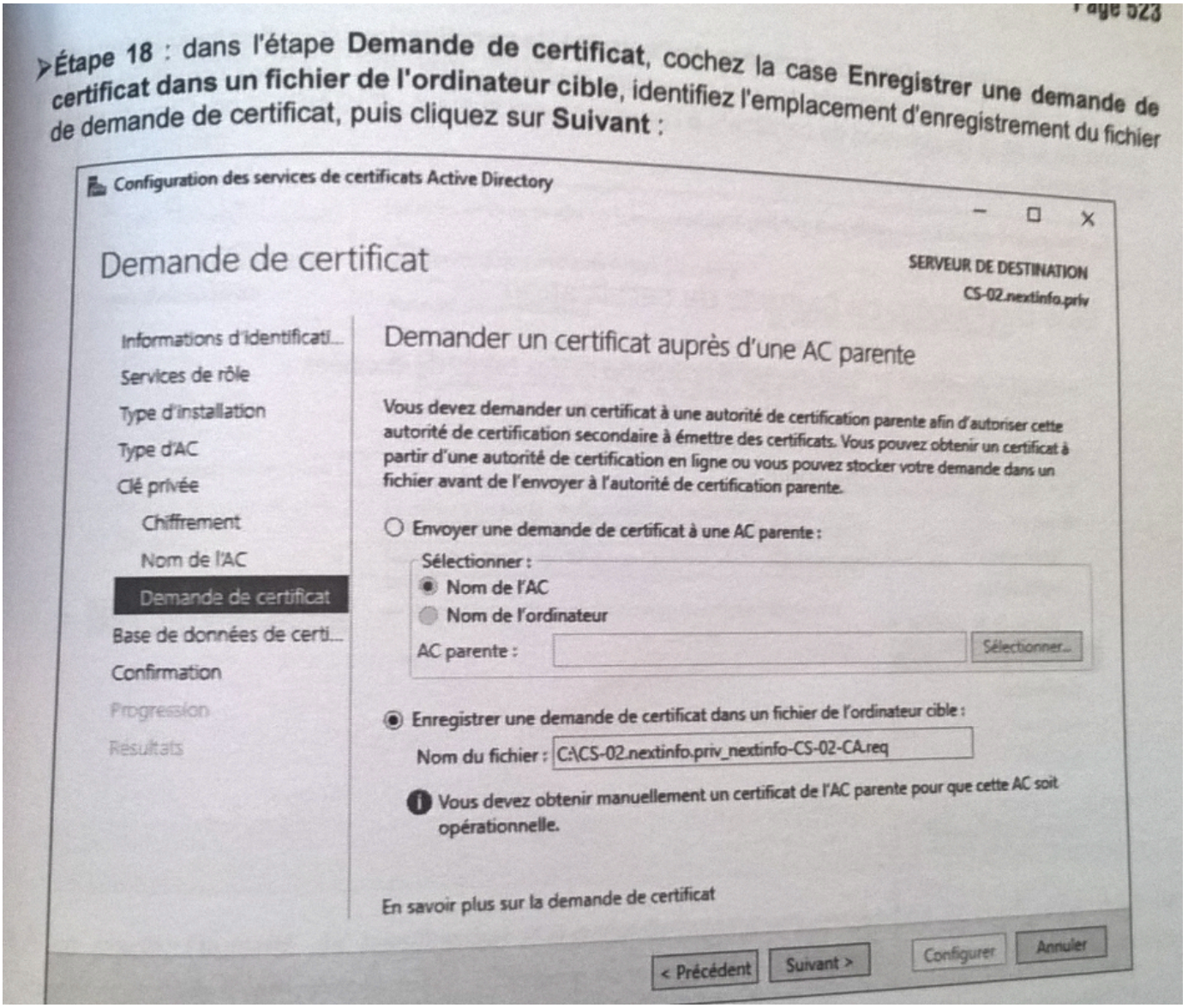
➢Étape 15 : dans la fenêtre **Clé privée**, cochez la case **Créer une clé privée**, puis cliquez sur **Suivant**.

➢Étape 16 : dans la fenêtre **Chiffrement pour l'autorité de certification**, laissez les options par défaut et cliquez sur **Suivant**.

➢ **Étape 17** : dans l'étape **Nom de l'autorité de certification**, tapez *Nextinfo-Emettrice-CA* dans le champ **Nom commun de cette AC**, puis cliquez sur **Suivant** :



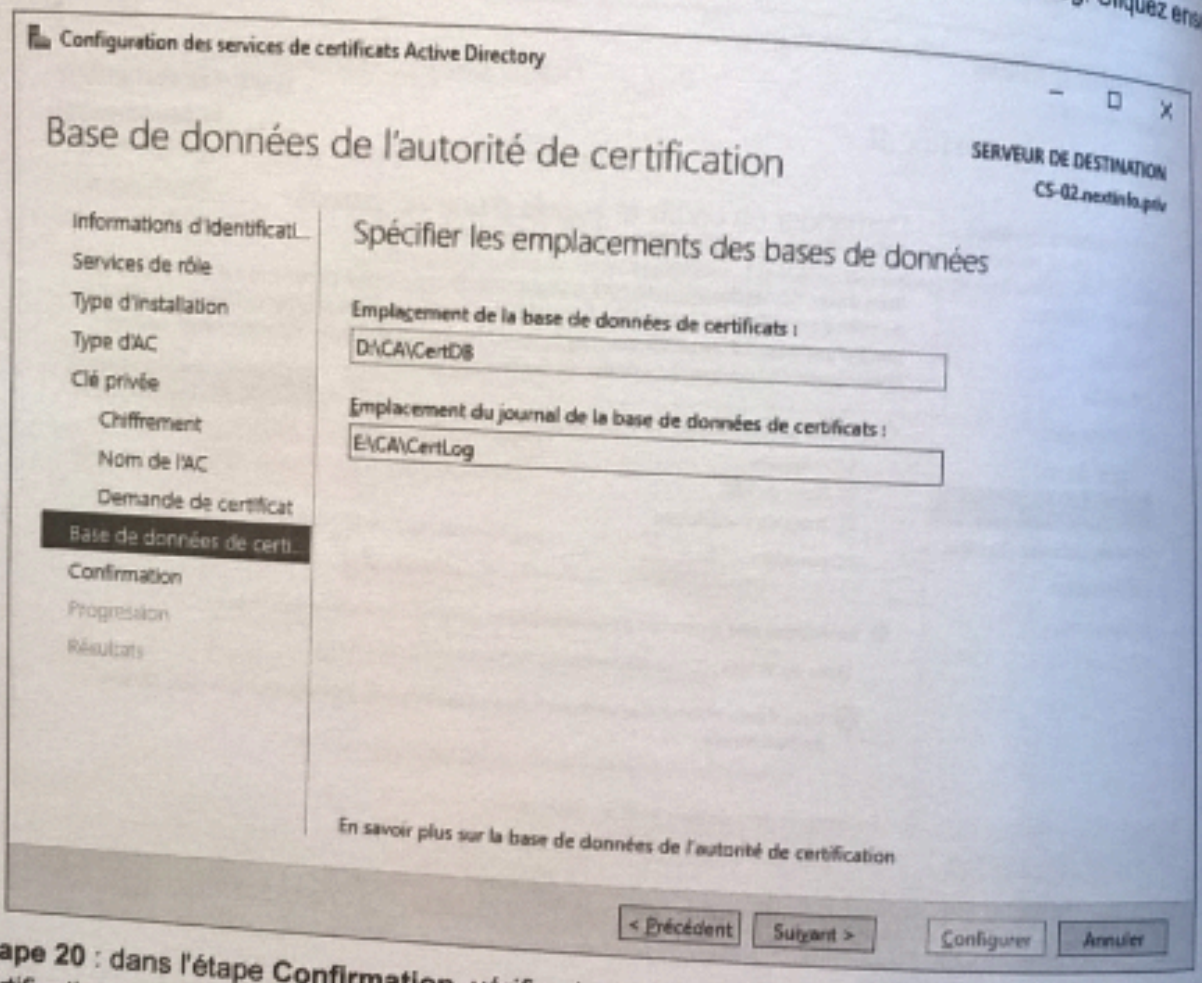
REMPLACER Nexinfo par webcourses



REMPLACER le nom du fichier par

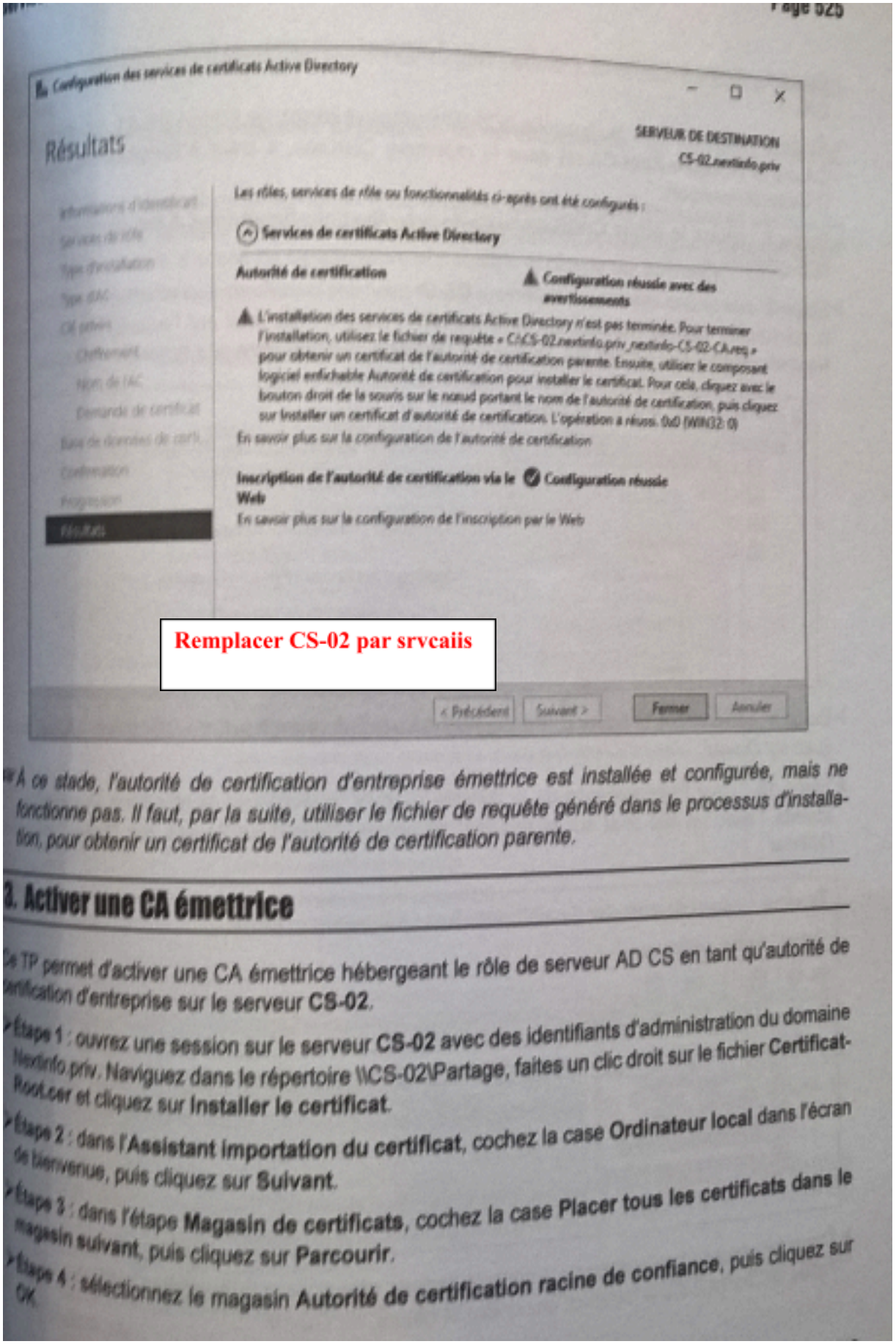
C:\ srvcaiis.webcourses.sio_webcourses-srvcaiis-CA.req

➢ **Étape 19** : dans l'étape **Base de données de l'autorité de certification**, spécifiez l'emplacement de la base de données de certificats dans le répertoire *D:\CA\CertDB*, puis spécifiez l'emplacement du journal de la base de données de certificats à l'emplacement suivant : *E:\CA\CertLog*. Cliquez ensuite sur **Suivant** :



➢ **Étape 20** : dans l'étape **Confirmation**, vérifiez les informations de configuration de votre autorité de certification secondaire, puis cliquez sur **Configurer**.

➢ **Étape 21** : dans l'étape **Résultats**, l'installation de l'autorité de certification d'entreprise affiche un message d'avertissement, indiquant qu'il ne faut pas oublier de demander un certificat de l'autorité de certification parente pour autoriser cette autorité de certification d'entreprise à émettre des certificats. Assurez-vous que l'installation du service de rôle **Inscription de l'autorité de certification via le web** indique un état de configuration réussie. Cliquez ensuite deux fois sur **Fermer**.



À ce stade, l'autorité de certification d'entreprise émettrice est installée et configurée, mais ne fonctionne pas. Il faut, par la suite, utiliser le fichier de requête généré dans le processus d'installation, pour obtenir un certificat de l'autorité de certification parente.

2. Activer une CA émettrice

Ce TP permet d'activer une CA émettrice hébergeant le rôle de serveur AD CS en tant qu'autorité de certification d'entreprise sur le serveur **CS-02**.

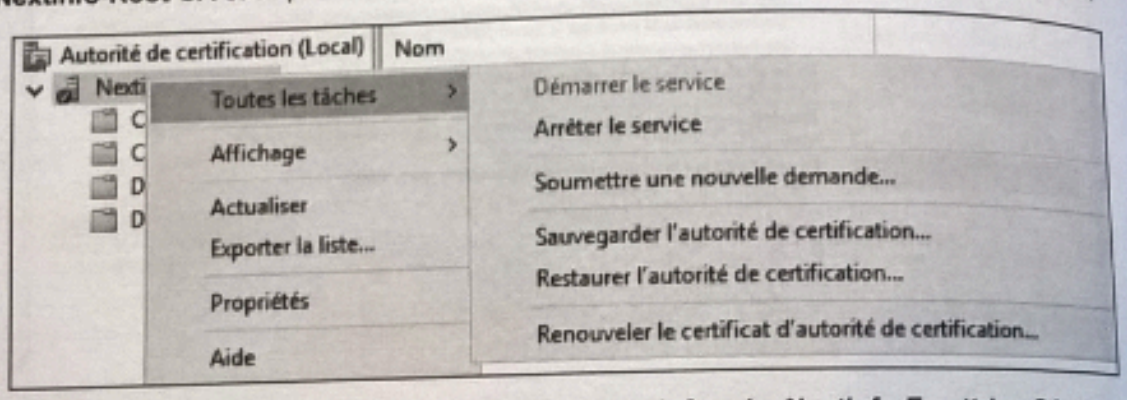
- **Étape 1** : ouvrez une session sur le serveur **CS-02** avec des identifiants d'administration du domaine Nextinfo.priv. Naviguez dans le répertoire \\CS-02\Partage, faites un clic droit sur le fichier **Certificat-Root.cer** et cliquez sur **Installer le certificat**.
- **Étape 2** : dans l'**Assistant importation du certificat**, cochez la case **Ordinateur local** dans l'écran de bienvenue, puis cliquez sur **Suivant**.
- **Étape 3** : dans l'étape **Magasin de certificats**, cochez la case **Placer tous les certificats dans le magasin suivant**, puis cliquez sur **Parcourir**.
- **Étape 4** : sélectionnez le magasin **Autorité de certification racine de confiance**, puis cliquez sur OK.

➢ **Étape 5** : cliquez sur **Suivant**, puis **Terminer**. Lorsque l'importation du certificat a réussi, cliquez sur **OK**.

➢ **Étape 6** : naviguez dans le répertoire *\\CS-02\Partage* et copiez les fichiers **CS-01_Nextinfo-Root-CA.crt** et **Nextinfo-Root-CA.crl** dans le répertoire CertData, à créer à l'emplacement suivant : C:\inetpub\wwwroot\

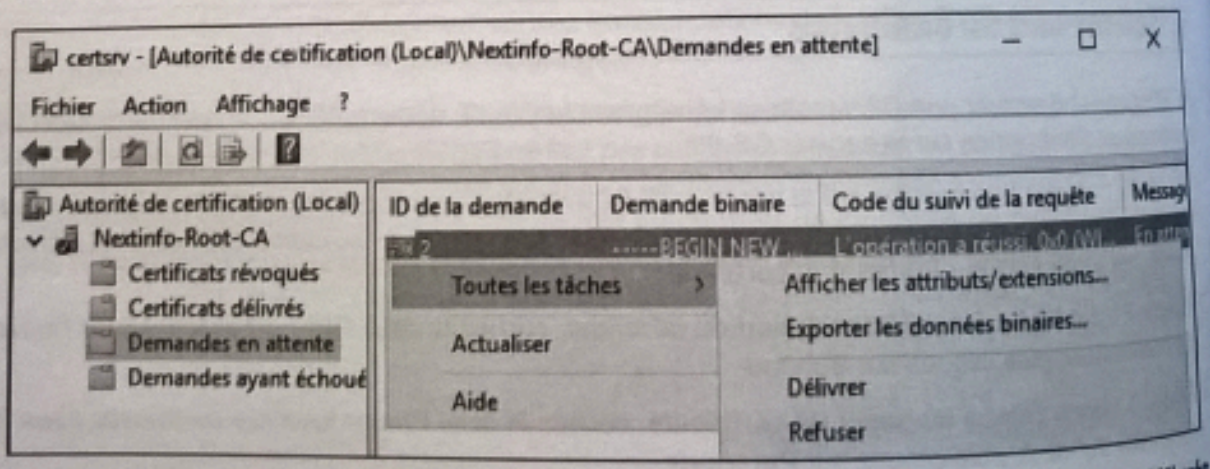
➢ **Étape 7** : copiez le fichier **C:\CS-02.nextinfo.priv_Nextinfo-Emettrice-CA.req** dans le répertoire \\CS-02\Partage.

➢ **Étape 8** : ouvrez une session sur le serveur **CS-01** avec des identifiants d'administration, et démarrez la console de gestion **Autorité de certification**. Faites un clic droit sur l'autorité de certification **Nextinfo-Root-CA** et cliquez sur **Toutes les tâches** puis **Soumettre une nouvelle demande** :



➢ **Étape 9** : sélectionnez le fichier **C:\Partage\CS-02.nextinfo.priv_Nextinfo-Emettrice-CA.req** et cliquez sur **Ouvrir**.

➢ **Étape 10** : dans l'arborescence de la console **certsrv**, sélectionnez le répertoire **Demandes en attente**. Faites un clic droit sur la requête disponible, cliquez sur **Toutes les tâches**, puis sur **Délivrer** :



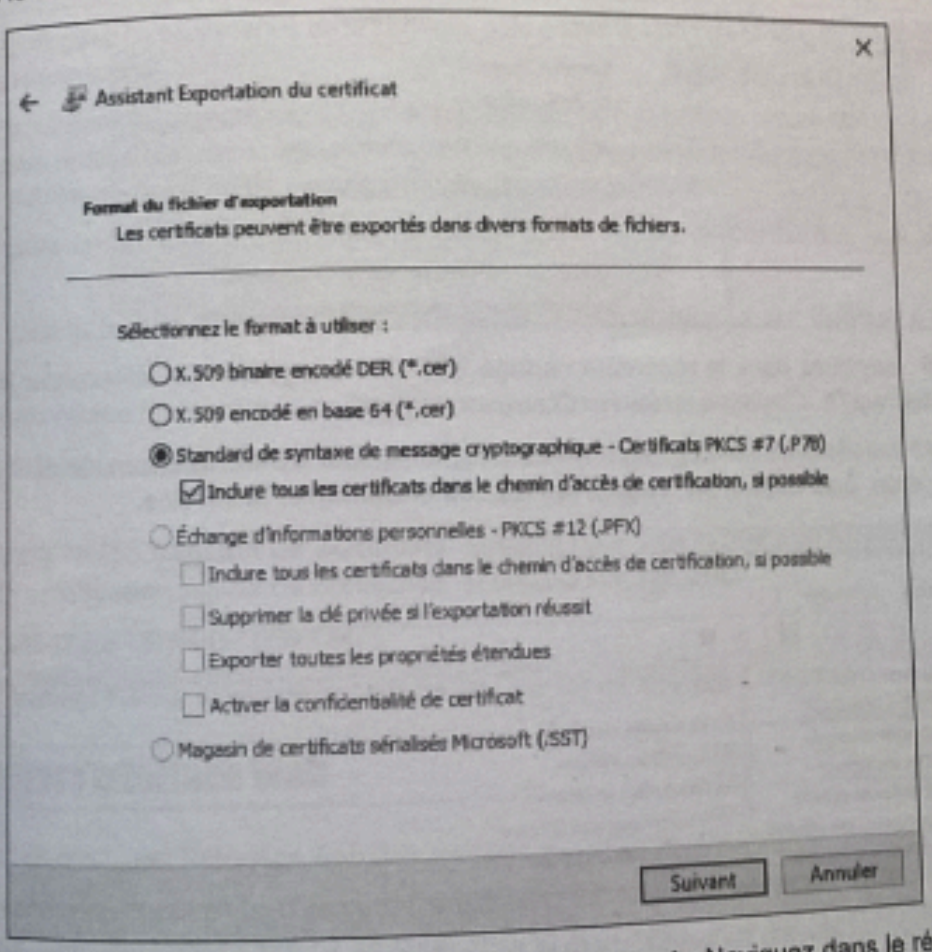
➢ **Étape 11** : dans l'arborescence de la console **certsrv**, sélectionnez le répertoire **Certificats délivrés**. Faites un clic droit sur le certificat disponible et cliquez sur **Ouvrir**.

REMPLACER CS-01 par srvcaracine
REMPLACER CS-02 srvcaiis
REMPLACER le nom du fichier par C:\ Partage \srvcaiis.webcourses.sio_webcourses-Emettrice-CA

➢ **Étape 12** : dans la fenêtre **Certificat**, cliquez sur l'onglet **Détails**, puis cliquez sur **Copier dans un fichier**.

➢ **Étape 13** : dans la fenêtre **Assistant Exportation du certificat**, cliquez sur **Suivant** à l'écran de bienvenue.

➢ **Étape 14** : dans l'étape **Format du fichier d'exportation**, cochez la case **Standard de syntaxe de message cryptographique - Certificats PKCS #7 (.P7B)**. Cochez la case **Inclure tous les certificats dans le chemin d'accès de certification, si possible** et cliquez sur **Suivant** :

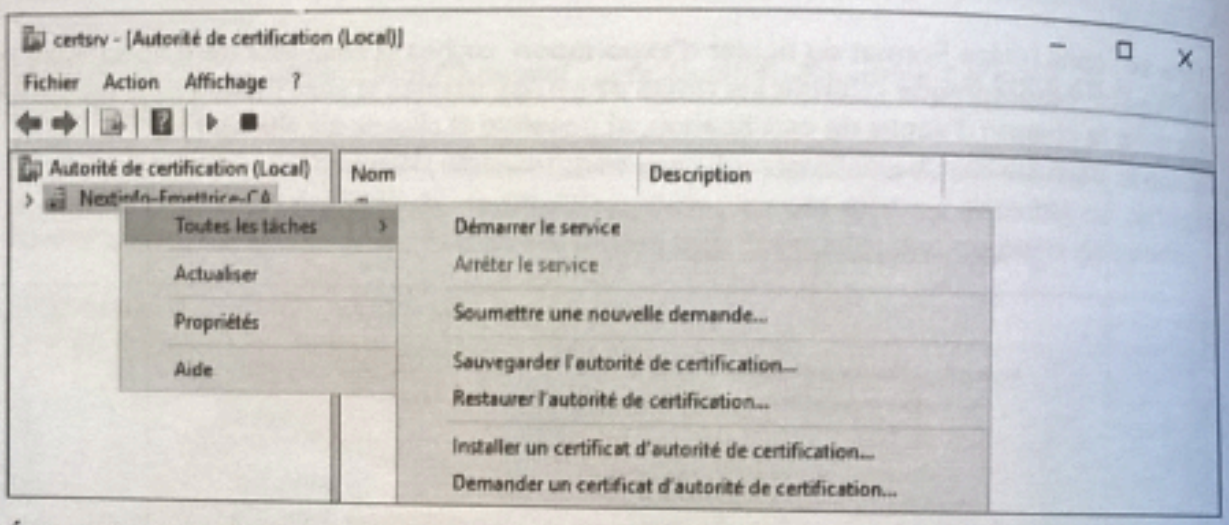


➢ **Étape 15** : dans l'étape **Fichier à exporter**, cliquez sur **Parcourir**. Naviguez dans le répertoire partagé \\CS-02\Partage et tapez *CA-Intermediaire.p7b* dans le **Nom du fichier**. Cliquez ensuite sur **Enregistrer**.

D'après les bonnes pratiques, l'autorité de certification racine doit être déconnectée du réseau après son installation. En condition réelle, l'opération de transfert d'un certificat vers un autre ordinateur doit être réalisée à l'aide d'un support amovible.

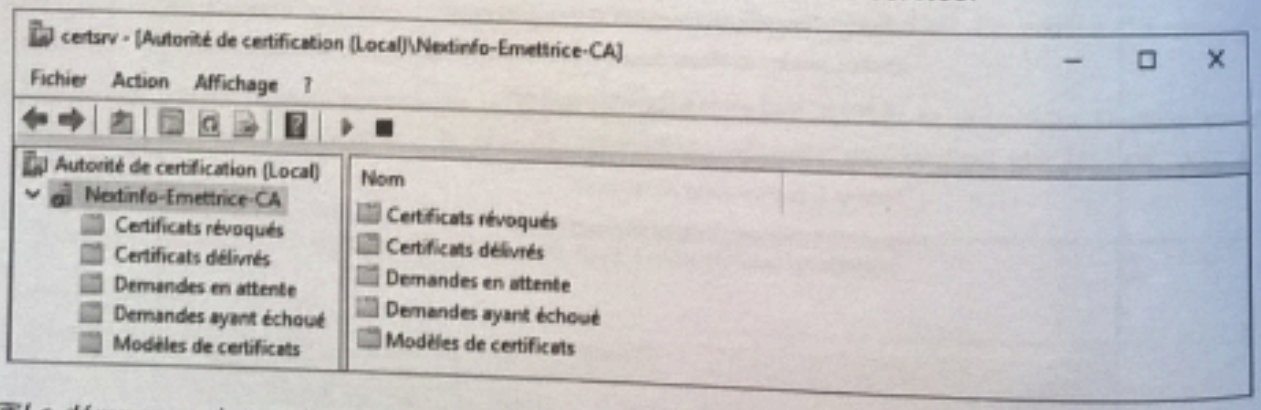
➢ **Étape 16** : cliquez sur **Suivant** puis **Terminer**. Lorsque l'exportation du certificat est terminée, cliquez sur **OK** deux fois.

➢ **Étape 17** : ouvrez une session sur le serveur **CS-02** avec des identifiants d'administration du domaine Nextinfo.priv, et démarrez la console de gestion **Autorité de certification**. Faites un clic droit sur l'autorité de certification *Nextinfo-Emettrice-CA* et cliquez sur **Toutes les tâches** puis **Installer un certificat d'autorité de certification** :



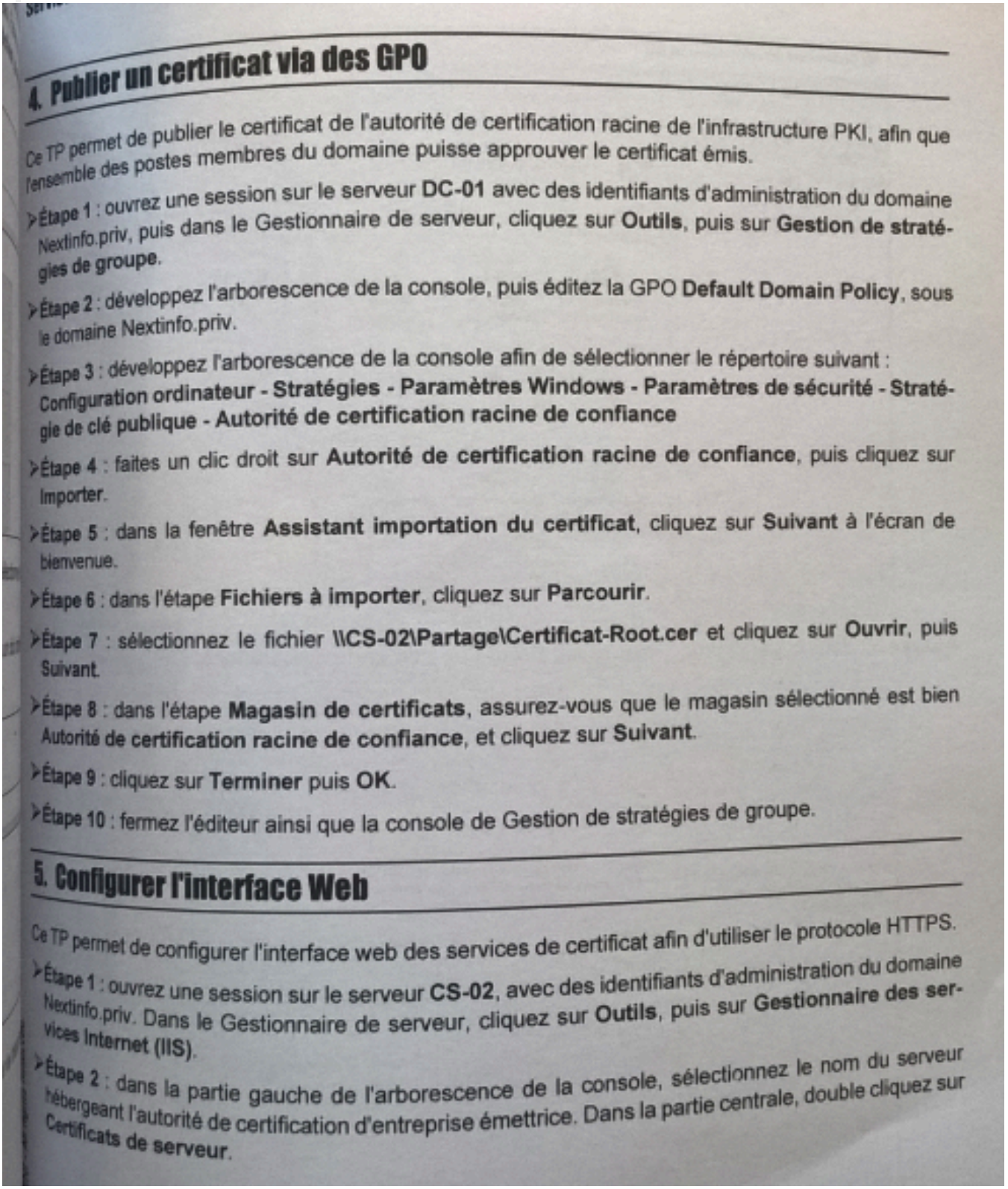
➢ **Étape 18** : naviguez dans le répertoire partagé \\CS-02\Partage afin de sélectionner le fichier **CA-Intermediaire.p7b**. Cliquez ensuite sur **Ouvrir**.

➢ **Étape 19** : dans la console de gestion **certsrv** sur le serveur **CS-02**, faites un clic droit sur l'autorité de certification, puis cliquez sur **Toutes les tâches** et **Démarrer le service**.



☞ *Le démarrage du service de certificats peut également se faire en cliquant sur le triangle vert de la barre des tâches.*

REMPLACER CS-02 srvcaiis



4. Publier un certificat via des GPO

Ce TP permet de publier le certificat de l'autorité de certification racine de l'infrastructure PKI, afin que l'ensemble des postes membres du domaine puisse approuver le certificat émis.

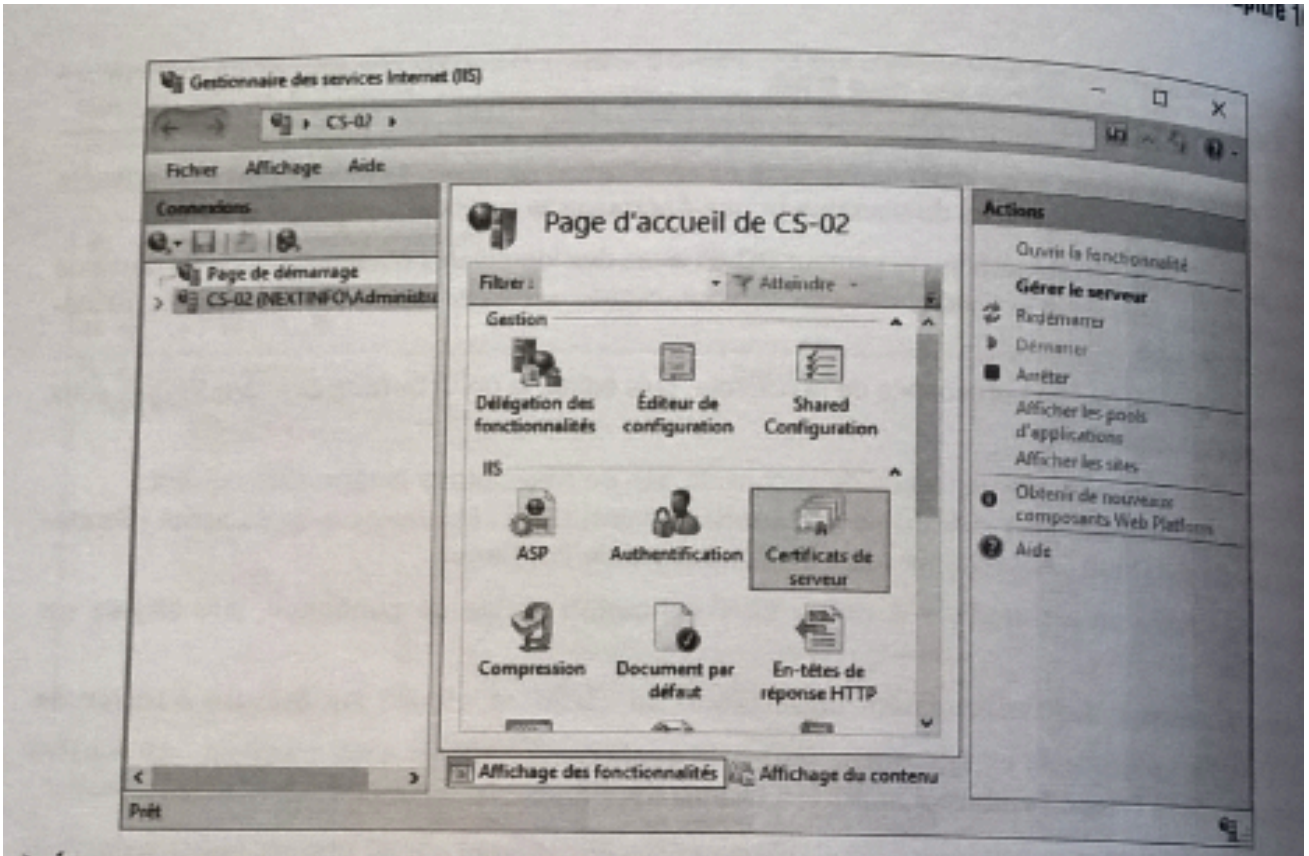
- Étape 1 : ouvrez une session sur le serveur **DC-01** avec des identifiants d'administration du domaine Nextinfo.priv, puis dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestion de stratégies de groupe**.
- Étape 2 : développez l'arborescence de la console, puis éditez la GPO **Default Domain Policy**, sous le domaine Nextinfo.priv.
- Étape 3 : développez l'arborescence de la console afin de sélectionner le répertoire suivant : **Configuration ordinateur - Stratégies - Paramètres Windows - Paramètres de sécurité - Stratégie de clé publique - Autorité de certification racine de confiance**
- Étape 4 : faites un clic droit sur **Autorité de certification racine de confiance**, puis cliquez sur Importer.
- Étape 5 : dans la fenêtre **Assistant importation du certificat**, cliquez sur **Suivant** à l'écran de bienvenue.
- Étape 6 : dans l'étape **Fichiers à importer**, cliquez sur **Parcourir**.
- Étape 7 : sélectionnez le fichier **\\CS-02\Partage\Certificat-Root.cer** et cliquez sur **Ouvrir**, puis Suivant.
- Étape 8 : dans l'étape **Magasin de certificats**, assurez-vous que le magasin sélectionné est bien **Autorité de certification racine de confiance**, et cliquez sur **Suivant**.
- Étape 9 : cliquez sur **Terminer** puis **OK**.
- Étape 10 : fermez l'éditeur ainsi que la console de Gestion de stratégies de groupe.

5. Configurer l'interface Web

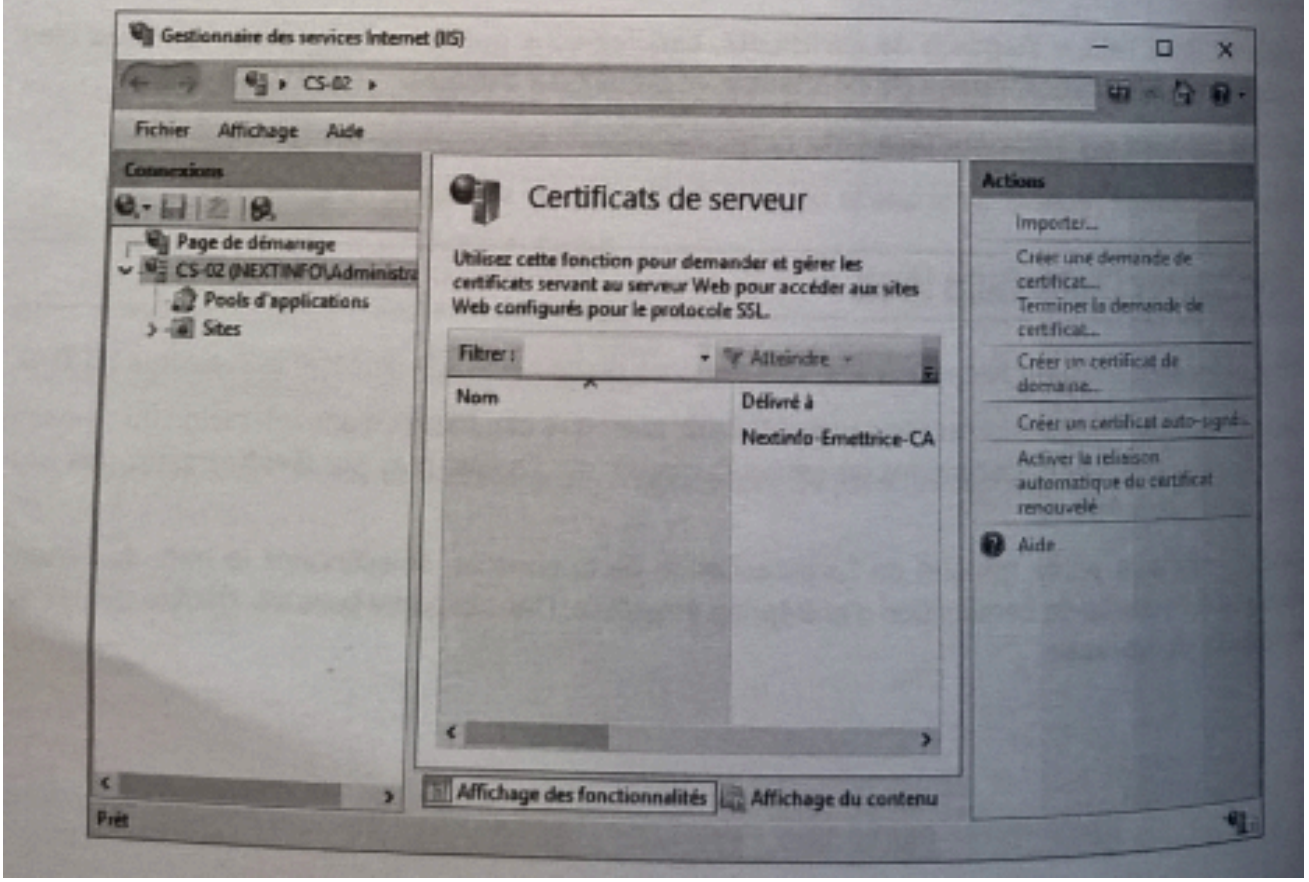
Ce TP permet de configurer l'interface web des services de certificat afin d'utiliser le protocole HTTPS.

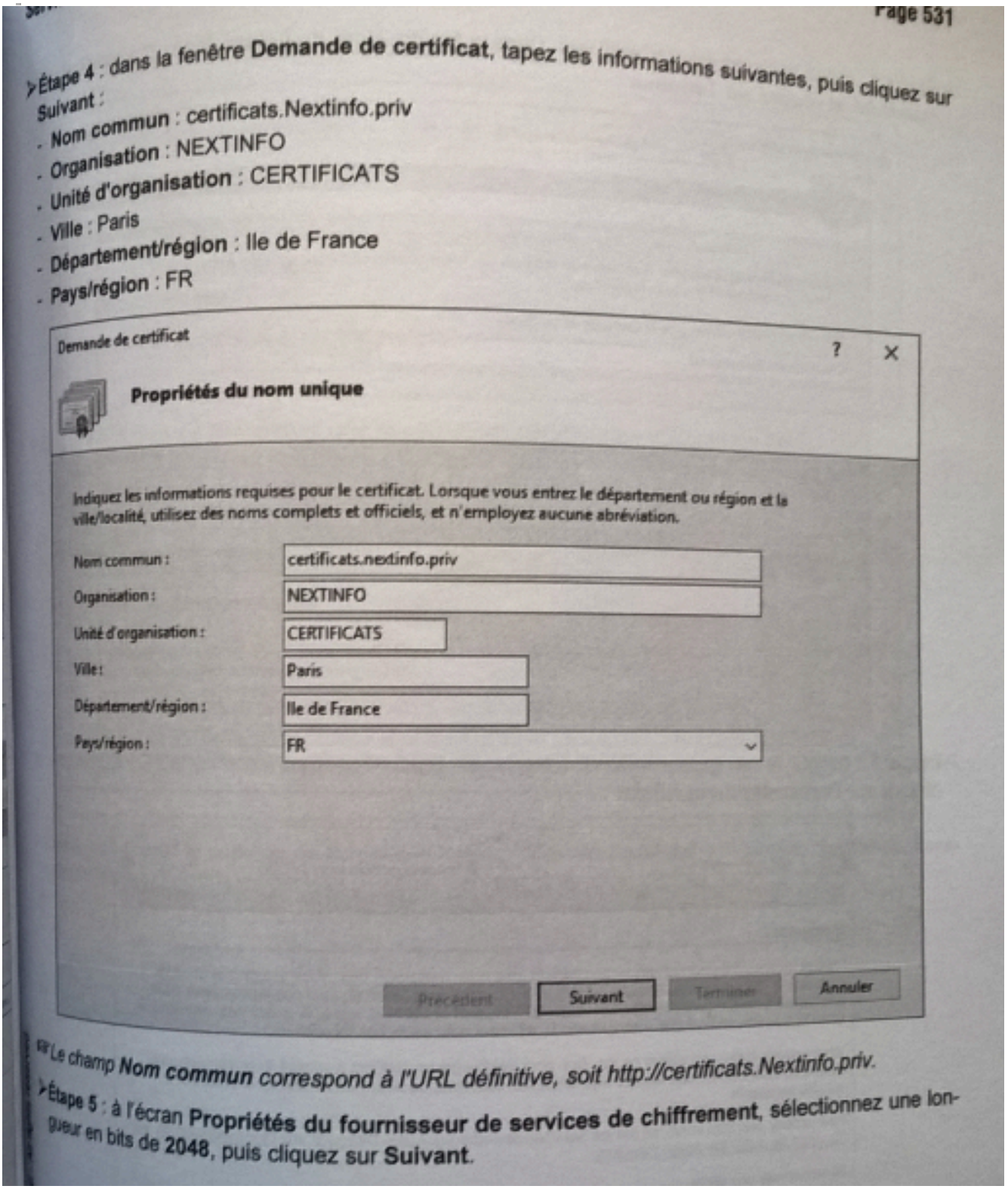
- Étape 1 : ouvrez une session sur le serveur **CS-02**, avec des identifiants d'administration du domaine Nextinfo.priv. Dans le Gestionnaire de serveur, cliquez sur **Outils**, puis sur **Gestionnaire des services Internet (IIS)**.
- Étape 2 : dans la partie gauche de l'arborescence de la console, sélectionnez le nom du serveur hébergeant l'autorité de certification d'entreprise émettrice. Dans la partie centrale, double cliquez sur **Certificats de serveur**.

REMPLACER CS-02 srvcaiis
REMPLACER DC-01 srvaddns



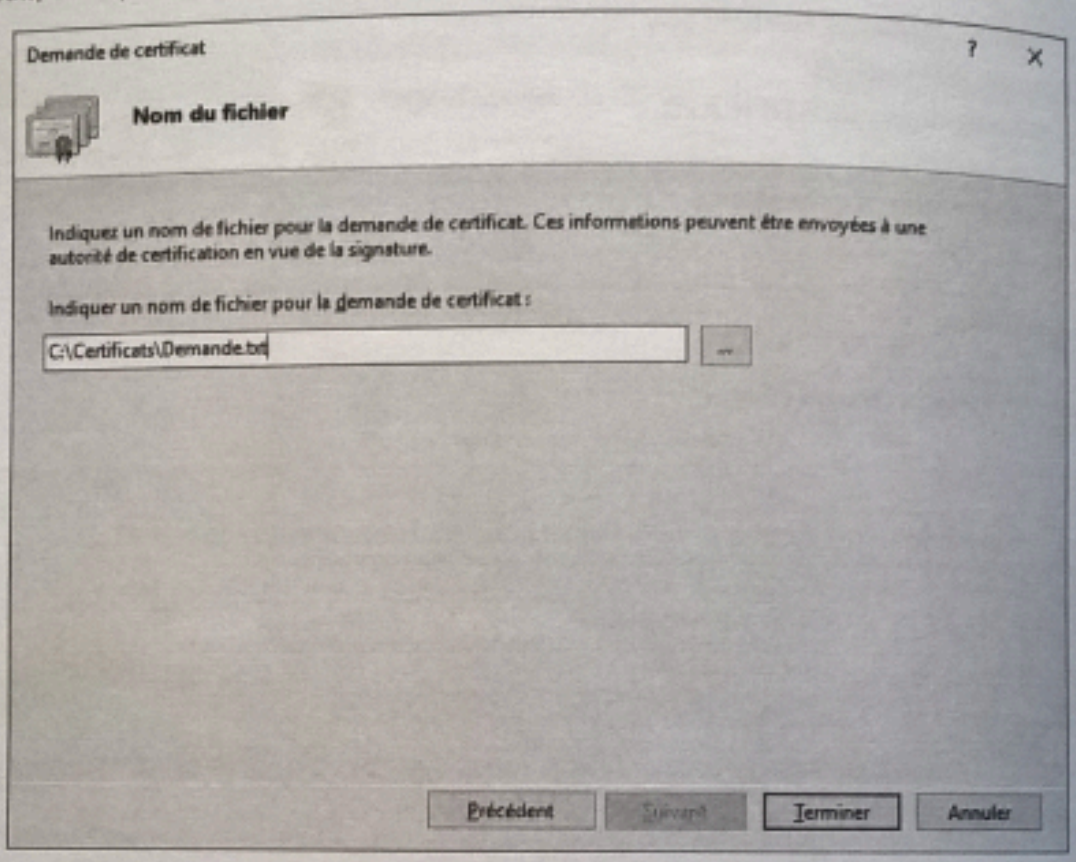
➢ **Étape 3** : dans la partie droite, cliquez sur **Créer une demande de certificat** :



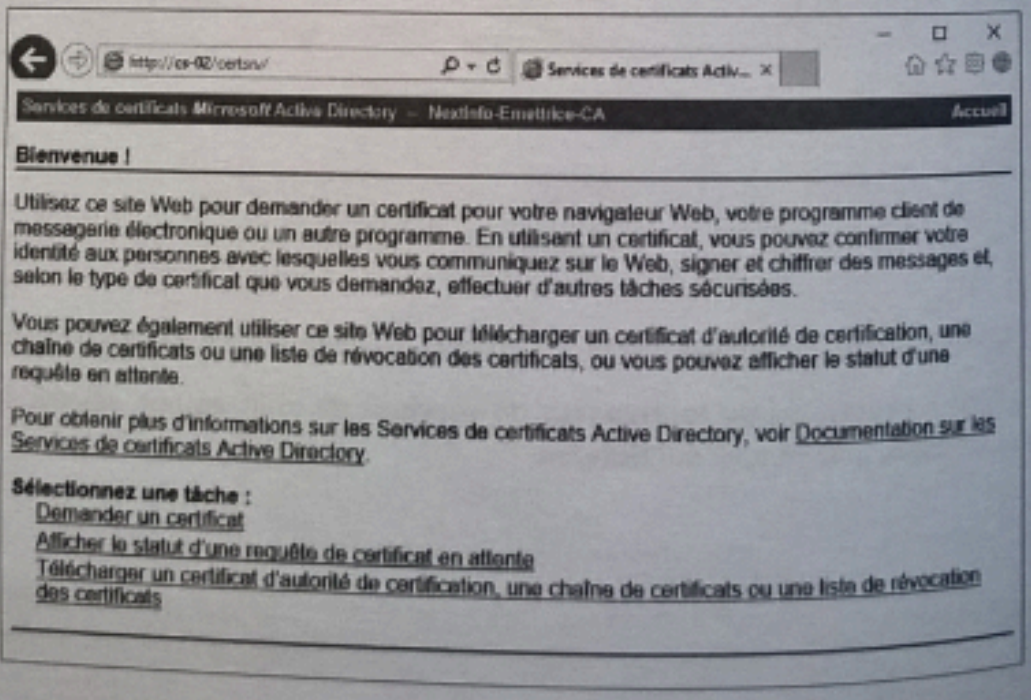


REMPLACER Nexinfo.priv par webcourses.sio
REMPLACER NEXINFO par webcourses

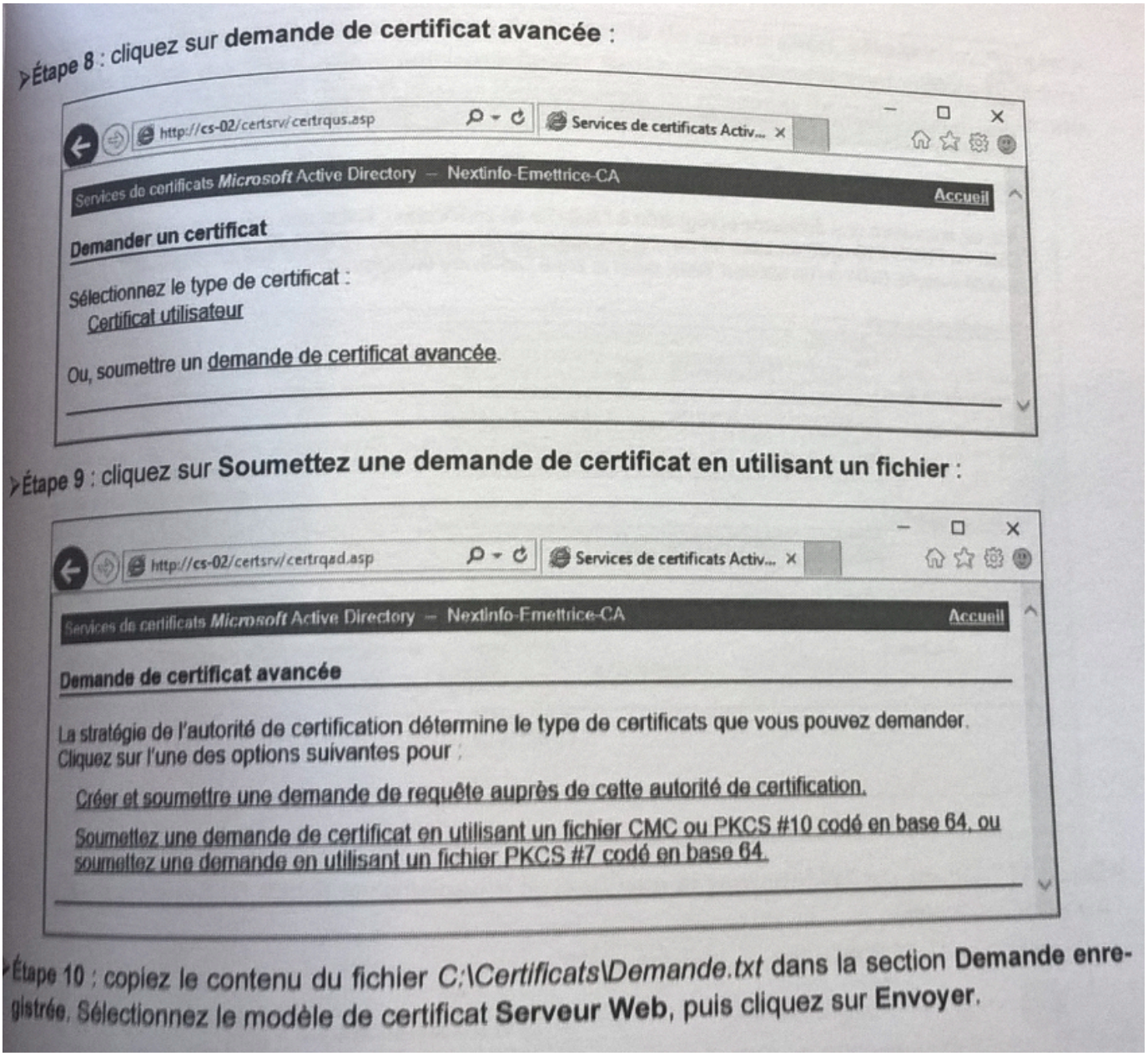
➢ **Étape 6** : créez le répertoire C:\Certificats. Dans la fenêtre **Nom du fichier**, tapez C:\Certificats\Demande.txt, et cliquez sur **Terminer** :



➢ **Étape 7** : ouvrez le navigateur Internet Explorer en tapant l'URL suivante : *http://CS-02/certsrv*, et cliquez sur **Demander un certificat** :

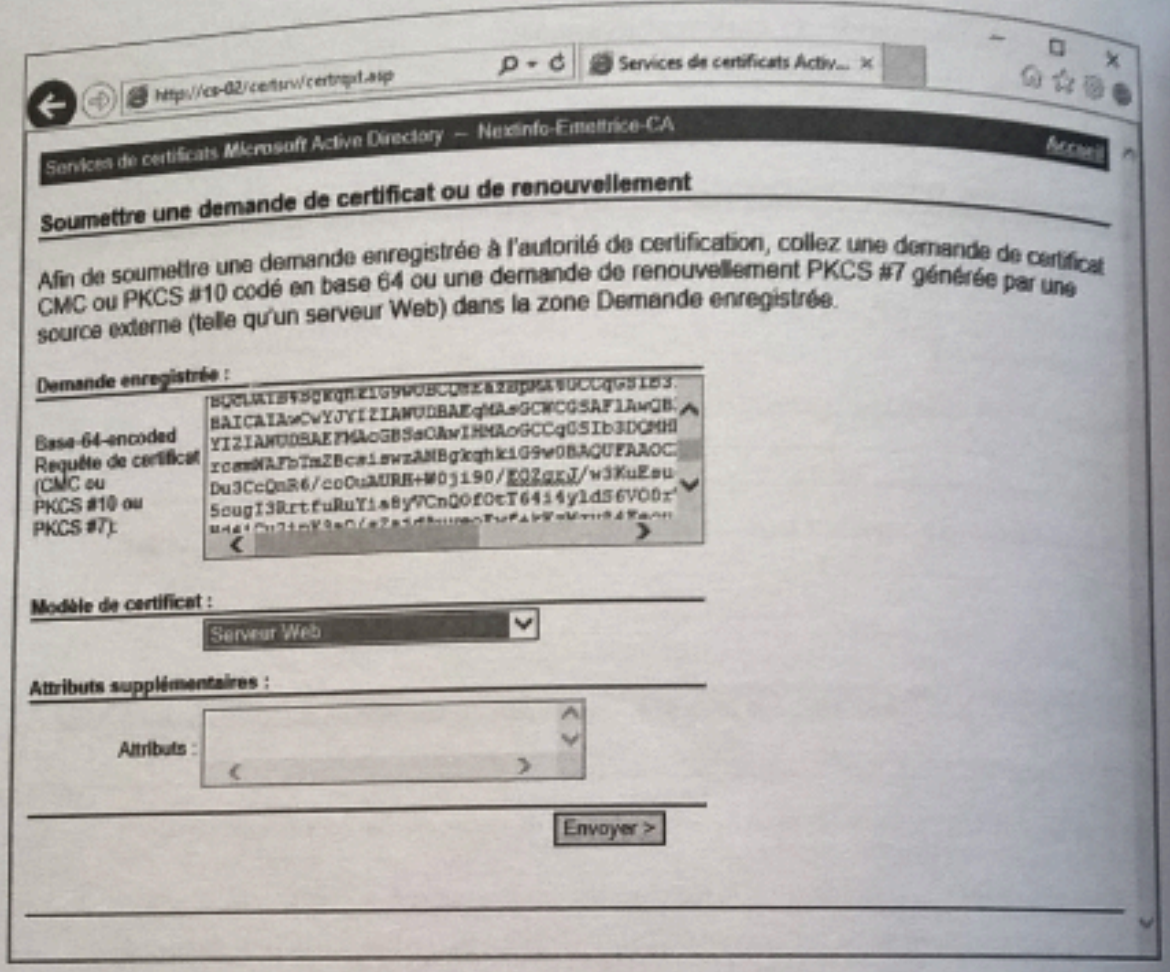


➢Étape 8 : cliquez sur **demande de certificat avancée** :

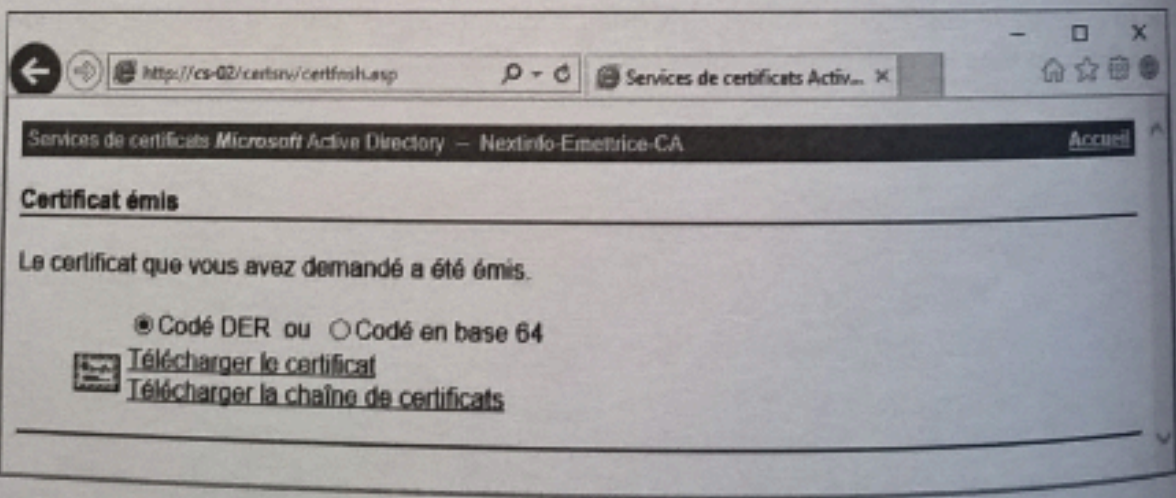


➢Étape 9 : cliquez sur **Soumettez une demande de certificat en utilisant un fichier** :

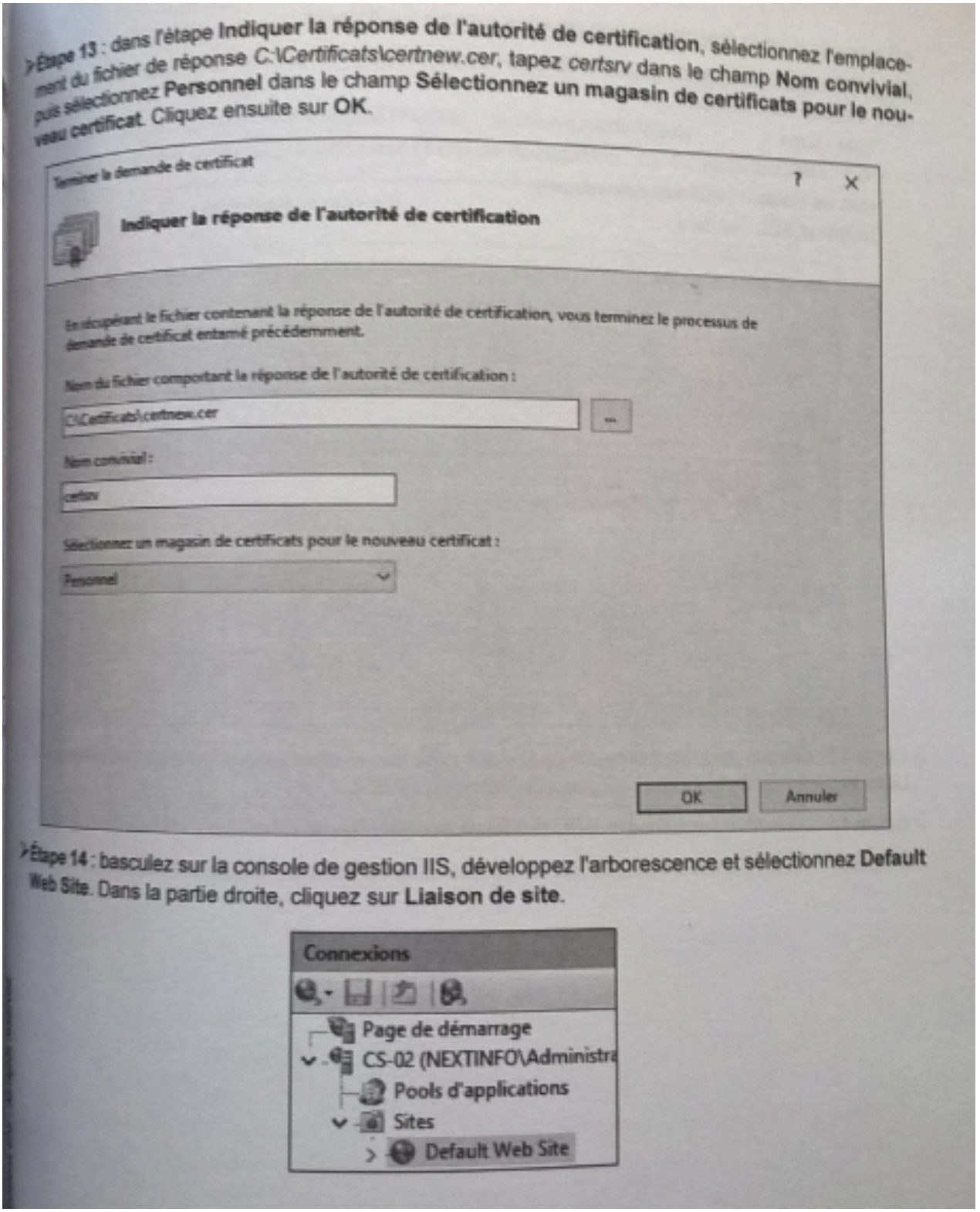
➢Étape 10 : copiez le contenu du fichier *C:\Certificats\Demande.txt* dans la section **Demande enregistrée**. Sélectionnez le modèle de certificat **Serveur Web**, puis cliquez sur **Envoyer**.



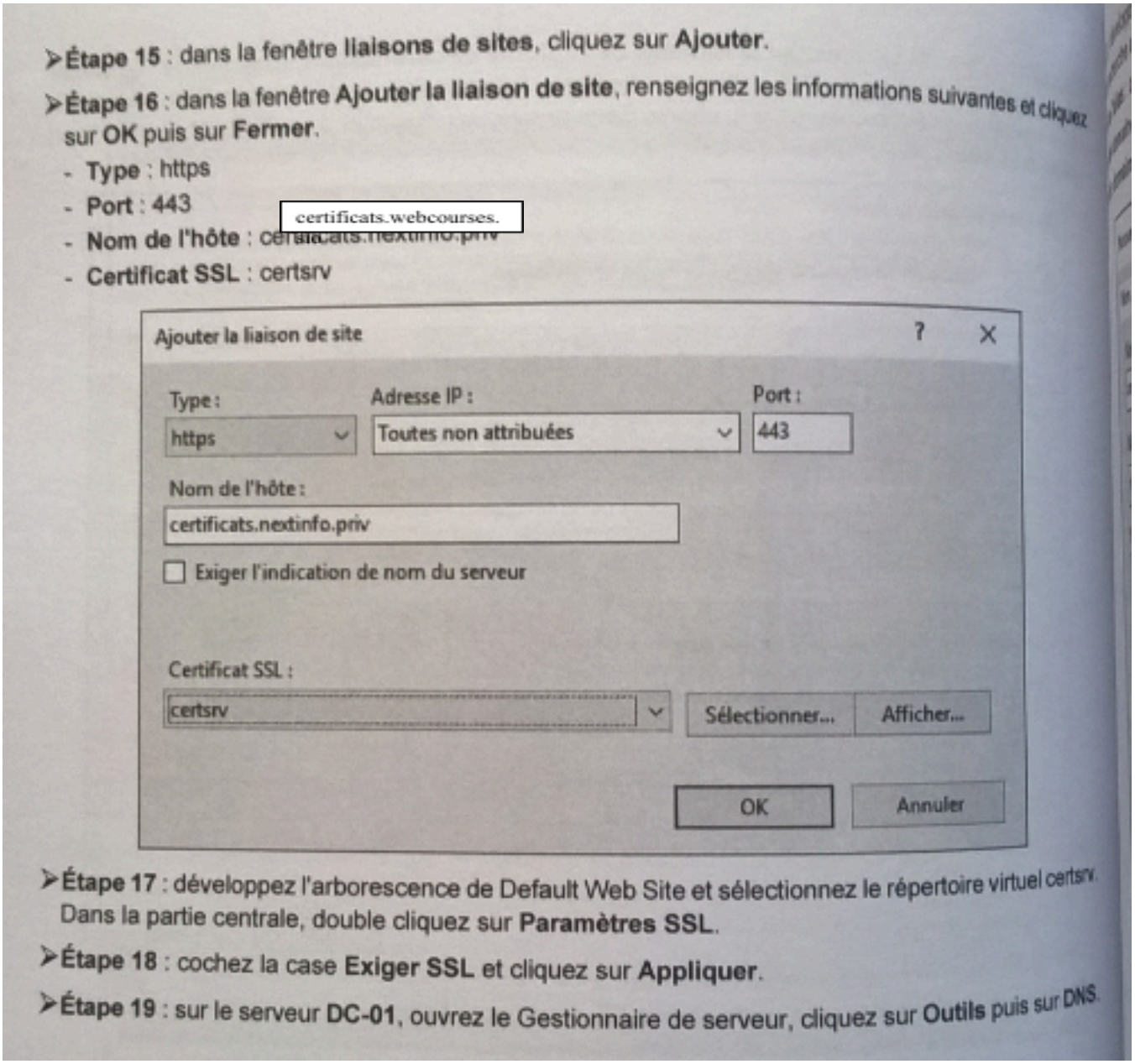
➢ **Étape 11** : cliquez sur **Télécharger le certificat** et enregistrez le fichier *Certnew.cer* dans le répertoire *C:\Certificats* :



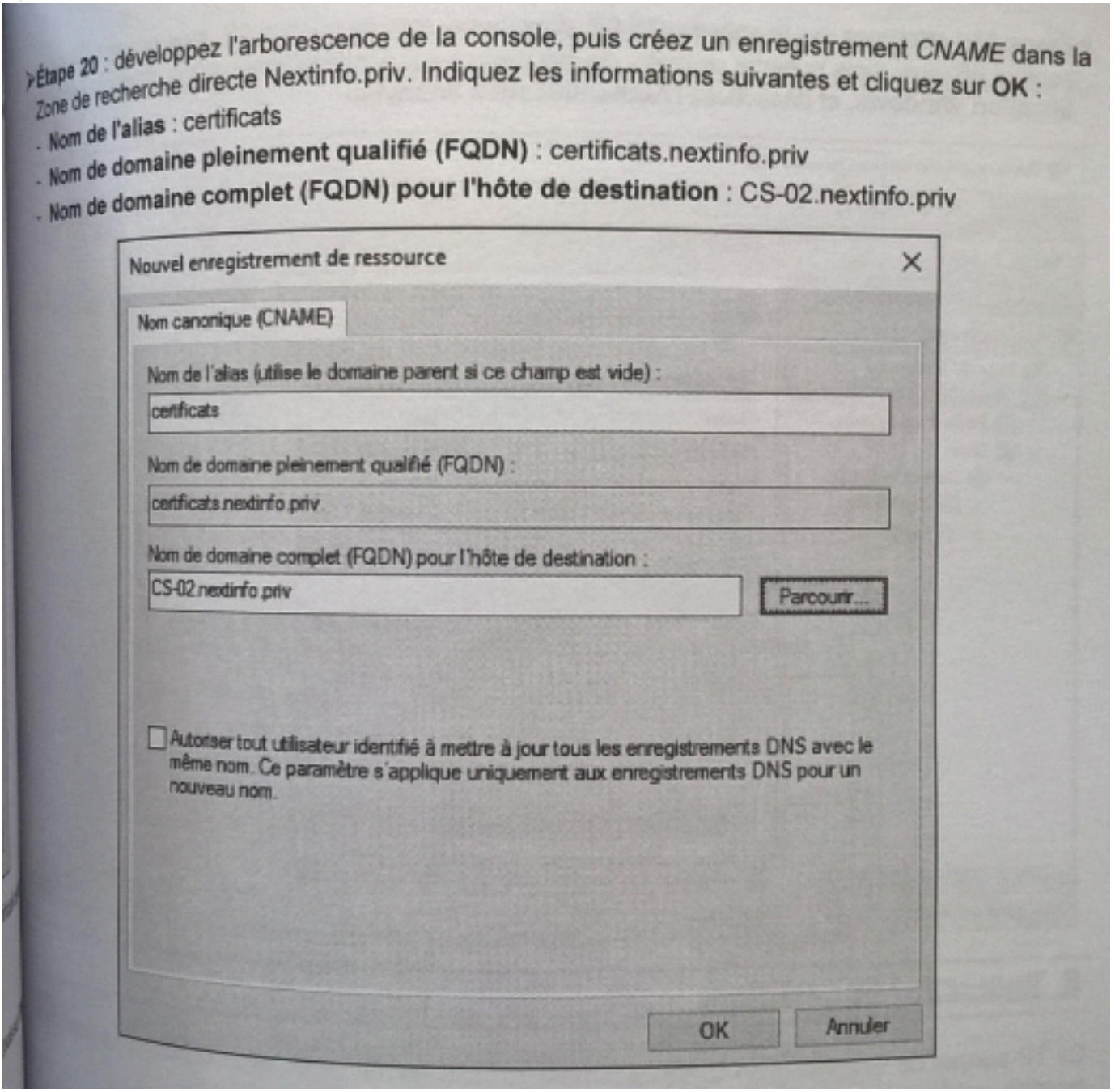
➢ **Étape 12** : basculez sur la console de gestion IIS et dans la partie droite, cliquez sur **Terminer la demande de certificat**.



Vous devez avoir srvcaiis (webcourses\Administrateur au lieu de CD-02 (NETINFO Administrateur

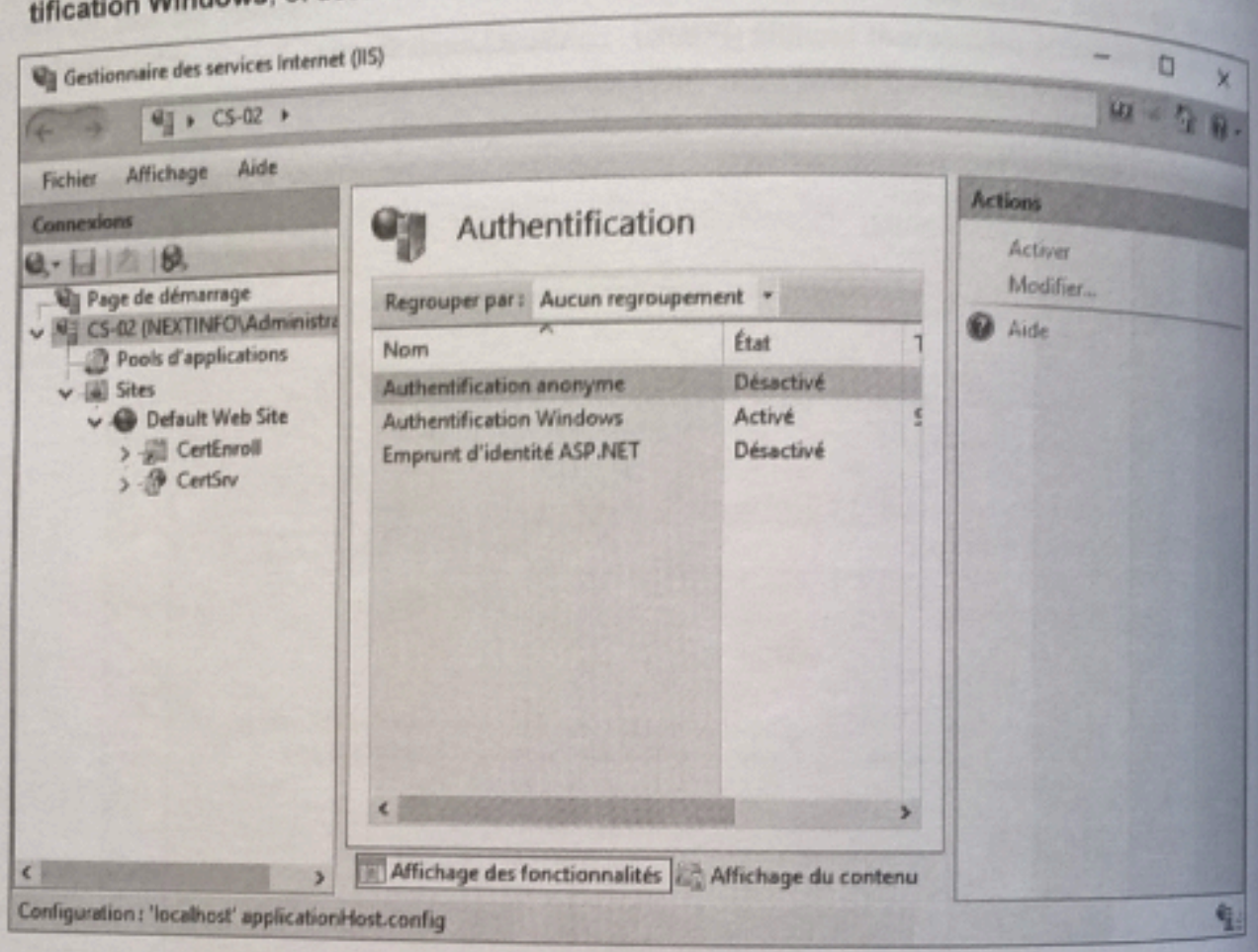


REMPLACER DC-01 par srvaddns



REMPLACER CS-02.netinfo.priv par srvcaiis.webcourses.sio

➢ **Étape 21** : retournez sur le serveur **CS-02**, dans la console de gestion IIS, sélectionnez le nom du serveur IIS, puis dans la partie centrale, double cliquez sur **Authentification** afin d'activer l'**Authentification Windows**, et désactivez l'**Authentification anonyme** :



6. Demander un certificat

Ce TP permet de demander un certificat auprès de l'autorité de certification émettrice. Le certificat à émettre doit être de type Basique EFS, pour l'utilisateur Jean DUPONT.

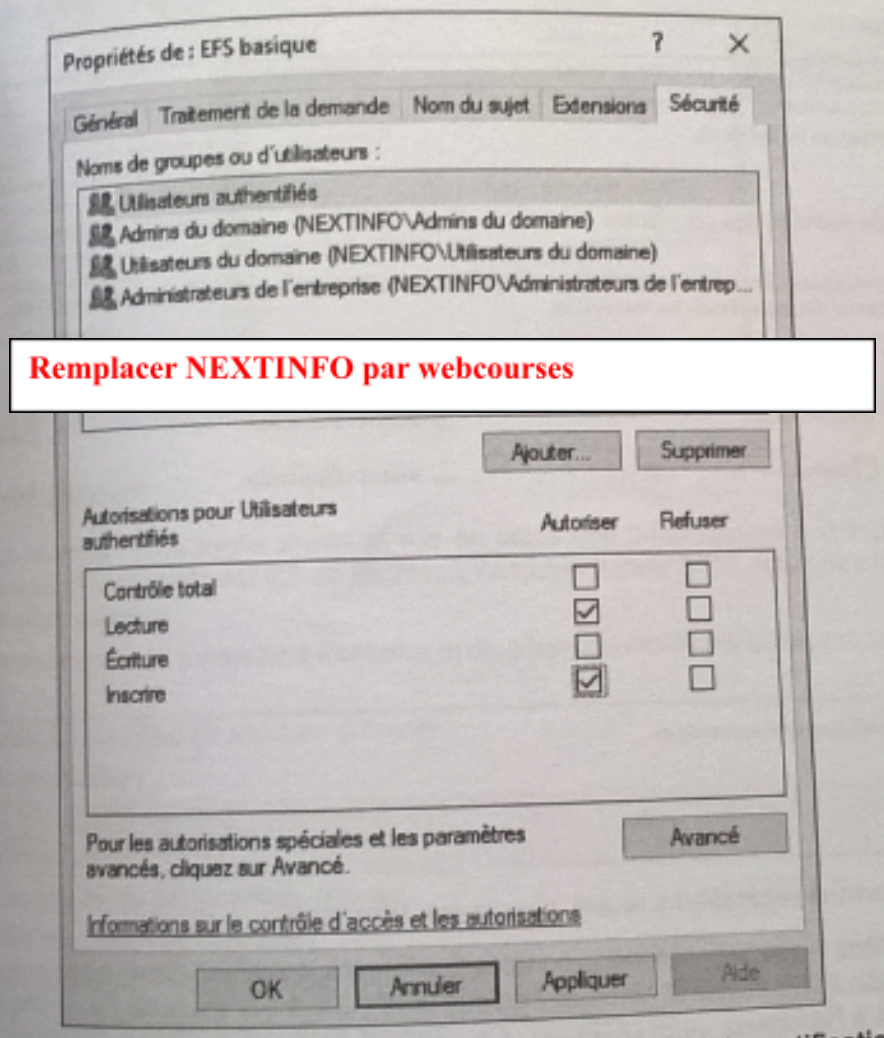
➢ **Étape 1** : ouvrez une session sur le serveur **CS-02** avec des identifiants d'administration du domaine *Nextinfo.priv*. Démarrez le Gestionnaire de serveur, cliquez sur **Outils** puis sur **Autorité de certification**.

➢ **Étape 2** : développez l'arborescence de la console **Autorité de certification**, sélectionnez le conteneur **Modèles de certificats**, faites un clic droit dessus puis cliquez sur **Gérer**.

➢ **Étape 3** : dans la liste des modèles de certificats disponibles, faites un clic droit sur **EFS basique** et cliquez sur **Propriétés**.

REMPLACER CS-02 srvcaiis
REPLACER Jean DUPONT par PDG

➢ Étape 4 : dans la fenêtre **Propriétés de : EFS basique**, cliquez sur l'onglet **Sécurité**. Sélectionnez le groupe **Utilisateurs authentifiés**, cochez le droit **Inscrire** comme étant autorisé, puis cliquez sur OK :



Remplacer NEXTINFO par webcourses

➢ Étape 5 : fermez toutes les fenêtres de la console de gestion **Autorité de certification**.

➢ Étape 6 : ouvrez une session sur le poste **CLIENT1** avec des identifiants d'utilisateur du domaine Nextinfo.priv (se connecter avec le login : jdupont ; si ce compte d'utilisateur n'existe pas dans la base Active Directory, créez-le).

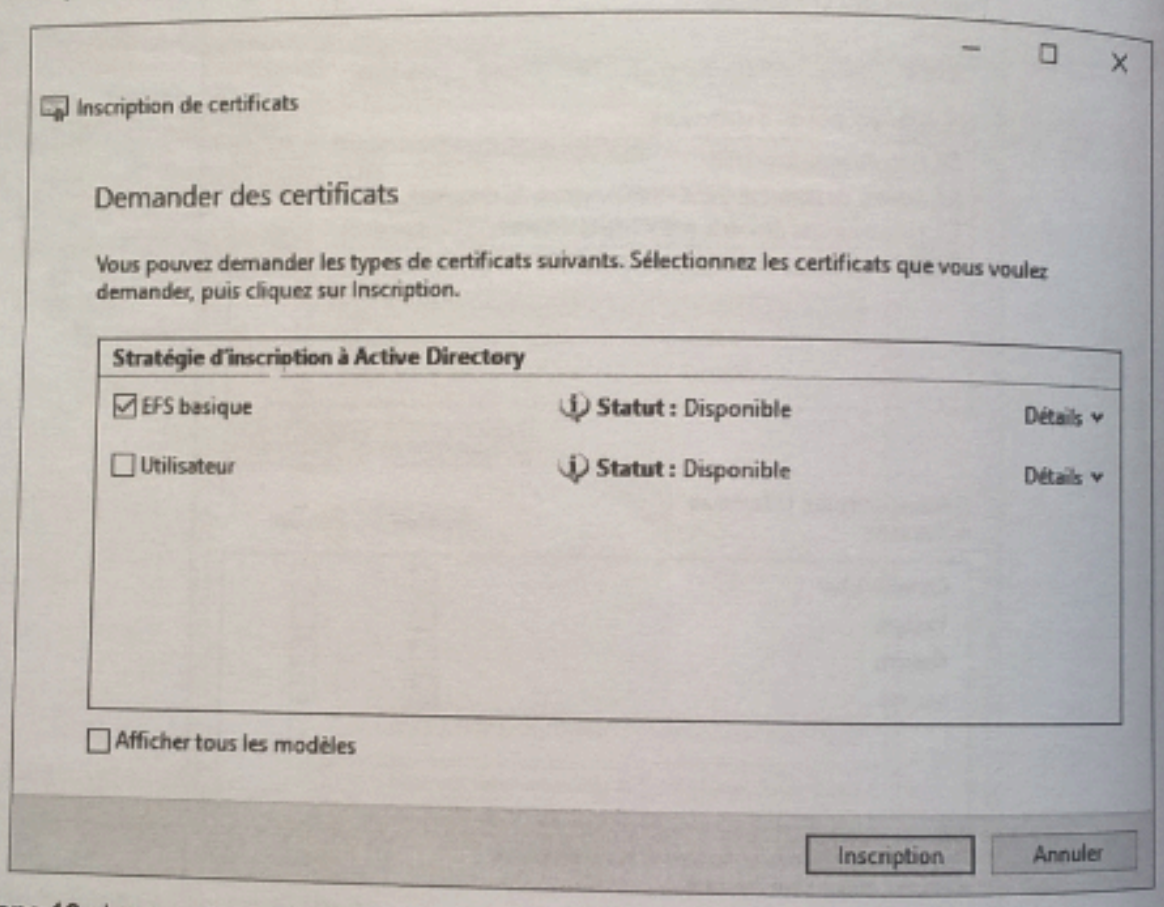
➢ Étape 7 : dans la console MMC, ajoutez le composant logiciel enfichable **Certificats**.

➢ Étape 8 : développez l'arborescence de la console afin de sélectionner le conteneur **Personnel**. Faites un clic droit dessus et cliquez sur **Toutes les tâches**, puis sur **Demander un nouveau certificat**.

➢ Étape 9 : à l'écran **Avant de commencer**, cliquez sur **Suivant**.

➢ **Étape 10** : à l'écran **Sélectionnez la stratégie d'inscription de certificat**, sélectionnez la stratégie d'inscription Active Directory et cliquez sur **Suivant**.

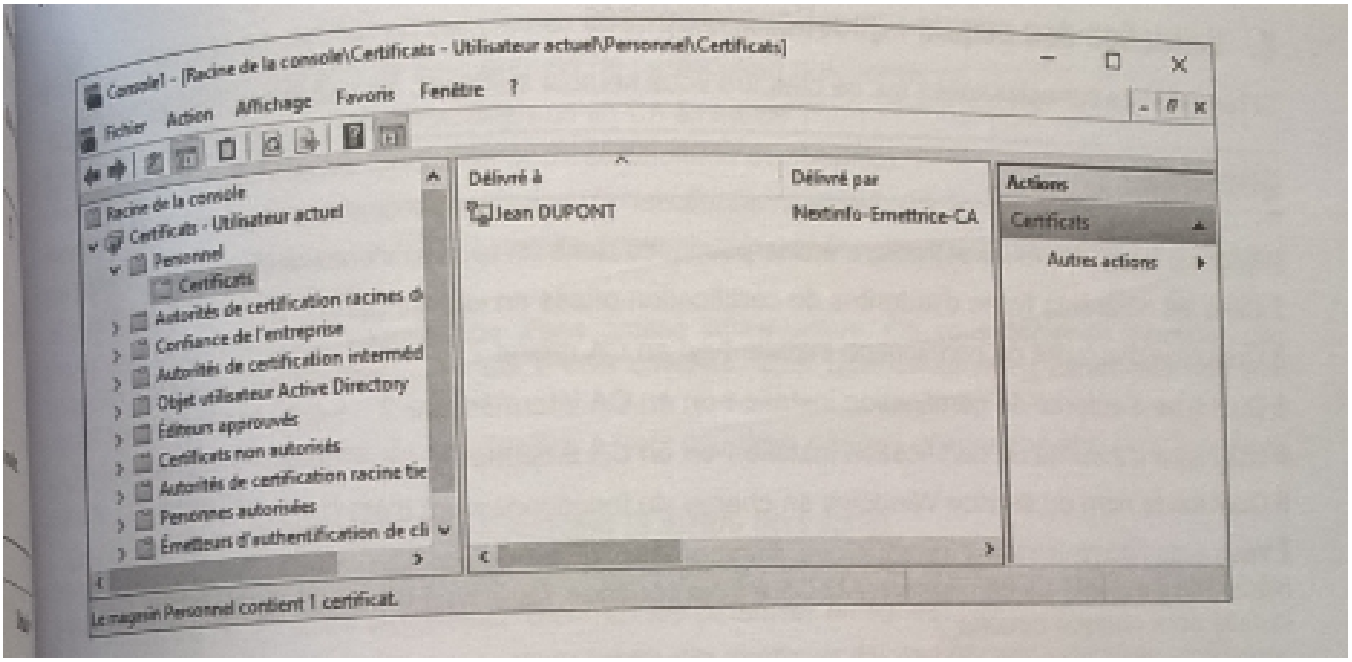
➢ **Étape 11** : cochez la case correspondant au modèle de certificat EFS basique, puis cliquez sur **Inscription** :



➢ **Étape 12** : lorsque l'opération a réussi, cliquez sur **Terminer**.

➢ **Étape 13** : dans l'arborescence de la console **Certificats**, naviguez dans le conteneur **Personnel/ Certificats** afin d'apercevoir le certificat basique EFS délivré par l'autorité de certification *Nextinfo-Emettrice-CA* à l'utilisateur Jean DUPONT. Ce certificat peut désormais être utilisé pour chiffrer des données locales avec la technologie EFS (*Encrypting File System*).

REPLACER Jean DUPONT par PDG<



Qu'est-ce qu'un certificat ?

Quel est son rôle ?

Mission 11 Documenter AD CS gestion des certificats

Compétences	Reprendre toutes les compétences relatives aux différentes missions
Objectifs	Documenter AD CS les certificats
Vocabulaire à connaître	
Évaluation	Compte-rendu à rendre pour évaluation sommative coefficient 2 Compte-rendu est à poser dans votre PFC Épreuve E4 certificative

Page de garde

10. L'entête de chaque page doit contenir les informations suivantes :

22. Nom de l'établissement
23. Titre complet de l'activité
24. La version du document

11. Le pied de chaque page doit contenir les informations suivantes :

25. L'auteur / les auteurs
26. Numéro de page
27. Date

12. Au centre de la page

28. Donner l'objectif principal de l'activité

Sommaire ou table des matières

4. **Automatiser** votre sommaire

Introduction

4. **Présenter**
   4.1. le contexte sur lequel vous travaillez (Description de la ligue de marathon)
   4.2. Description de son logo (celui que vous avez choisi sur votre site) représentation, symbole, lien Internet si vous l'avez récupéré sur une bibliothèque d'images

Déroulé de la mission 9

5. **Donner** le schéma réseau global associé au contexte de la mission 9
6. **Préciser** les contraintes liées aux Prérequis si nécessaires

7. **Notifier** les points de vigilance de la mission

8. **Expliquer** les points de blocage et les solutions apportées
9. **Montrer** à l'aide d'une copie écran les résultats obtenus après les mises en place des missions

Analyse de l'activité

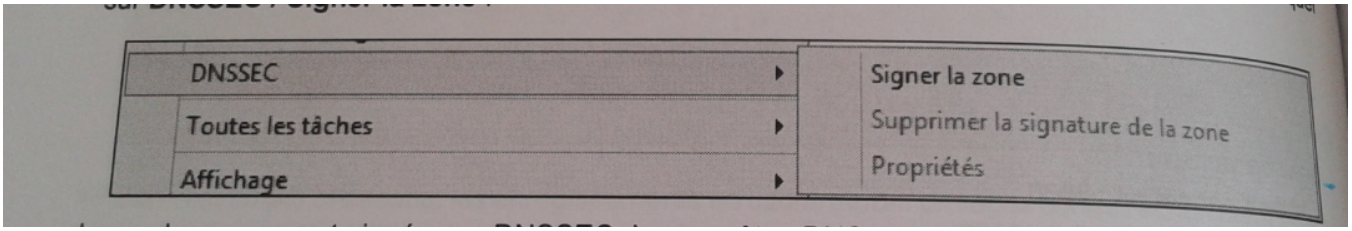
10. Spécifier les difficultés rencontrées au cours des différentes phases de mise en place
11. Mentionner les apports professionnels acquis à travers cette expérience
12. Préciser les apports personnels acquis à travers cette expérience

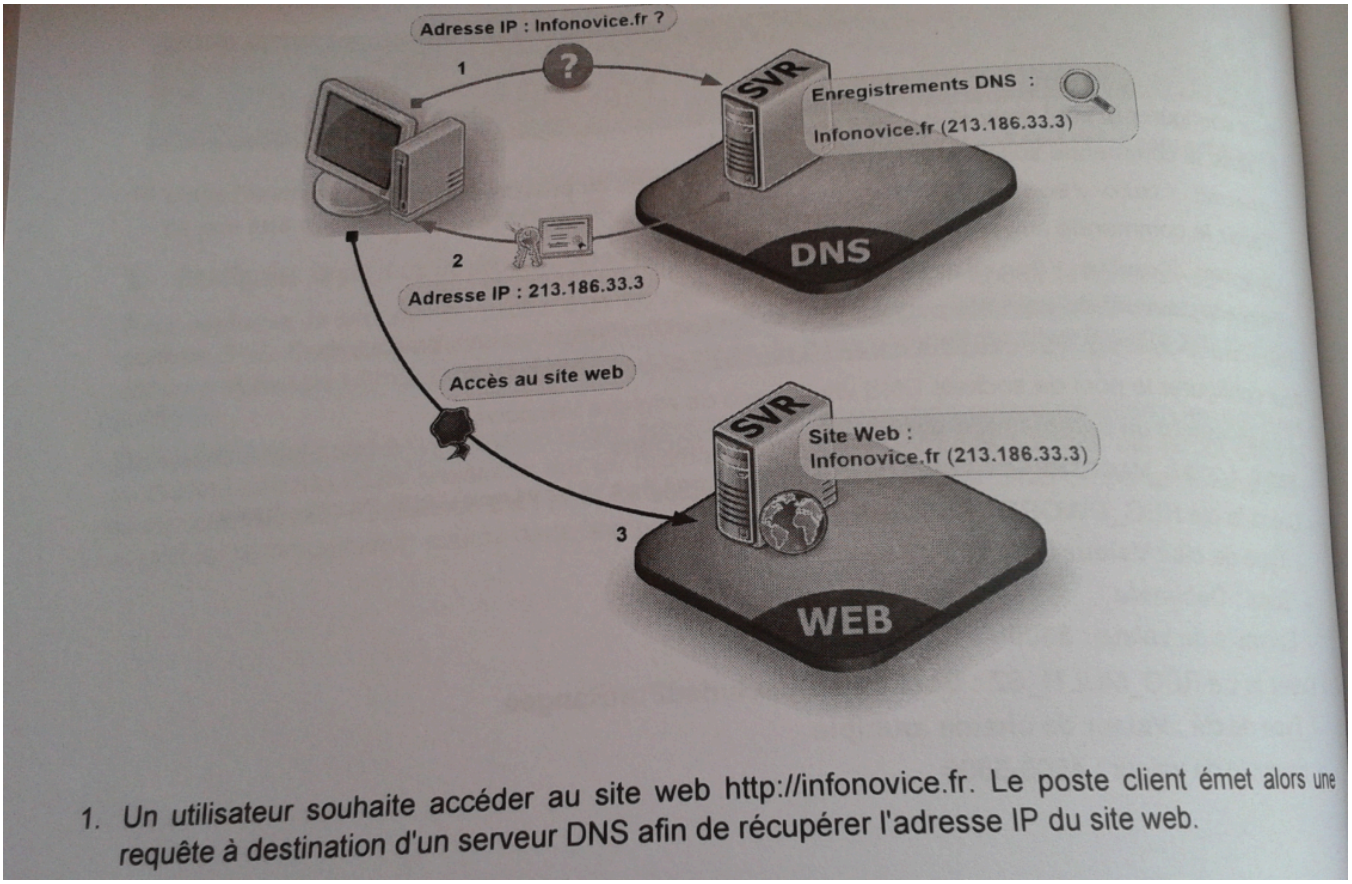
Mission 12 Cybersécurité DNSSEC

Compétences	Reprendre toutes les compétences relatives aux différentes missions
Objectifs	**Installer** le DNSSEC
Vocabulaire à connaître	
Évaluation	Compte-rendu à rendre pour évaluation sommative coefficient 2 Compte-rendu est à poser dans votre PFC Épreuve E4 certificative

Informations utiles

DNSSEC Domain Name System Security Extension) est un protocole standard permettant la signature numérique d'une zone.

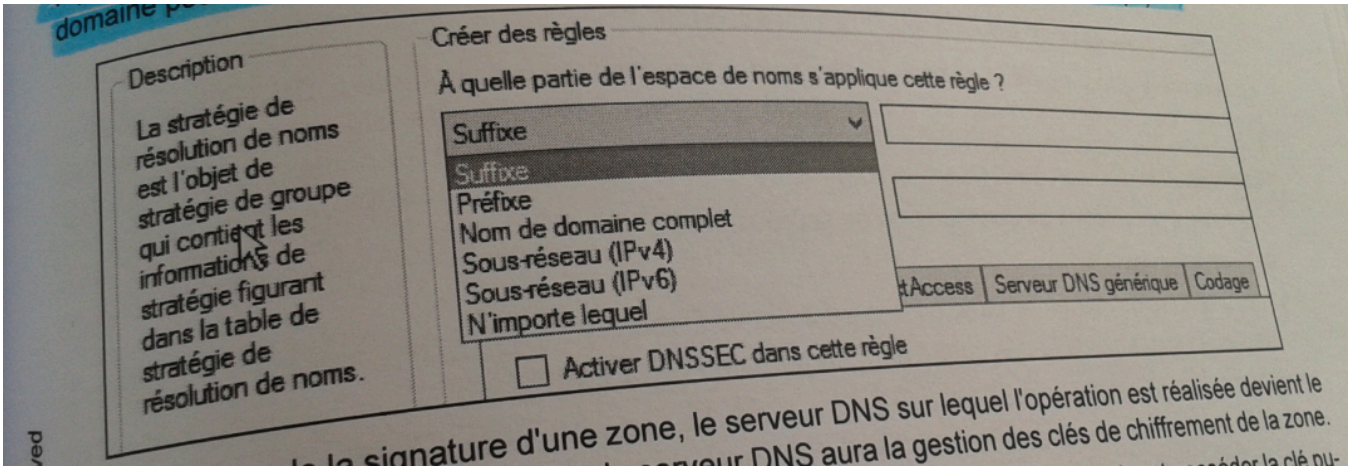




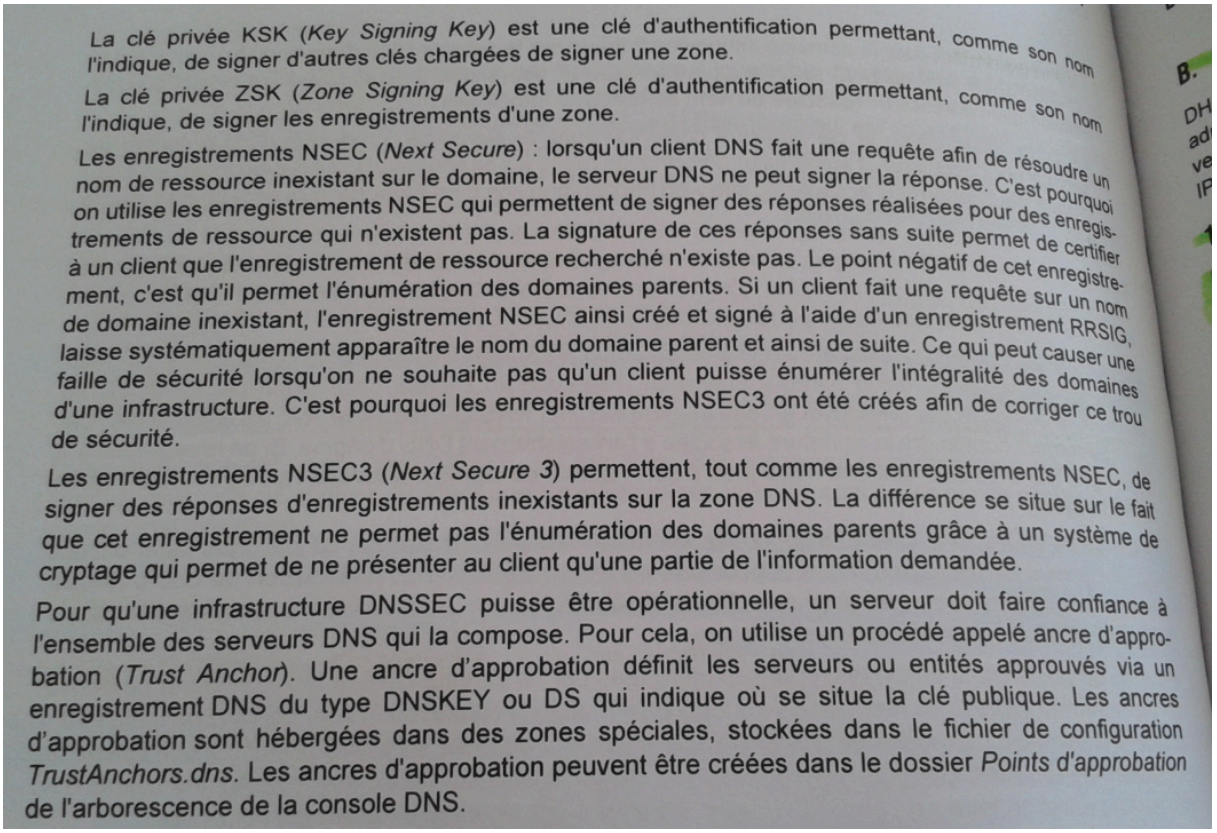
1. *Un utilisateur souhaite accéder au site web http://infonovice.fr. Le poste client émet alors une requête à destination d'un serveur DNS afin de récupérer l'adresse IP du site web.*

2. L'enregistrement pour le domaine infonovice.fr figure sur le serveur DNS dans une zone signée par DNSSEC. Le serveur DNS renvoie alors l'adresse IP demandée avec la signature numérique qui atteste que l'adresse IP associée au nom de domaine infonovice.fr est correcte.
3. Le poste client utilise la clé publique contenue dans la signature numérique et la présente au serveur pour déchiffrer et authentifier l'information reçue après comparaison avec la clé privée. L'utilisateur peut désormais accéder au site web http://infonovice.fr en étant sûr qu'il accède au bon site web.

Lorsqu'une zone DNS est signée numériquement, tous les enregistrements DNS de la zone sont automatiquement signés.
La signature d'une zone crée une clef privée sur le serveur puis stocke la clef publique dans chaque enregistrement de ressources.
Ce processus permet ainsi aux clients de vérifier une réponse reçue en comparant la clef publique avec la clef privée du serveur DNS.
Pour q'un poste client vérifie les réponses apportées par un serveur DNS, il faut configurer ce dernier en paramétrant sa table de résolution de noms (NRPT Name Resolution Policy Table). Cette table contient l'ensemble des règles de gestion qui définissent la manière dont un poste client doit valider les réponses de requêtes DNS.
La configuration de ce paramètre sur l'ensemble des postes clients d'un domaine est faisable avec une GPO.



Par défaut, lors de la signature d'une zone, le serveur DNS sur lequel l'opération est réalisée devient le maître des clefs. Ce serveur aura donc la gestion des clefs de chiffrement de la zone.



La clé privée KSK (*Key Signing Key*) est une clé d'authentification permettant, comme son nom l'indique, de signer d'autres clés chargées de signer une zone.

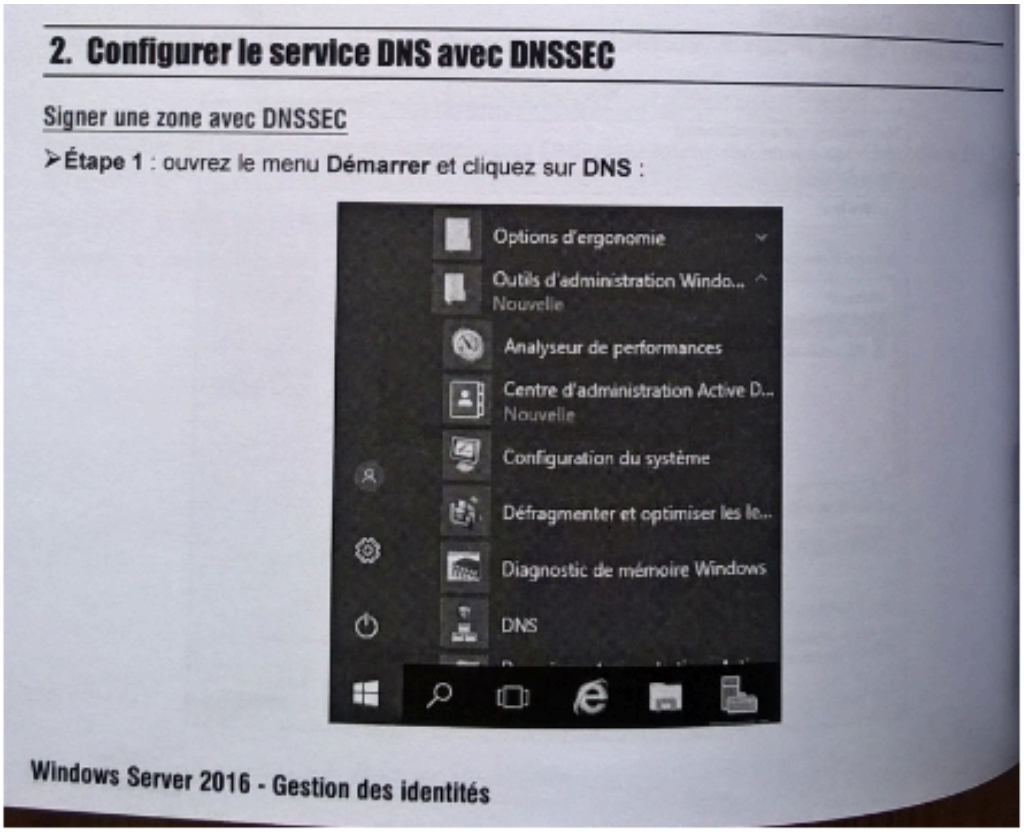
La clé privée ZSK (*Zone Signing Key*) est une clé d'authentification permettant, comme son nom l'indique, de signer les enregistrements d'une zone.

Les enregistrements NSEC (*Next Secure*) : lorsqu'un client DNS fait une requête afin de résoudre un nom de ressource inexistant sur le domaine, le serveur DNS ne peut signer la réponse. C'est pourquoi on utilise les enregistrements NSEC qui permettent de signer des réponses réalisées pour des enregistrements de ressource qui n'existent pas. La signature de ces réponses sans suite permet de certifier à un client que l'enregistrement de ressource recherché n'existe pas. Le point négatif de cet enregistrement, c'est qu'il permet l'énumération des domaines parents. Si un client fait une requête sur un nom de domaine inexistant, l'enregistrement NSEC ainsi créé et signé à l'aide d'un enregistrement RRSIG, laisse systématiquement apparaître le nom du domaine parent et ainsi de suite. Ce qui peut causer une faille de sécurité lorsqu'on ne souhaite pas qu'un client puisse énumérer l'intégralité des domaines d'une infrastructure. C'est pourquoi les enregistrements NSEC3 ont été créés afin de corriger ce trou de sécurité.

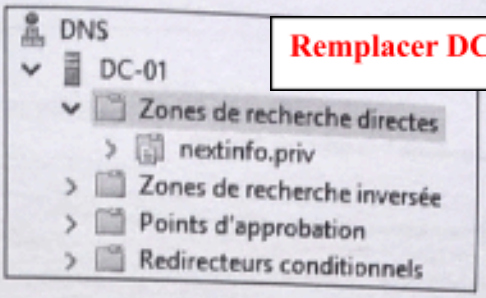
Les enregistrements NSEC3 (*Next Secure 3*) permettent, tout comme les enregistrements NSEC, de signer des réponses d'enregistrements inexistants sur la zone DNS. La différence se situe sur le fait que cet enregistrement ne permet pas l'énumération des domaines parents grâce à un système de cryptage qui permet de ne présenter au client qu'une partie de l'information demandée.

Pour qu'une infrastructure DNSSEC puisse être opérationnelle, un serveur doit faire confiance à l'ensemble des serveurs DNS qui la compose. Pour cela, on utilise un procédé appelé ancre d'approbation (*Trust Anchor*). Une ancre d'approbation définit les serveurs ou entités approuvés via un enregistrement DNS du type DNSKEY ou DS qui indique où se situe la clé publique. Les ancres d'approbation sont hébergées dans des zones spéciales, stockées dans le fichier de configuration *TrustAnchors.dns*. Les ancres d'approbation peuvent être créées dans le dossier *Points d'approbation* de l'arborescence de la console DNS.

Guide d'installation

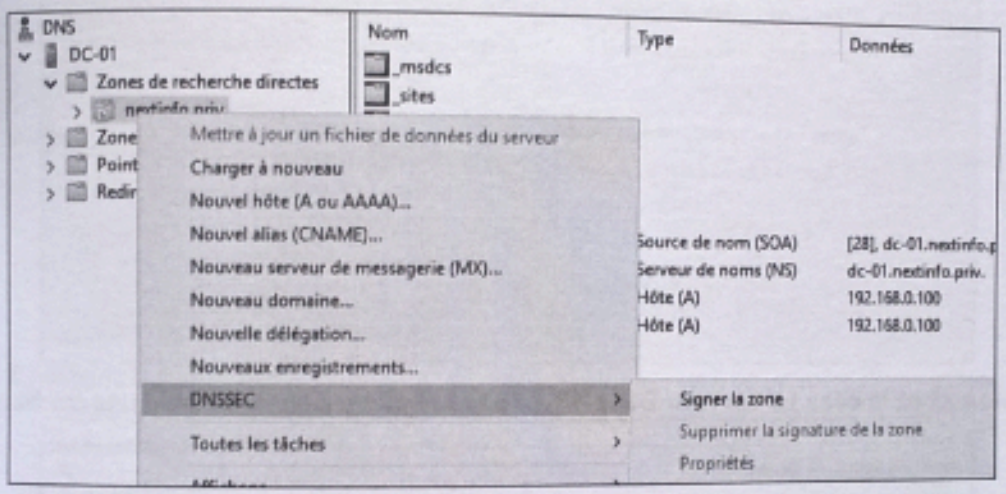

2. Configurer le service DNS avec DNSSEC
Signer une zone avec DNSSEC
Étape 1 : ouvrez le menu Démarrer et cliquez sur DNS :
Options d'ergonomie
Outils d'administration Windo...
Nouvelle
Analyseur de performances
Centre d'administration Active D...
Nouvelle
Configuration du système
Défragmenter et optimiser les le...
Diagnostic de mémoire Windows
DNS
Windows Server 2016 - Gestion des identités

➢ Étape 2 : développez l'arborescence de la console et sélectionnez la zone **nextinfo.priv** :

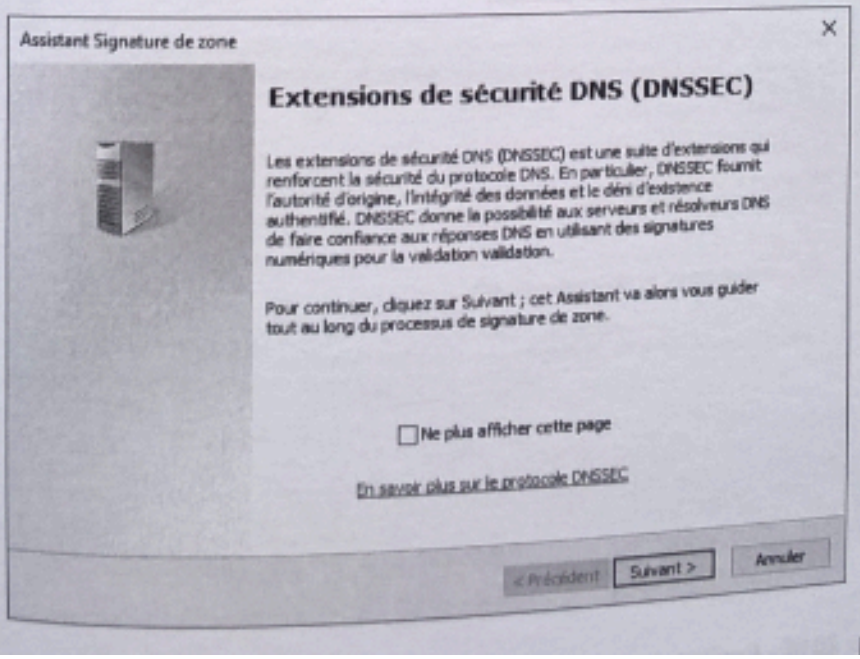


Remplacer DC-01 par srvaddns

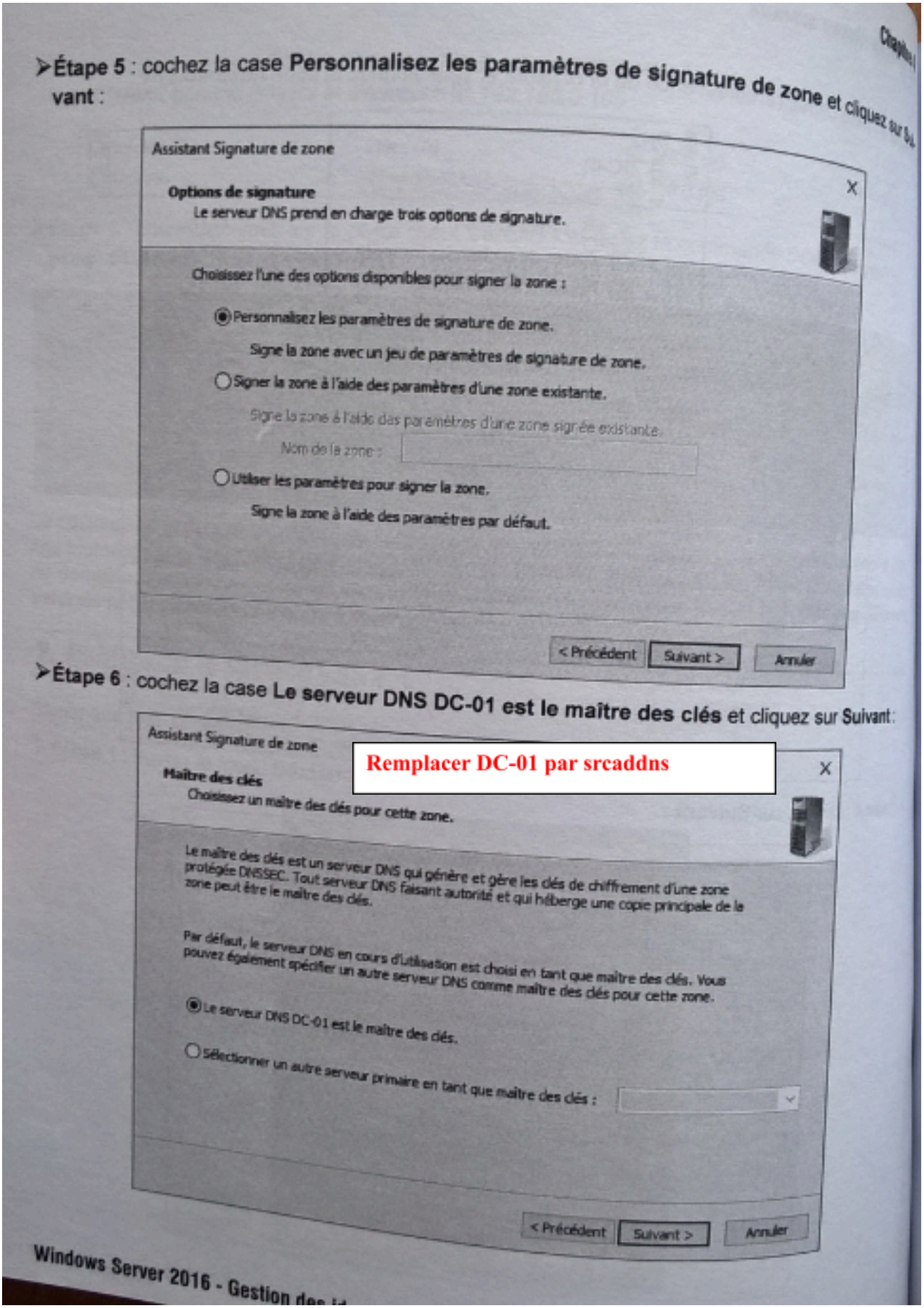
➢ Étape 3 : affichez le menu contextuel et cliquez sur **DNSSEC** puis **Signer la zone** :



➢ Étape 4 : cliquez sur **Suivant** :



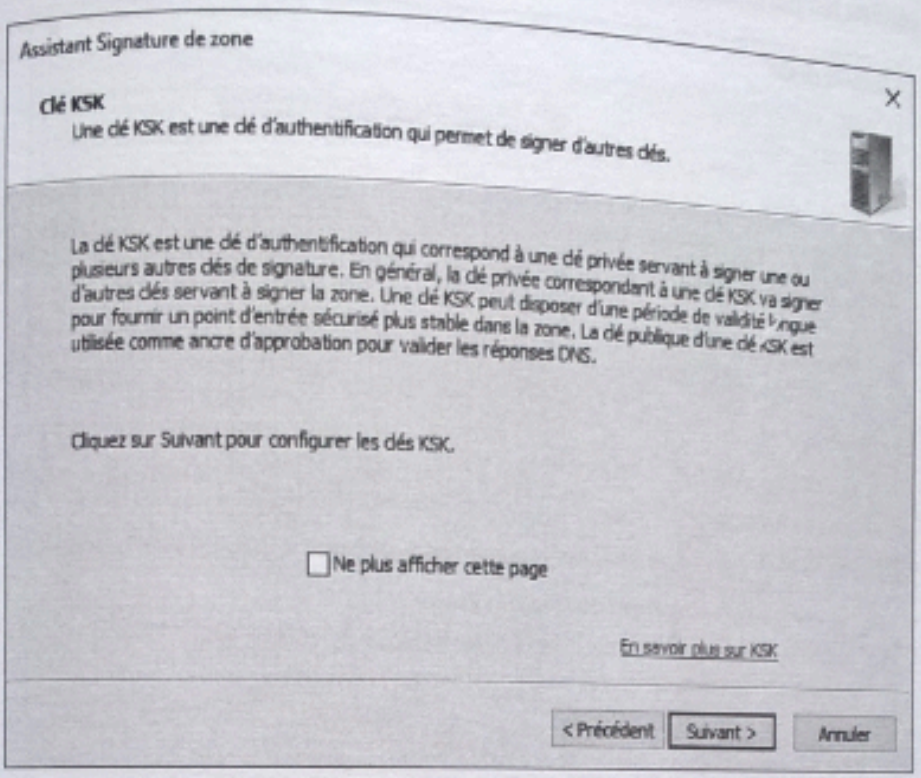
➢**Étape 5** : cochez la case **Personnalisez les paramètres de signature de zone** et cliquez sur Suivant :



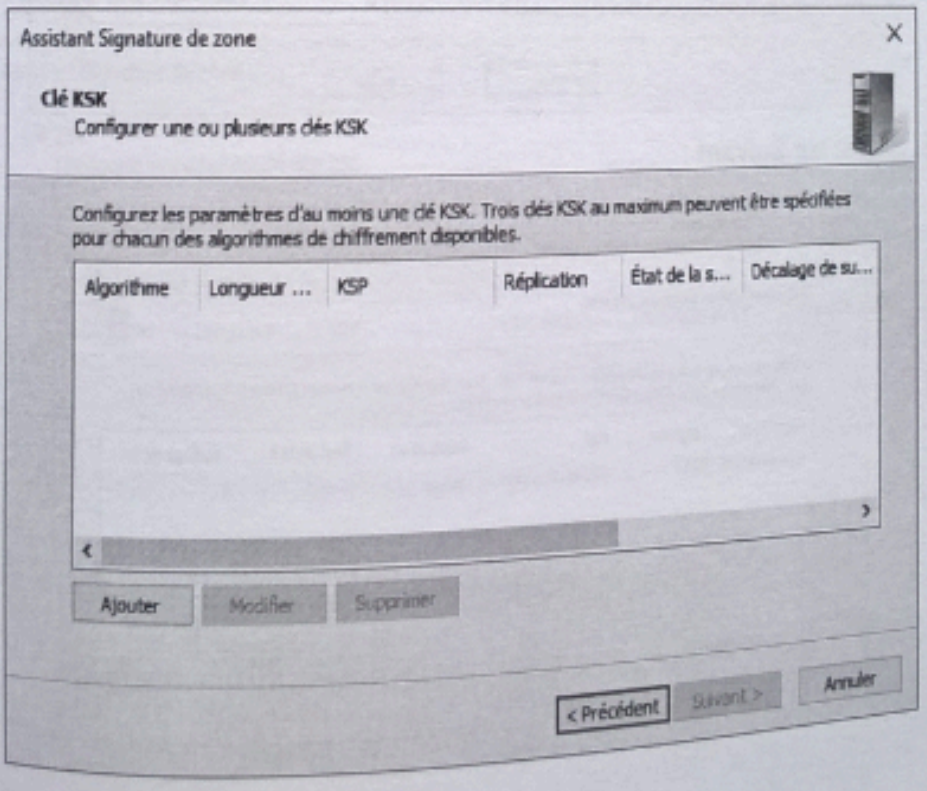
➢**Étape 6** : cochez la case **Le serveur DNS DC-01 est le maître des clés** et cliquez sur Suivant:

Windows Server 2016 - Gestion des

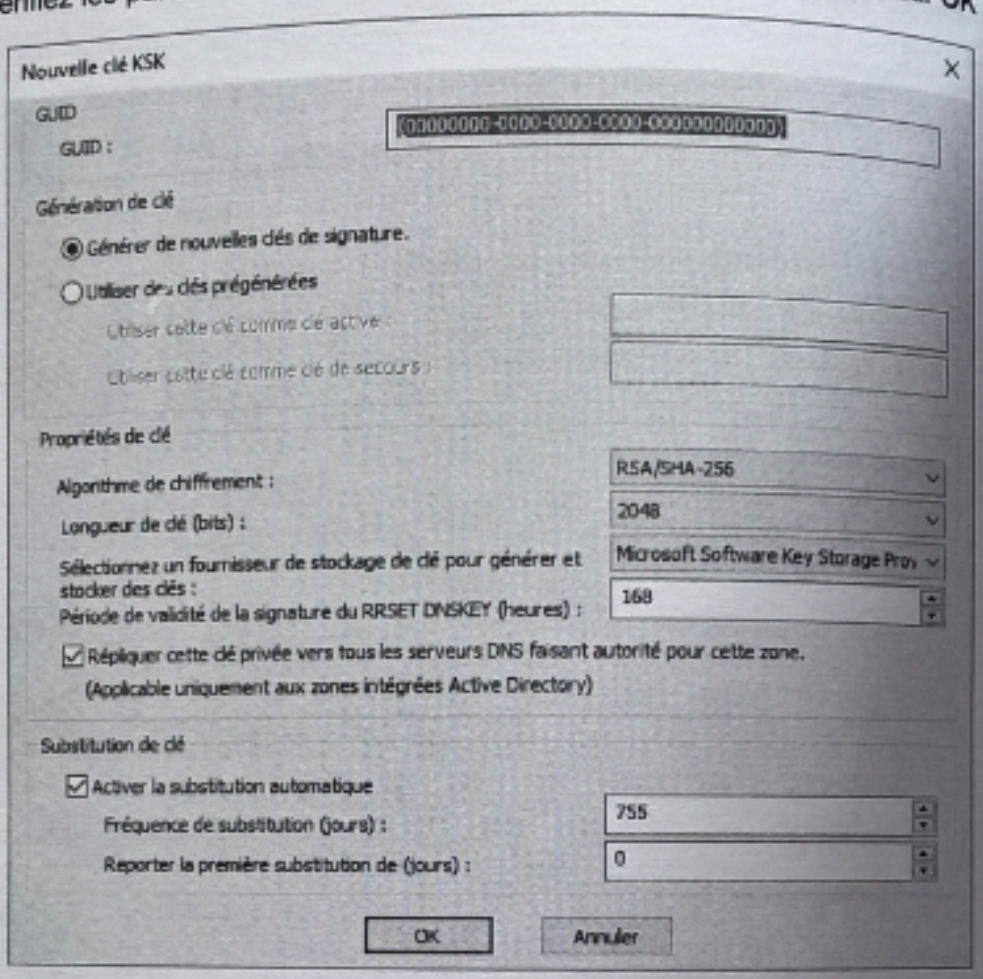
➢Étape 7 : cliquez sur **Suivant** :



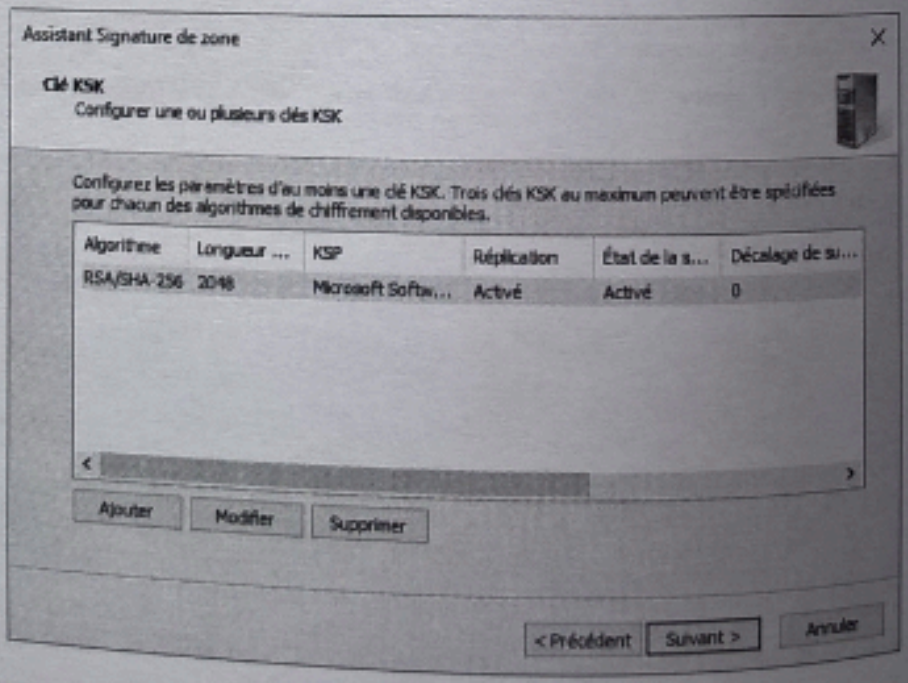
➢Étape 8 : cliquez sur **Ajouter** :



➢**Étape 9** : vérifiez les paramètres de la clé d'authentification (KSK) puis cliquez sur **OK** :

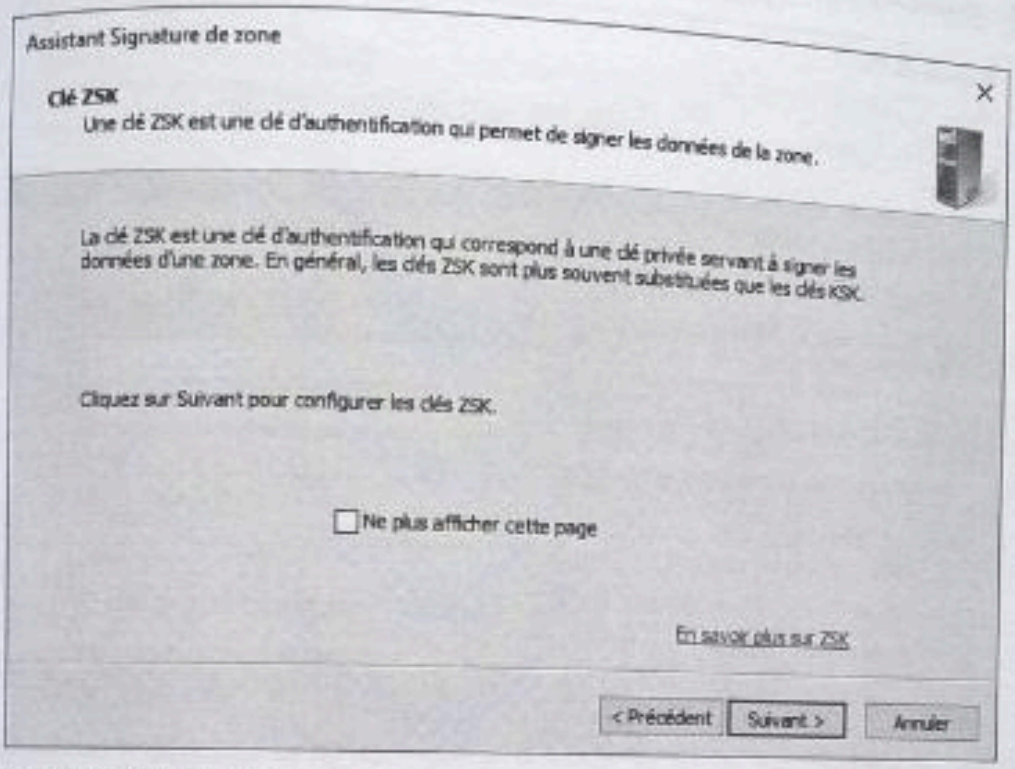


➢**Étape 10** : cliquez sur **Suivant** :

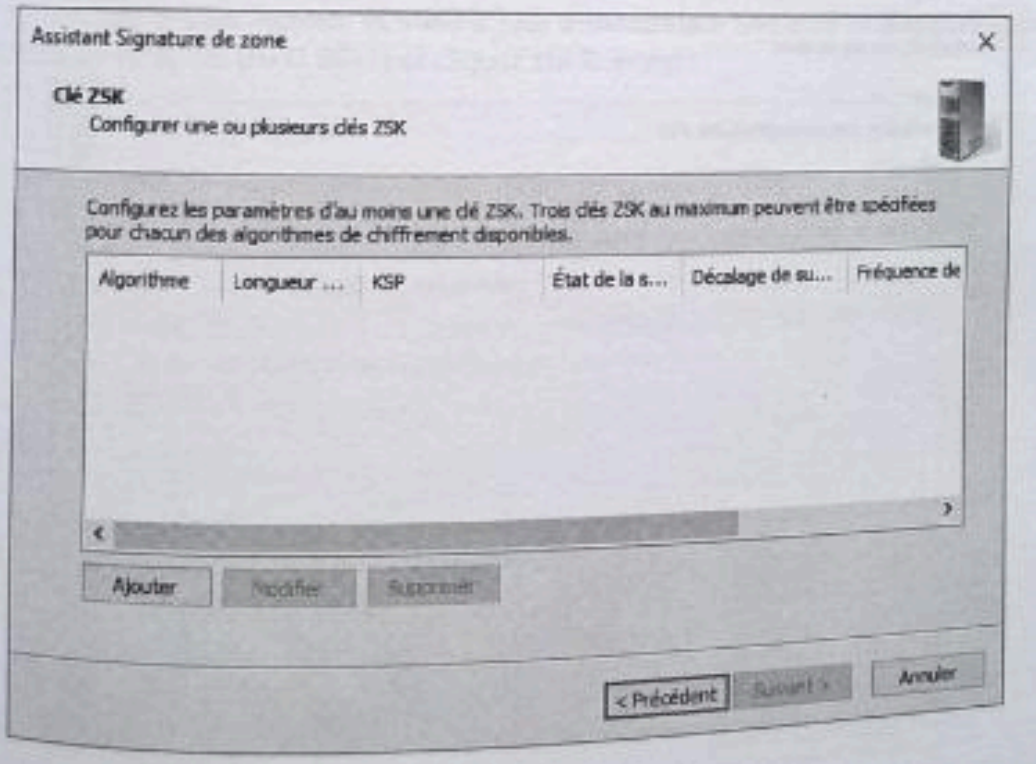


Windows Server 2016

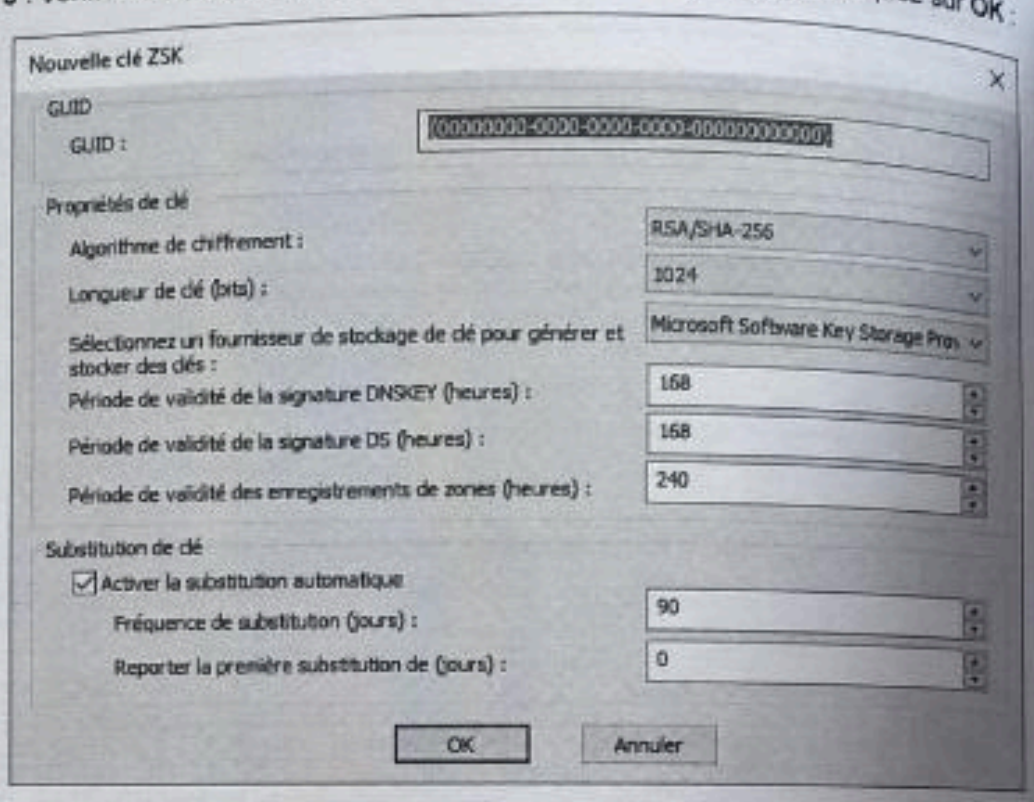
➢Étape 11 : cliquez sur **Suivant** :



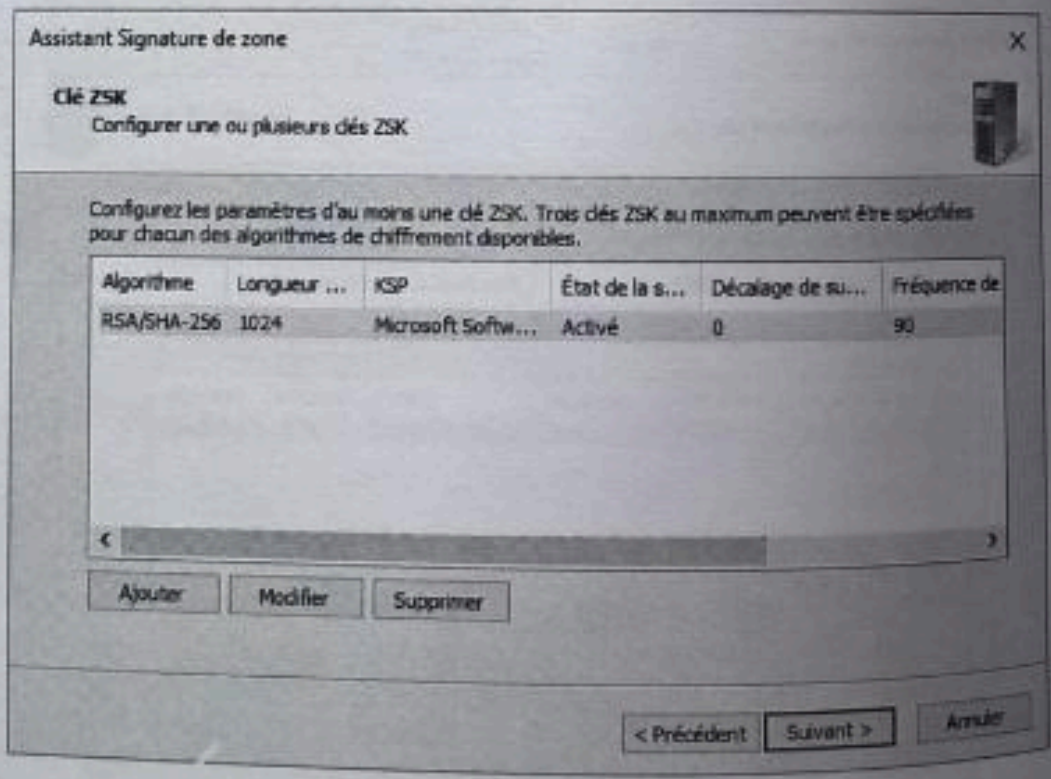
➢Étape 12 : cliquez sur **Ajouter** :



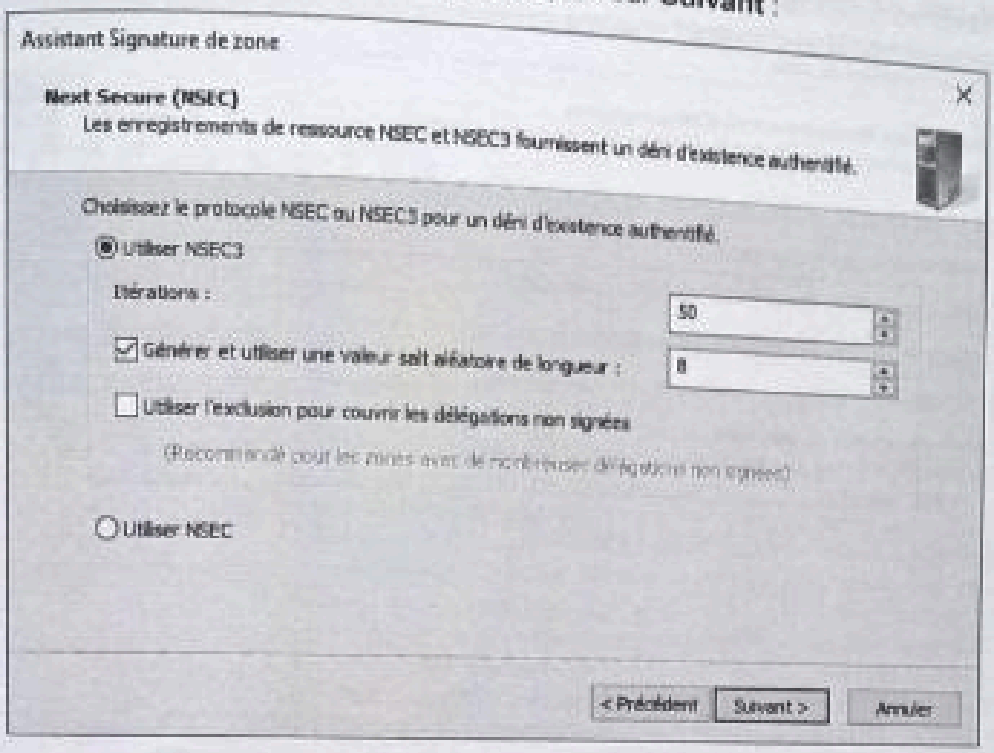
➢ **Étape 13** : vérifiez les paramètres de la clé d'authentification (ZSK) puis cliquez sur **OK** :



➢ **Étape 14** : cliquez sur **Suivant** :

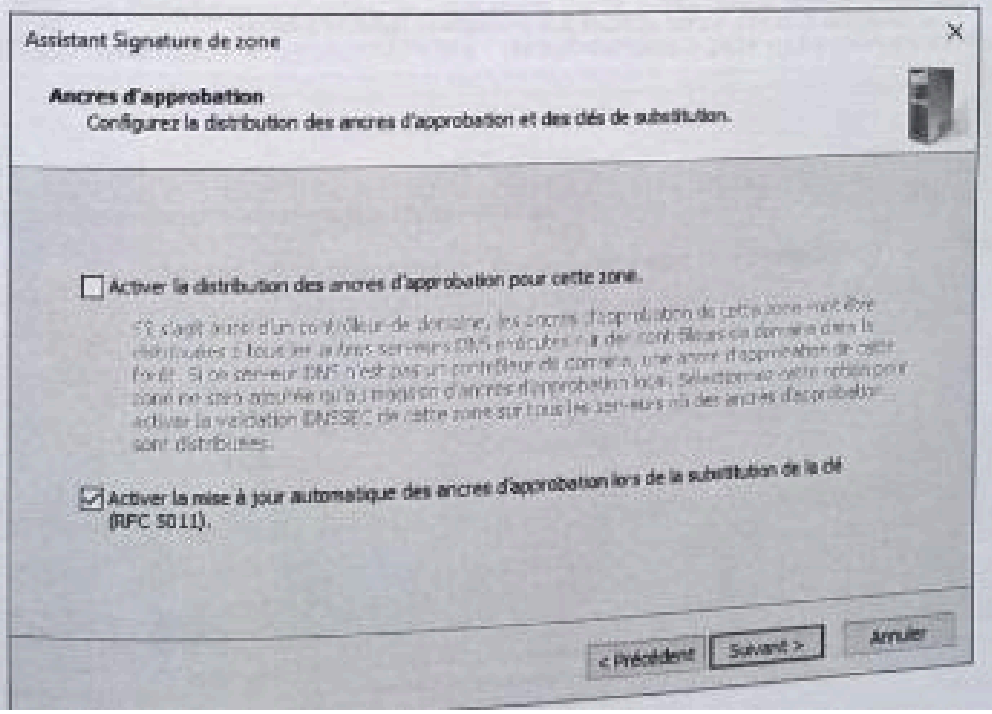


➢ **Étape 15** : cochez la case **Utiliser NSEC3** puis cliquez sur **Suivant** :

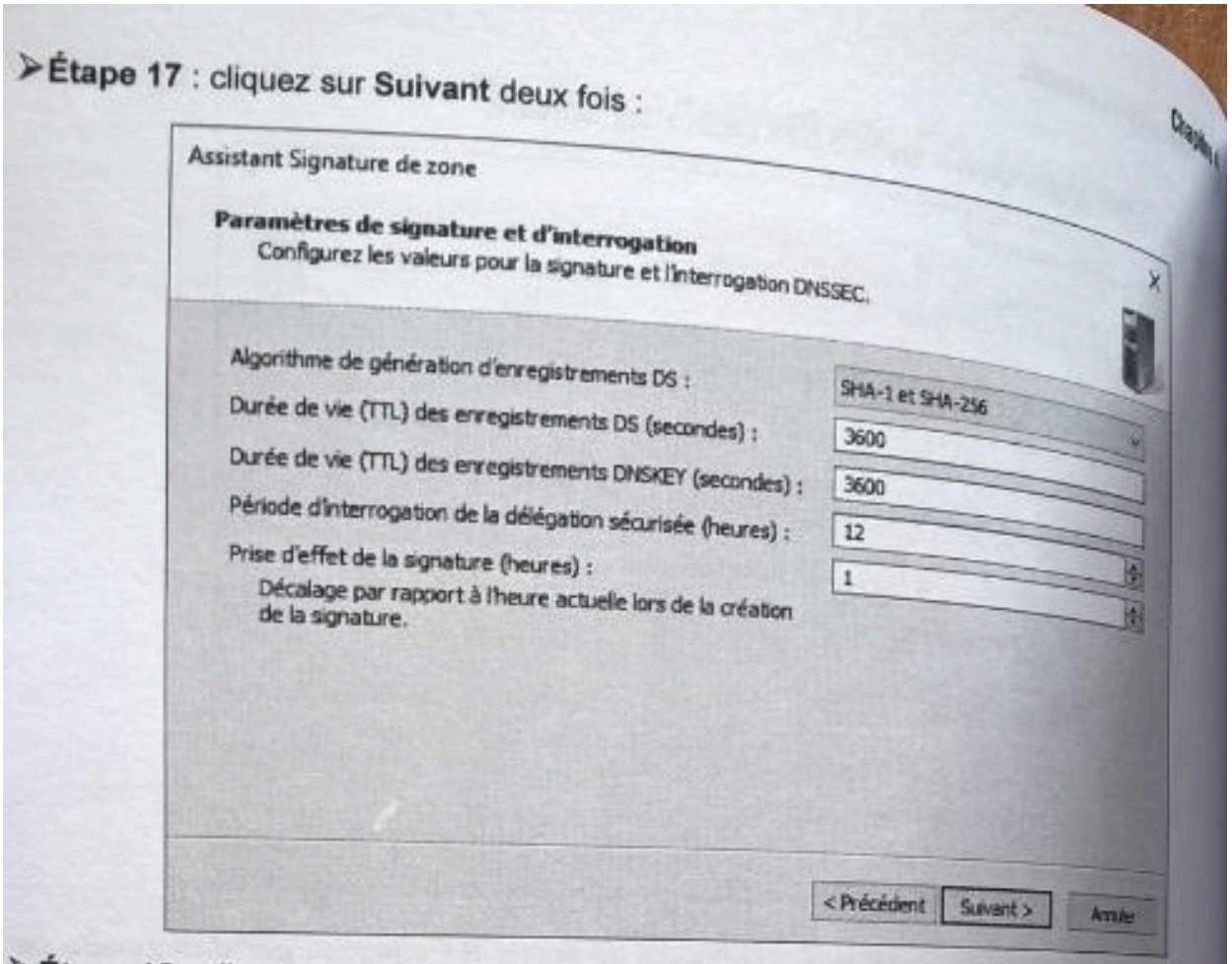


☞ *Les paramètres d'itérations et de sel (salt) permettent de limiter les attaques par dictionnaire ou brute-force dans le but de décrypter le chiffrement.*

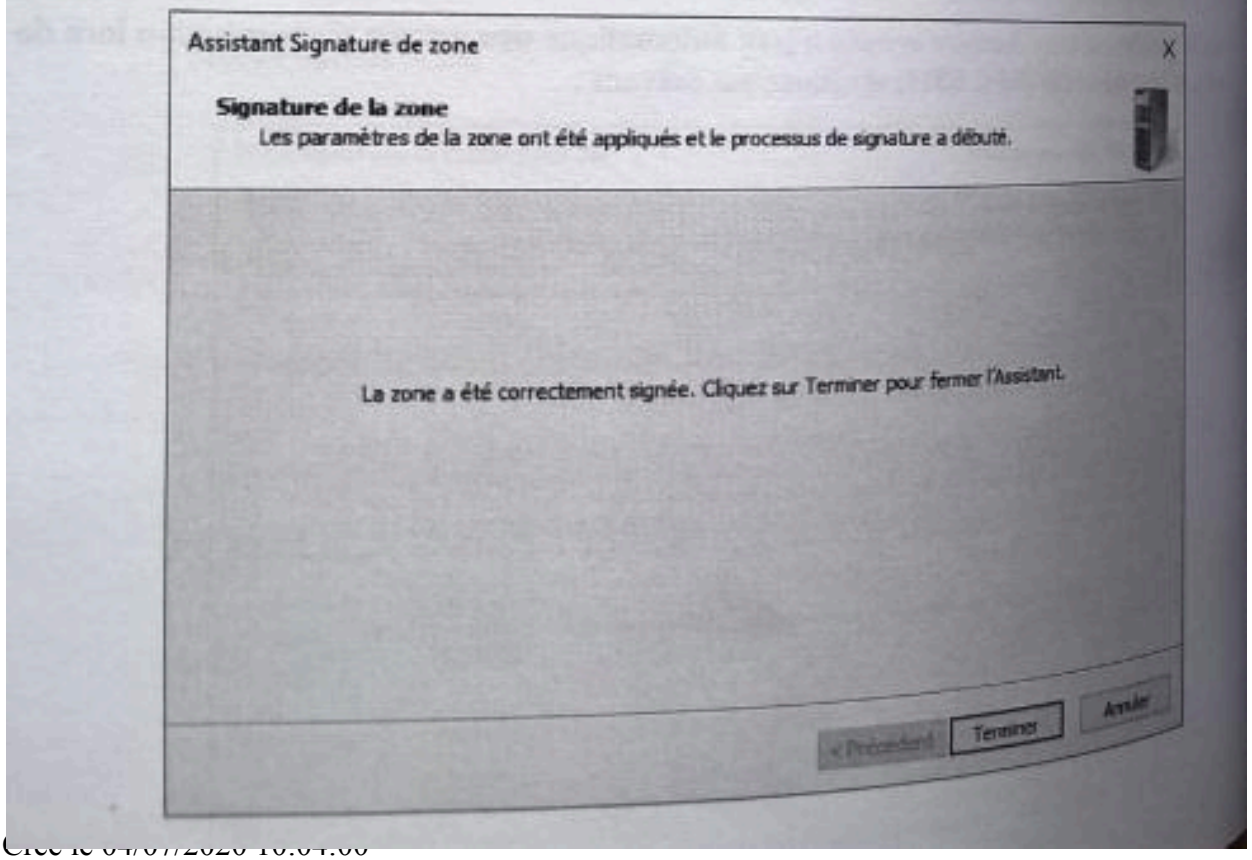
➢ **Étape 16** : cochez la case **Activer la mise à jour automatique des ancres d'approbation lors de la substitution de la clé (RFC 5011)** et cliquez sur **Suivant** :



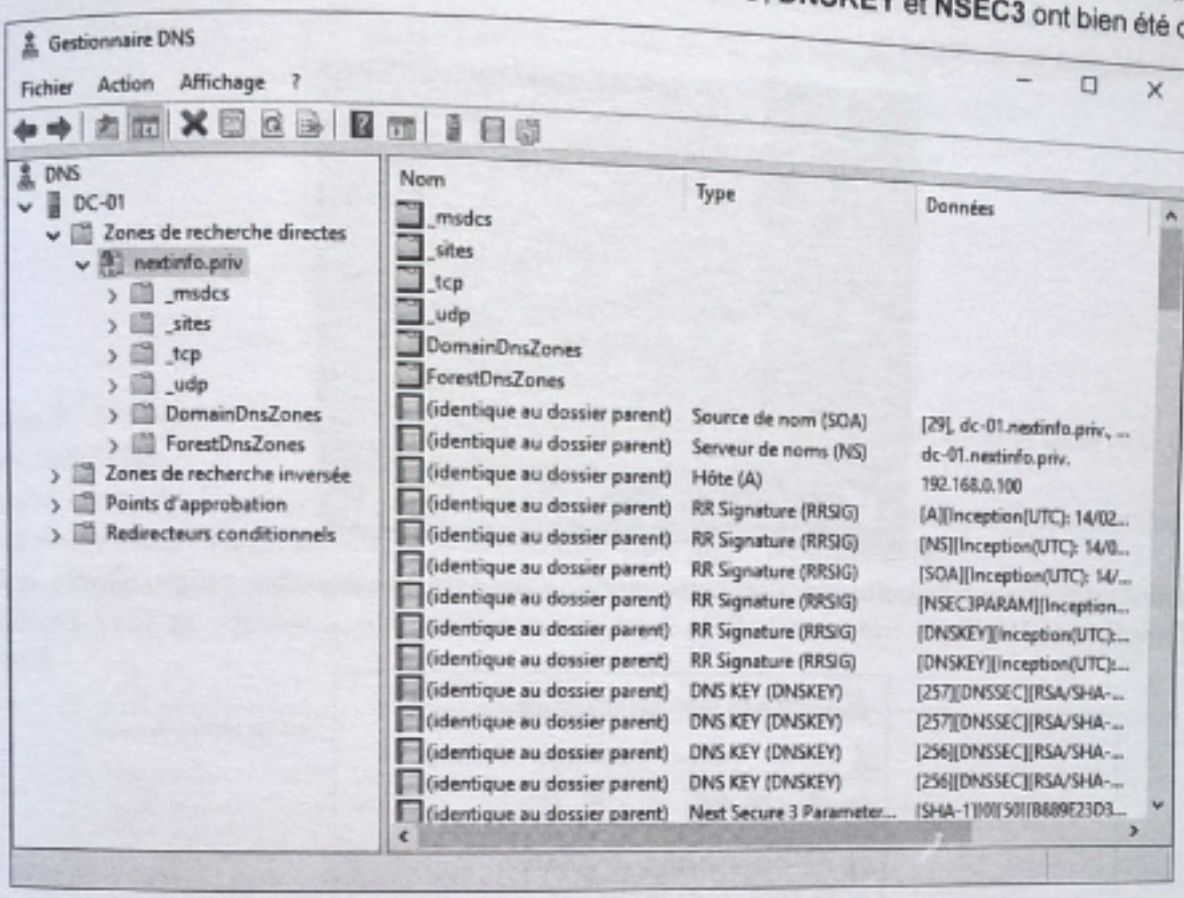
➢ **Étape 17** : cliquez sur **Suivant** deux fois :



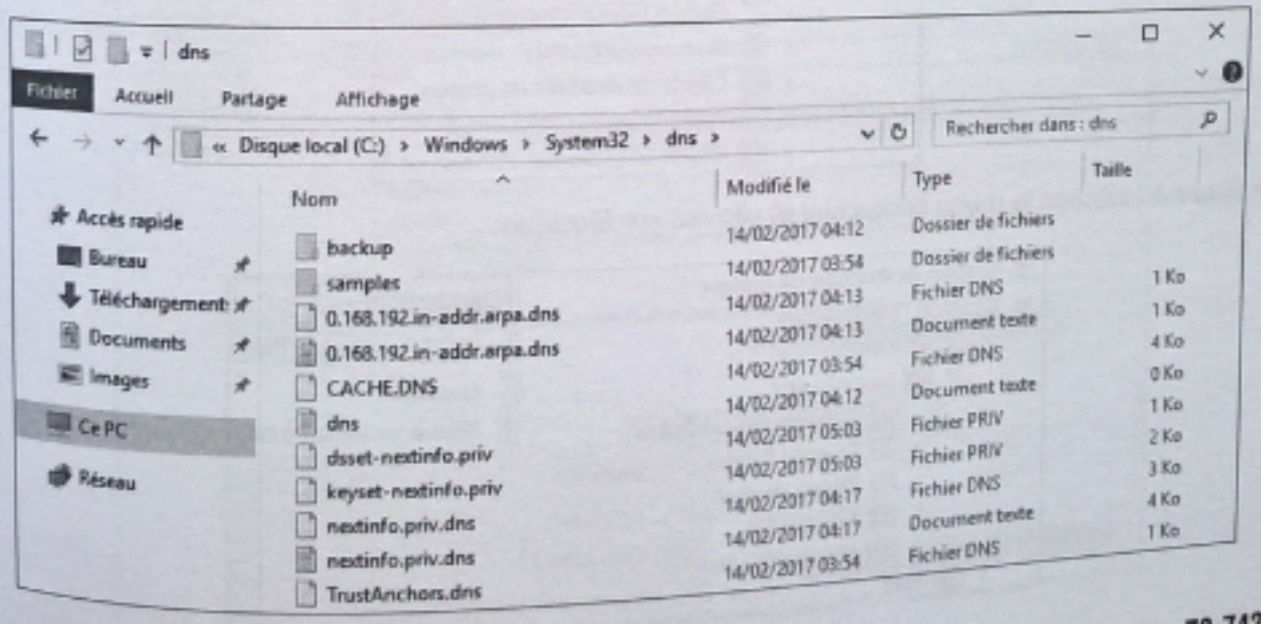
➢ **Étape 18** : cliquez sur **Terminer** :



➢ **Étape 19** : vérifiez que la zone sélectionnée porte bien un petit logo en forme de cadenas indiquant que la zone est signée, puis que les enregistrements **RRSIG**, **DNSKEY** et **NSEC3** ont bien été créés :



➢ **Étape 20** : on peut constater qu'après la signature de la zone, deux fichiers ont été créés dans le répertoire **%SYSTEMROOT%\System32\dns** : **dsset-nextinfo.priv** et **keyset-nextinfo.priv**.

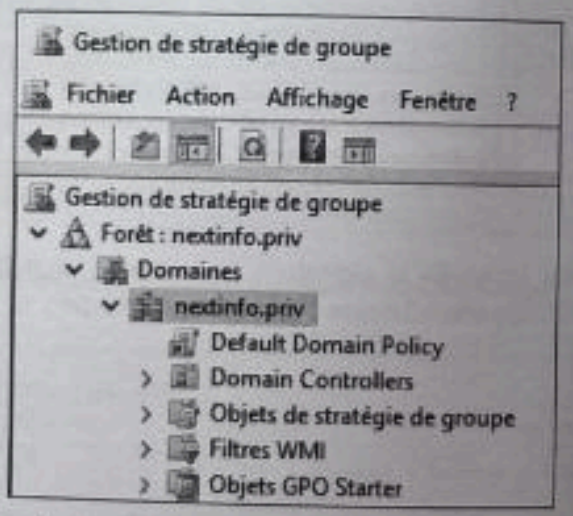


Configurer la table NRPT des clients DNS

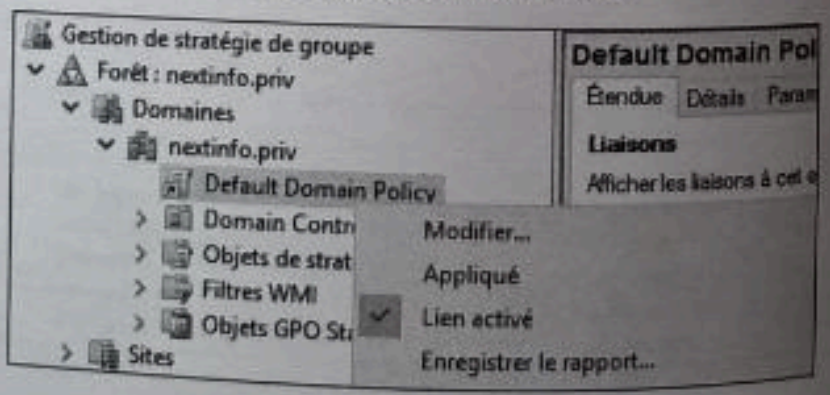
➢ **Étape 1** : dans le menu **Démarrer** de Microsoft Windows Server 2016, cliquez sur l'icône Gestion des stratégies de groupes :

➢ **Étape 2** : développez l'arborescence et sélectionnez l'objet de stratégie de groupe (GPO) nommé **Default Domain Policy** :

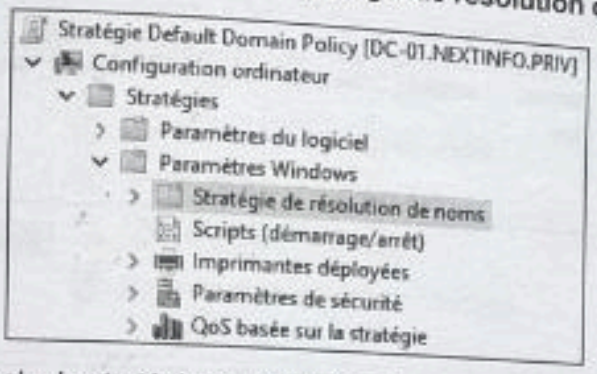
Remplacer nextinfo.priv par webcourses.sio



➢ **Étape 3** : affichez le menu contextuel et cliquez sur **Modifier...** :

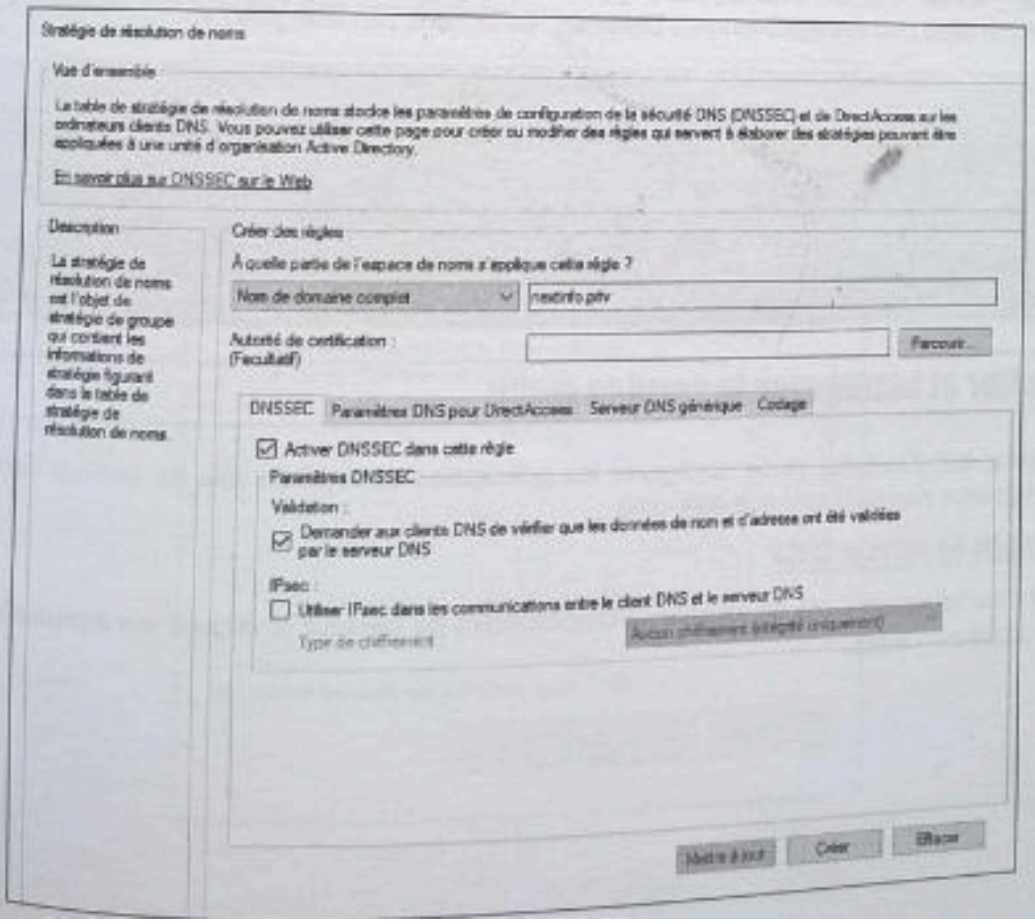


➢ **Étape 4** : développez l'arborescence de la console et sélectionnez le nœud suivant : **Configuration ordinateur\Stratégies\Paramètres Windows\Stratégie de résolution de noms** :

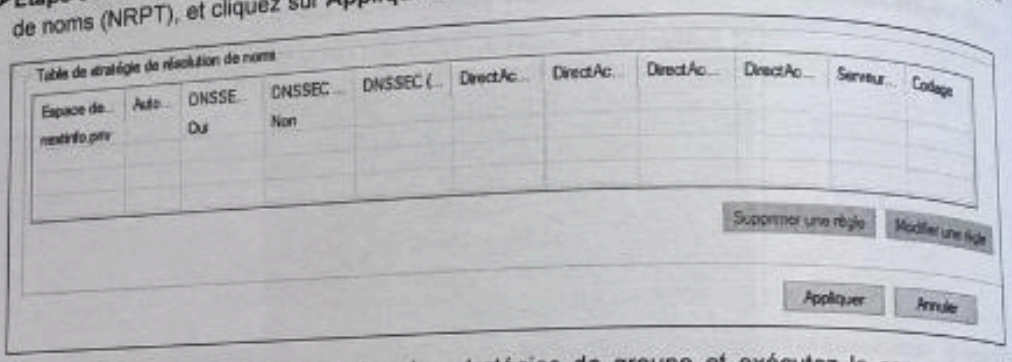


➢ **Étape 5** : remplissez la règle de stratégie de résolution de noms afin d'alimenter la table NRPT et cliquez sur **Créer** :

- Dans le champ **À quelle partie de l'espace de noms s'applique cette règle ?**, sélectionnez **Nom de domaine complet** dans la liste déroulante, puis tapez **nextinfo.priv**.
- Dans l'onglet **DNSSEC**, cochez les cases **Activer DNSSEC dans cette règle** et **Demander aux clients DNS de vérifier que les données de nom et d'adresse ont été validées par le serveur DNS**.



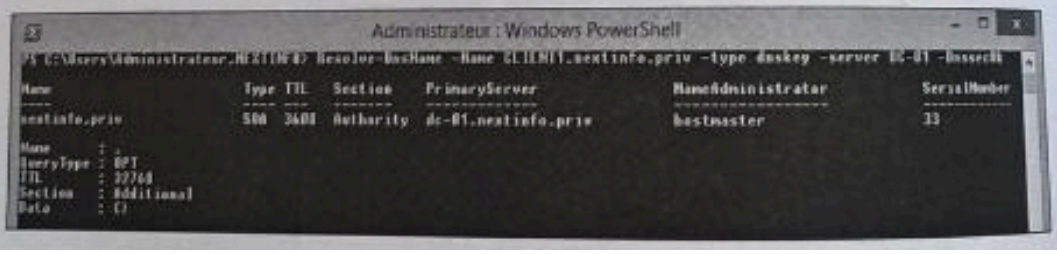
➢ **Étape 6** : vérifiez que la règle créée précédemment figure bien dans la table de stratégie de résolution de noms (NRPT), et cliquez sur **Appliquer** :



➢ **Étape 7** : fermez l'éditeur de gestion des stratégies de groupe et exécutez la commande DOS `gpupdate /force`.

➢ **Étape 8** : connectez-vous sur le poste **CLIENT1**, ouvrez une fenêtre DOS et exécutez la commande `gpupdate /force`. Cette opération a pour but d'actualiser les stratégies de sécurité du domaine.

➢ **Étape 9** : toujours sur **CLIENT1**, ouvrez une fenêtre PowerShell et tapez la commande `Resolve-dnsname -name CLIENT1.nextinfo.priv -type dnskey -server DC-01 -dnssecok`. On interroge ainsi des enregistrements DNSSEC de la zone *nextinfo.priv*.



Mission 13 Documenter DNSSEC

Compétences	Reprendre toutes les compétences relatives aux différentes missions
Objectifs	Documenter DNSEC
Vocabulaire à connaître	
Évaluation	Compte-rendu à rendre pour évaluation sommative coefficient 2 Compte-rendu est à poser dans votre PFC Épreuve E4 certificative

Page de garde

1. **L'entête de chaque page doit contenir les informations suivantes :**
   29. Nom de l'établissement
   30. Titre complet de l'activité
   31. La version du document

2. **Le pied de chaque page doit contenir les informations suivantes :**
   32. L'auteur / les auteurs
   33. Numéro de page
   34. Date

3. **Au centre de la page**
   35. Donner l'objectif principal de l'activité

Sommaire ou table des matières

4. **Automatiser** votre sommaire

Introduction

5. **Présenter**
   5.1. le contexte sur lequel vous travaillez (Description de la ligue de marathon)
   5.2. Description de son logo (celui que vous avez choisi sur votre site) représentation, symbole, lien Internet si vous l'avez récupéré sur une bibliothèque d'images

Déroulé de la mission 11

6. **Donner** le schéma réseau global associé au contexte de la mission 11
7. **Préciser** les contraintes liées aux Prérequis si nécessaires
8. **Notifier** les points de vigilance de la mission
9. **Expliquer** les points de blocage et les solutions apportées
10. **Montrer** à l'aide d'une copie écran les résultats obtenus après les mises en place des missions

Analyse de l'activité

13. **Spécifier** les difficultés rencontrées au cours des différentes phases de mise en place
14. **Mentionner** les apports professionnels acquis à travers cette expérience
15. **Préciser** les apports personnels acquis à travers cette expérience