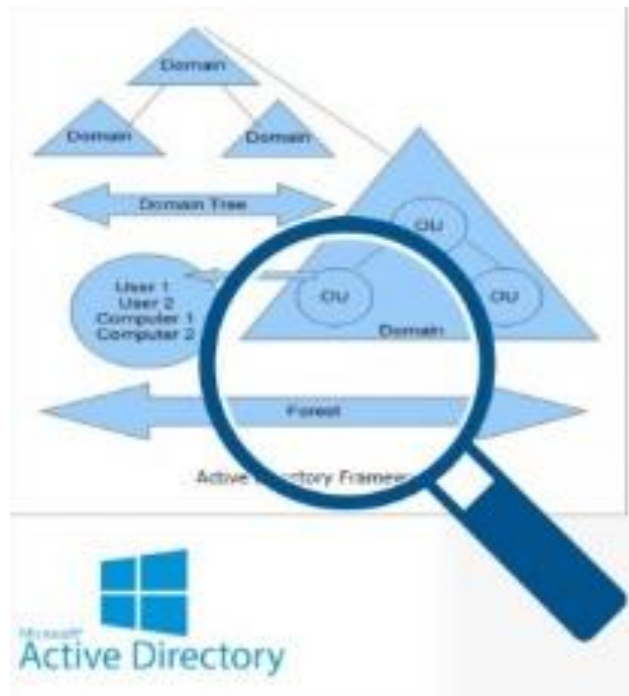


---

# PROJET ANNUAIRE ET SUPERVISION

---



Réalisé par :

- HAMADOU Ousman
- MANFOUO Fredy
- SEUNGTO Stephane
- TAMANDJOU Kassandra

Sous la supervision de :  
M. Tanguy KUATE

---

# RAPPORT TECHNIQUE

---

## Table des matières

Sous la supervision de : .....	0
Résumé .....	2
Abstract.....	3
I. Présentation du projet .....	4
1. Contexte .....	4
2. Objectifs et finalités du projet .....	4
3. Cahier de charge .....	4
4. Durée du projet .....	5
5. Ressources .....	5
II. Mise en place de l'architecture d'annuaire .....	6
1. Installation des services ADDS, DHCP et DNS sur Windows Server .....	6
2. Promotion du serveur en contrôleur de domaine .....	11
3. Configuration du DHCP.....	15
4. Configuration du DNS .....	16
5. Création des « Organisation Units », des groupes et des utilisateurs .....	28
6. Ajouter un utilisateur dans un domaine .....	30
7. Création des GPO « Stratégie de groupes » .....	30
8. Supervision.....	35
9. Création de la Relation d'approbation .....	44
10. Installation et configuration de ISEC Groupe Réplica » .....	44
III. Justification des choix techniques .....	44
1. Choix des outils de supervision .....	45
2. Choix de l'hyperviseur .....	47
IV. Conclusion.....	48

---

# RAPPORT TECHNIQUE

---

## Résumé

Dans le but de former des ingénieurs informatiques dignes de ce nom, l'institut UCAC-ICAM confronte ses étudiants aux situations réelles des entreprises. Le présent rapport présente un ensemble de procédures conduisant à la réalisation du projet et à l'exécution des différents points du cahier de charge fourni du projet **ANNUAIRE ET SUPERVISION**.

Le projet en question réalisé du Jeudi 22 au Mercredi 27 Octobre 202 portait sur les problèmes que rencontrait le groupe ISEC plus précisément sur la mise en œuvre d'une architecture Active Directory de la maison mère et de la filiale Telecom, sur l'installation de nouveaux clients Windows dans le cadre d'améliorer ses services et enfin de mettre en place un logiciel de supervision pour surveiller la charge des serveurs de la filiale Télécom.

---

# RAPPORT TECHNIQUE

---

## Abstract

---

# RAPPORT TECHNIQUE

---

## I. Présentation du projet

### 1. Contexte

Après avoir évolué dans divers secteurs depuis fort longtemps, le **Groupe ISEC** s'est récemment fait intéresser aux Télécoms avec le rachat d'une toute jeune entreprise prometteuse dans ce secteur d'où ressort le besoin d'interconnecter la maison mère du **Groupe ISEC** à la nouvelle filiale de ce dernier, mettre en œuvre l'architecture Active Directory de la maison mère et celle de la filiale télécom est le travail qui nous a été confié en tant que Ingénieur en informatique sans oublier la supervision afin de surveiller la charge des serveurs de la filiale télécom.

### 2. Objectifs et finalités du projet

L'objectif de ce projet tourne sur l'application d'un moyen pour assurer la gestion des ressources administratives transitant de façon unidirectionnelle entre la maison mère du Groupe ISEC et la filiale Télécom via une architecture Active Directory ainsi qu'un ensemble de technique de suivi, qui permettra de surveiller, analyser, rapporter et d'alerter les fonctionnements anormaux des systèmes informatiques de façon à assurer la plus grande cohérence possible entre les systèmes informatiques et les composants physiques.

### 3. Cahier de charge

Dans le cahier de charge de ce projet, il nous a été demandé de :

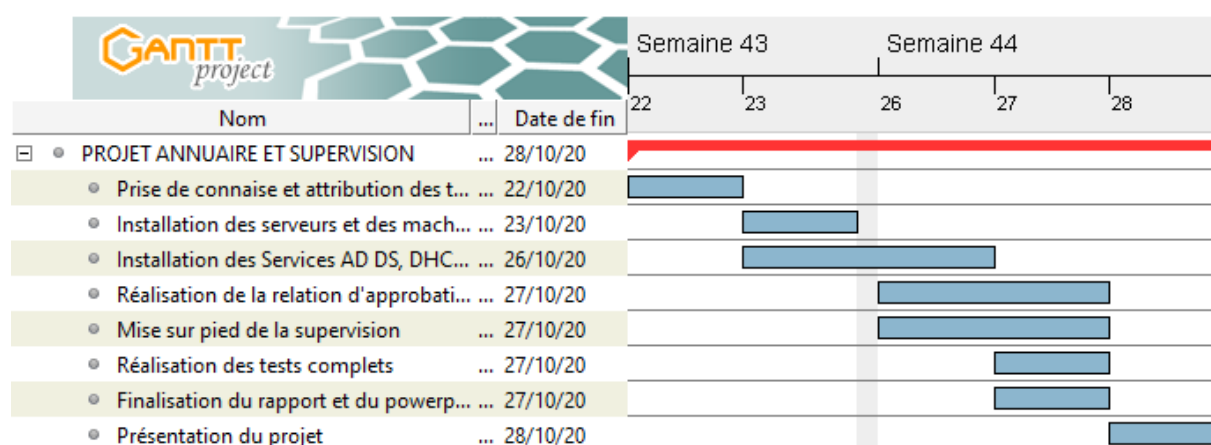
- ❖ Justification de l'organigramme choisi pour l'ordonnancement des utilisateurs.
- ❖ Création des répertoires partagés qui se trouvera sur le contrôleur de domaine principal.
- ❖ Il figurera comme lecteur réseau dans le poste de travail de l'utilisateur et portera la lettre S: comme **Share**. Ce répertoire, propre à chaque service ne sera pas lisible par les autres
- ❖ services (sauf la direction)
- ❖ Création des répertoires communs respectivement pour le groupe et la filiale.
- ❖ Création des répertoires personnels. Il s'agira d'une redirection du dossier Documents.
- ❖ Création des imprimantes réseaux et communes à l'ensemble des utilisateurs.
- ❖ Création des fonds d'écran propre à chaque service.
- ❖ Création des mots de passe.
- ❖ Désactivation de l'exécution automatique des périphériques amovibles.

# RAPPORT TECHNIQUE

- ❖ Configuration du logiciel de compression/décompression 7Zip pour tous les utilisateurs.
- ❖ Mise sur pieds d'une relation d'approbation unidirectionnelle.

## 4. Durée du projet

Ce projet a été réalisé sur 4 jours allant du 22 Octobre au 27 Octobre 2020.



## 5. Ressources

### a) Ressources Humaines

Les acteurs de ce projet figurent dans le tableau ci-dessous :

Noms	Prénoms
HAMADOU	Ousman Bagoudou
MANFOUO	Fredy
SEUNGTO	Stephane
TAMANDJOU	Kassandra

### b) Ressources Matérielles et Logicielles

Lors de la réalisation de ce projet, nous avons besoin de certains logiciels et matériels :

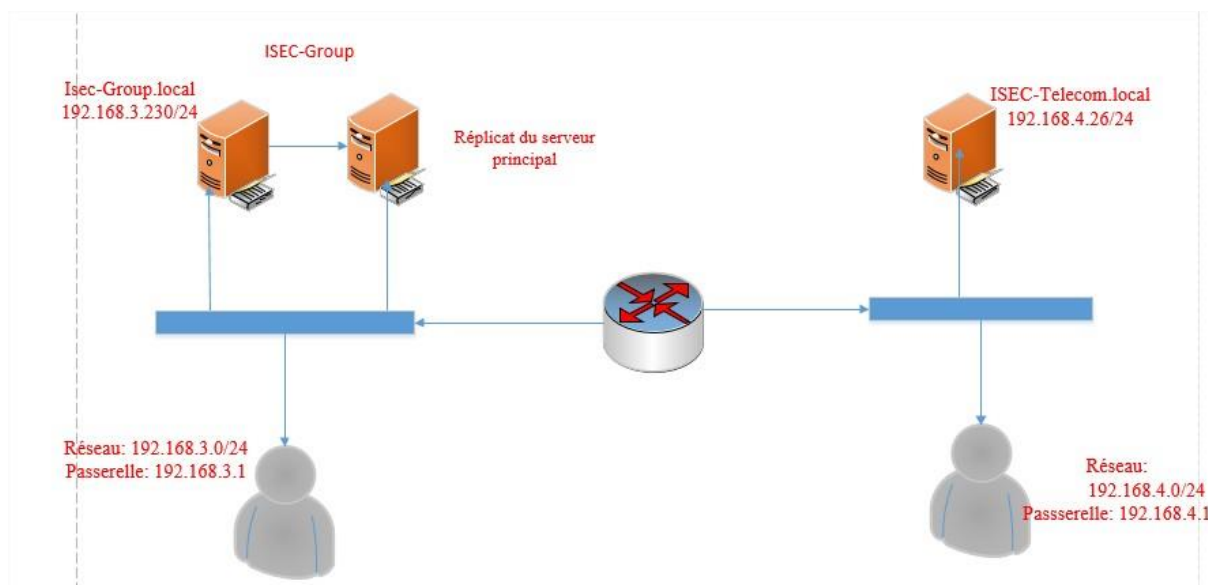
Désignations	Quantités
Windows Server 2016	3
Windows 2016	2
Ordinateurs portables	2

# RAPPORT TECHNIQUE

## II. Mise en place de l'architecture d'annuaire

Avant toute chose, il est impératif d'installer notre hyperviseur (dans notre cas, il s'agit de Virtual Box) pour faire fonctionner sur une machine hôte plusieurs systèmes d'exploitation indépendants les uns des autres comme des machines physiques.

Ci-dessous l'architecture qui a été déployée :



### 1. Installation des services ADDS, DHCP et DNS sur Windows Server

Avant toutes configurations sur les serveurs, il est important de configurer leur carte réseau de la façon suivante :

- ❖ Ouvrir « *Centre de réseau et partage* »
- ❖ Cliquer sur « *Modifier les paramètres de la carte* »
- ❖ Aller dans les propriétés et choisir « *Protocol Internet Version 4* »
- ❖ Insérer une adresse IP et son masque de sous réseau

# RAPPORT TECHNIQUE

- ❖ Une passerelle par défaut et l'adresse IP du DNS

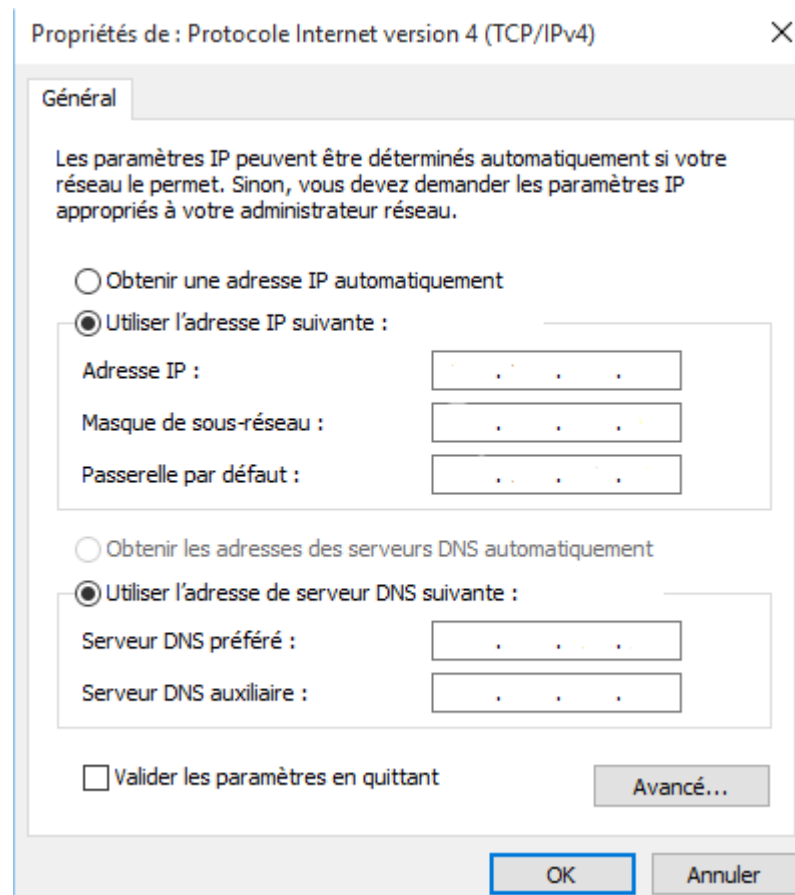
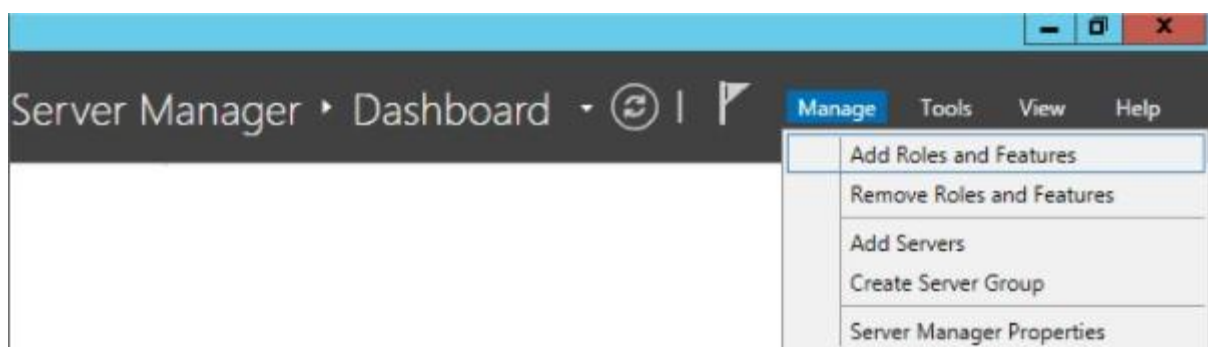


Figure 1: Configuration carte réseau

Pour l'installation des services, il faut ajouter ses rôles au serveur.

- ❖ Après avoir ouvert l'application « *Gestionnaire de serveur* »
- ❖ Accéder au menu « *Gérer* »
- ❖ Cliquez sur « *Ajouter des rôles et des fonctionnalités* ».



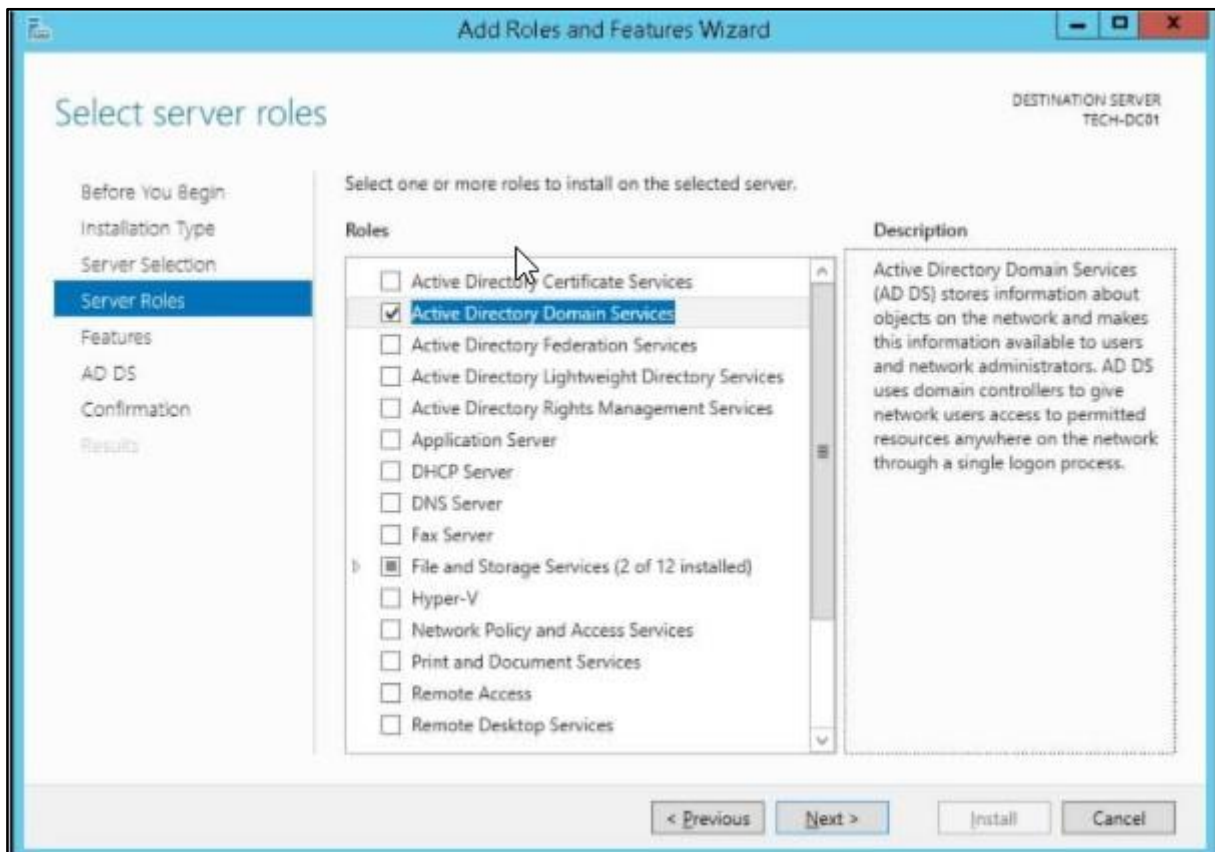


---

# RAPPORT TECHNIQUE

---

- ❖ Accédez à la fenêtre « **Rôle du serveur** », sélectionnez les services de **domaine Active Directory, DHCP, DNS et Service d'impression**.

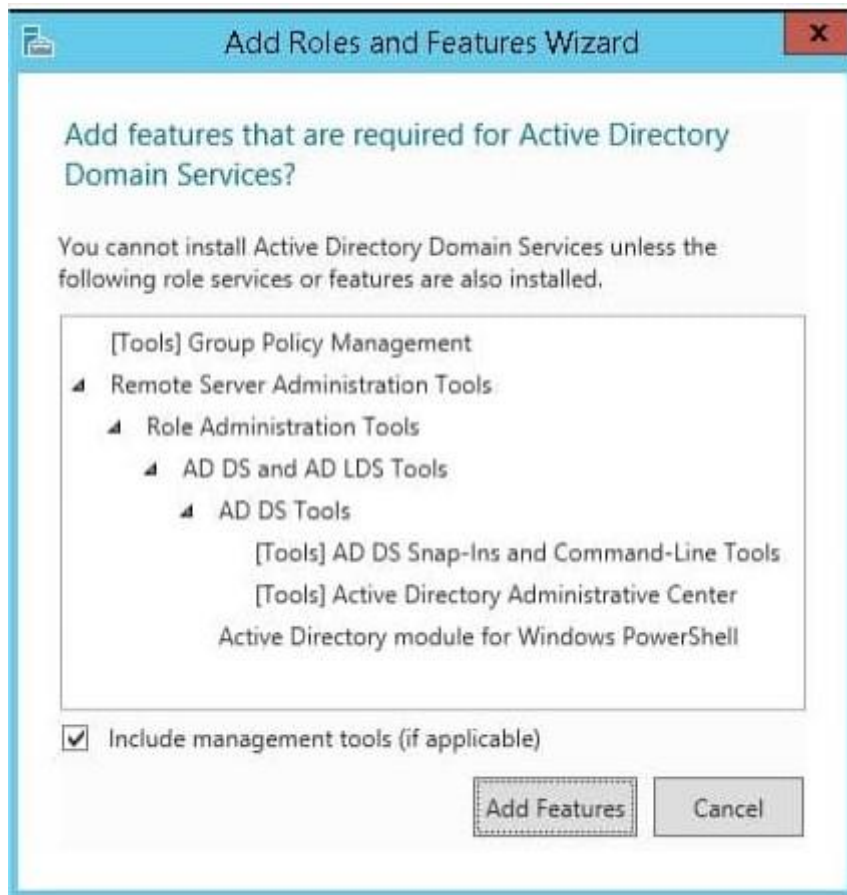


Sur la fenêtre qui s'affichera, cliquez sur le bouton « **Ajouter des fonctionnalités** ».

---

# RAPPORT TECHNIQUE

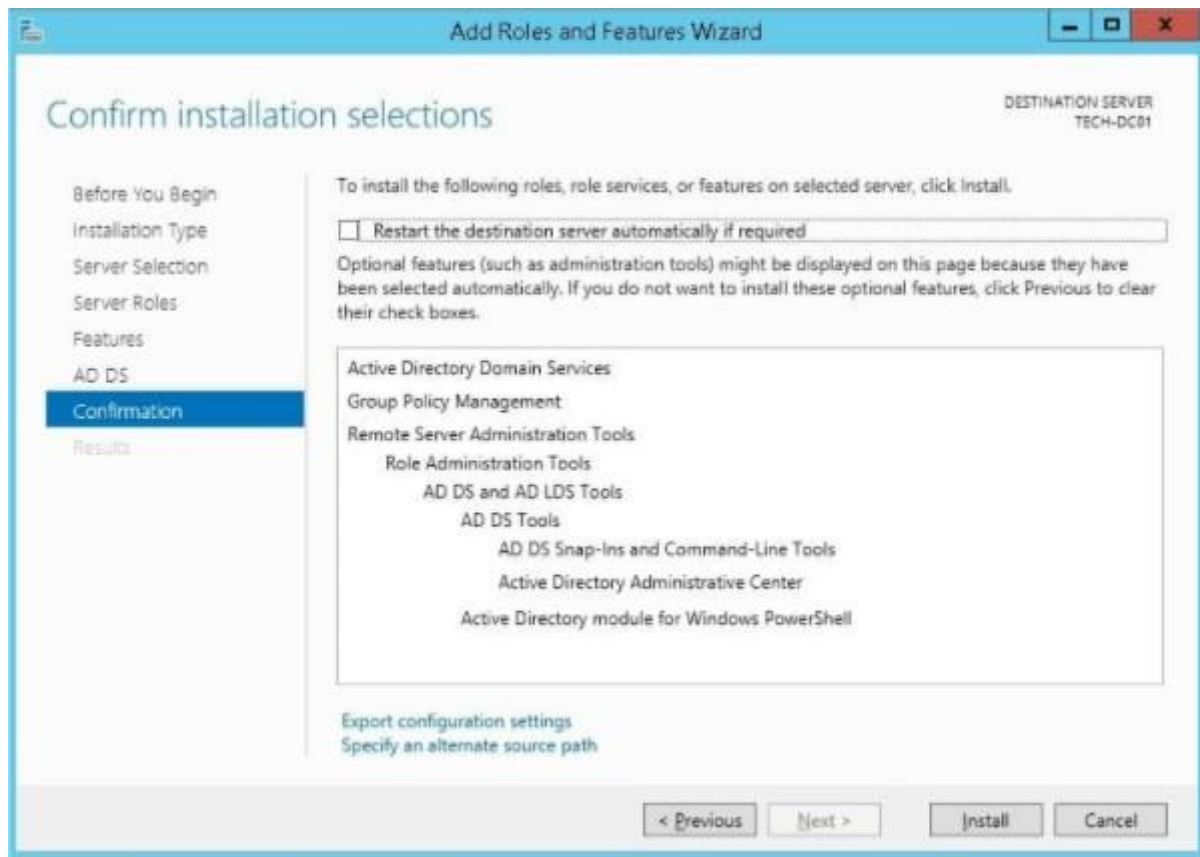
---



Continuez à cliquer sur le bouton **Suivant** jusqu'à atteindre la dernière fenêtre.

# RAPPORT TECHNIQUE

Sur la fenêtre de confirmation, cliquez sur le bouton **Installer**.

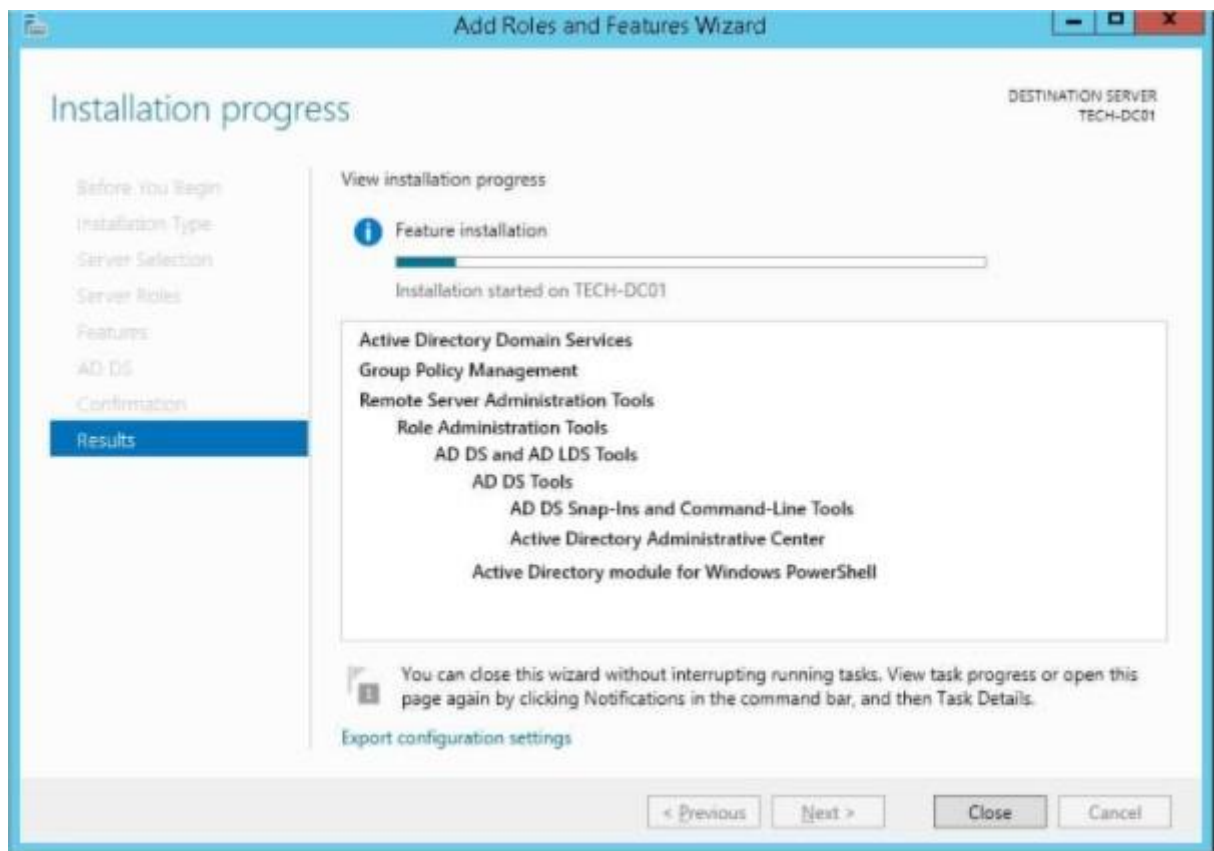


Attendez que l'installation des services se termine.

---

# RAPPORT TECHNIQUE

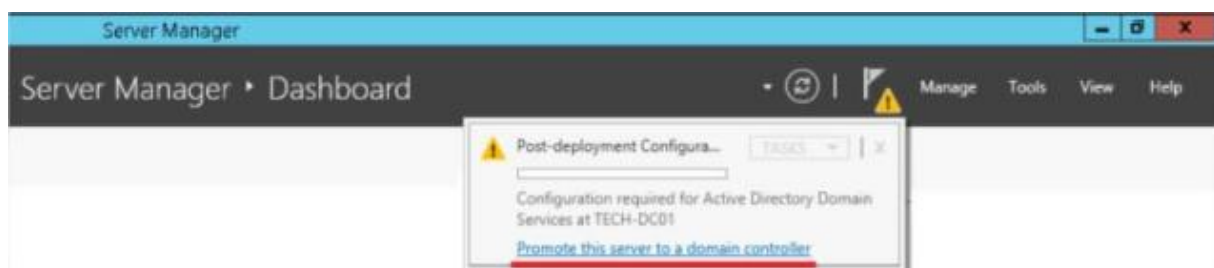
---



Vous avez terminé l'installation des services.

## 2. Promotion du serveur en contrôleur de domaine

Après avoir ouvert l'application « **Gestionnaire de serveur** », cliquer sur le menu du drapeau jaune et sélectionner l'option pour promouvoir ce serveur en contrôleur de domaine.

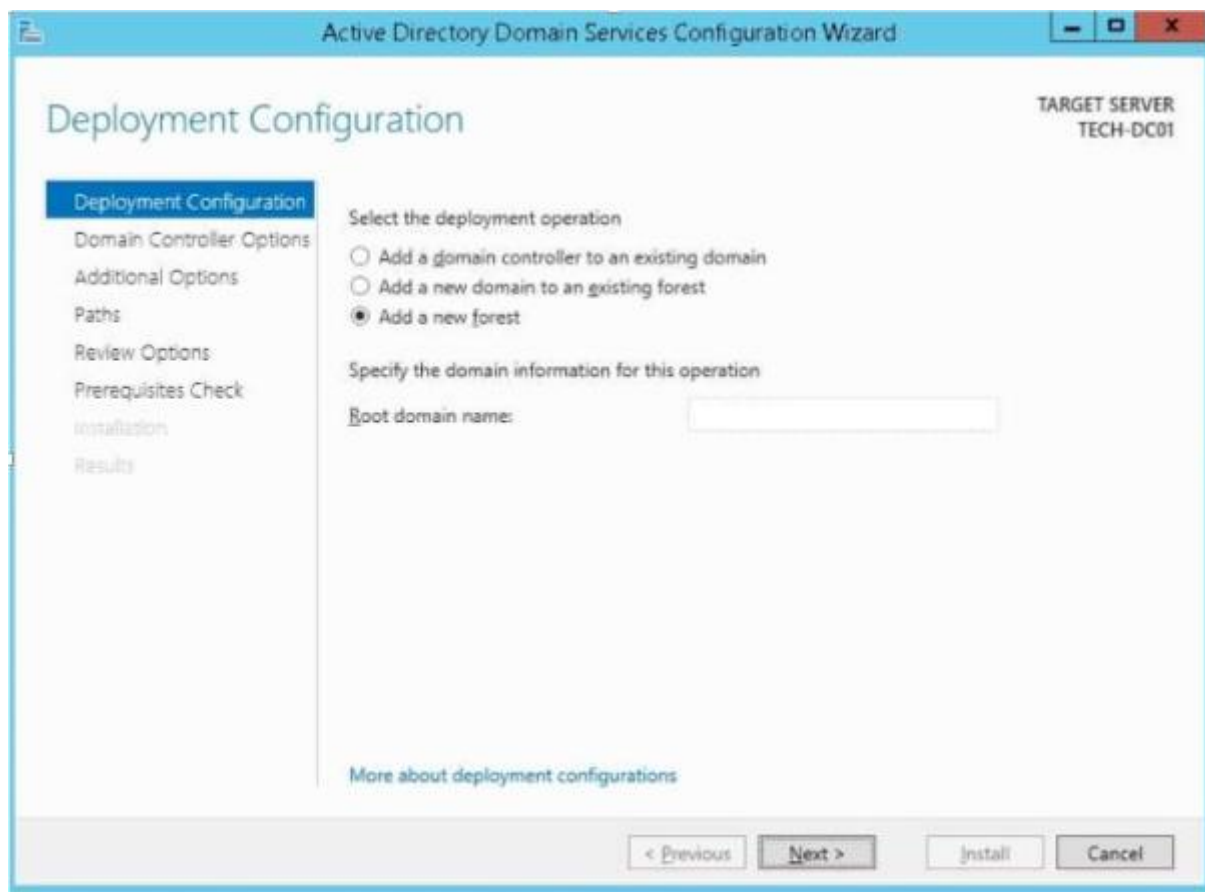


---

# RAPPORT TECHNIQUE

---

Sélectionnez l'option « ajouter une nouvelle forêt » en anglais Add a new forest et entrez le nom de domaine racine, pour le groupe ISEC c'est **isec-group.local** et pour telecom ISEC c'est **isec-telecom.local**.



Créer un mot de passe pour autoriser la restauration Active Directory.

# RAPPORT TECHNIQUE

The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window. The title bar includes standard Windows window controls. The main window has a blue header with the title. On the left is a navigation pane with the following items: 'Deployment Configuration', 'Domain Controller Options' (highlighted in blue), 'DNS Options', 'Additional Options', 'Paths', 'Review Options', 'Prerequisites Check', 'Installation', and 'Results'. The main content area is titled 'Domain Controller Options' and shows the 'TARGET SERVER' as 'TECH-DC01'. The content is organized into sections: 'Select functional level of the new forest and root domain' with dropdowns for 'Forest functional level' and 'Domain functional level', both set to 'Windows Server 2012 R2'; 'Specify domain controller capabilities' with checkboxes for 'Domain Name System (DNS) server' (checked), 'Global Catalog (GC)' (checked), and 'Read only domain controller (RODC)' (unchecked); and 'Type the Directory Services Restore Mode (DSRM) password' with 'Password:' and 'Confirm password:' fields, both masked with dots. At the bottom right of the main area is a link 'More about domain controller options'. The bottom of the window features a grey bar with four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

Active Directory Domain Services Configuration Wizard

Domain Controller Options

TARGET SERVER  
TECH-DC01

Deployment Configuration  
Domain Controller Options  
DNS Options  
Additional Options  
Paths  
Review Options  
Prerequisites Check  
Installation  
Results

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2012 R2

Domain functional level: Windows Server 2012 R2

Specify domain controller capabilities

☒ Domain Name System (DNS) server  
☒ Global Catalog (GC)  
☐ Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password: .....

Confirm password: .....

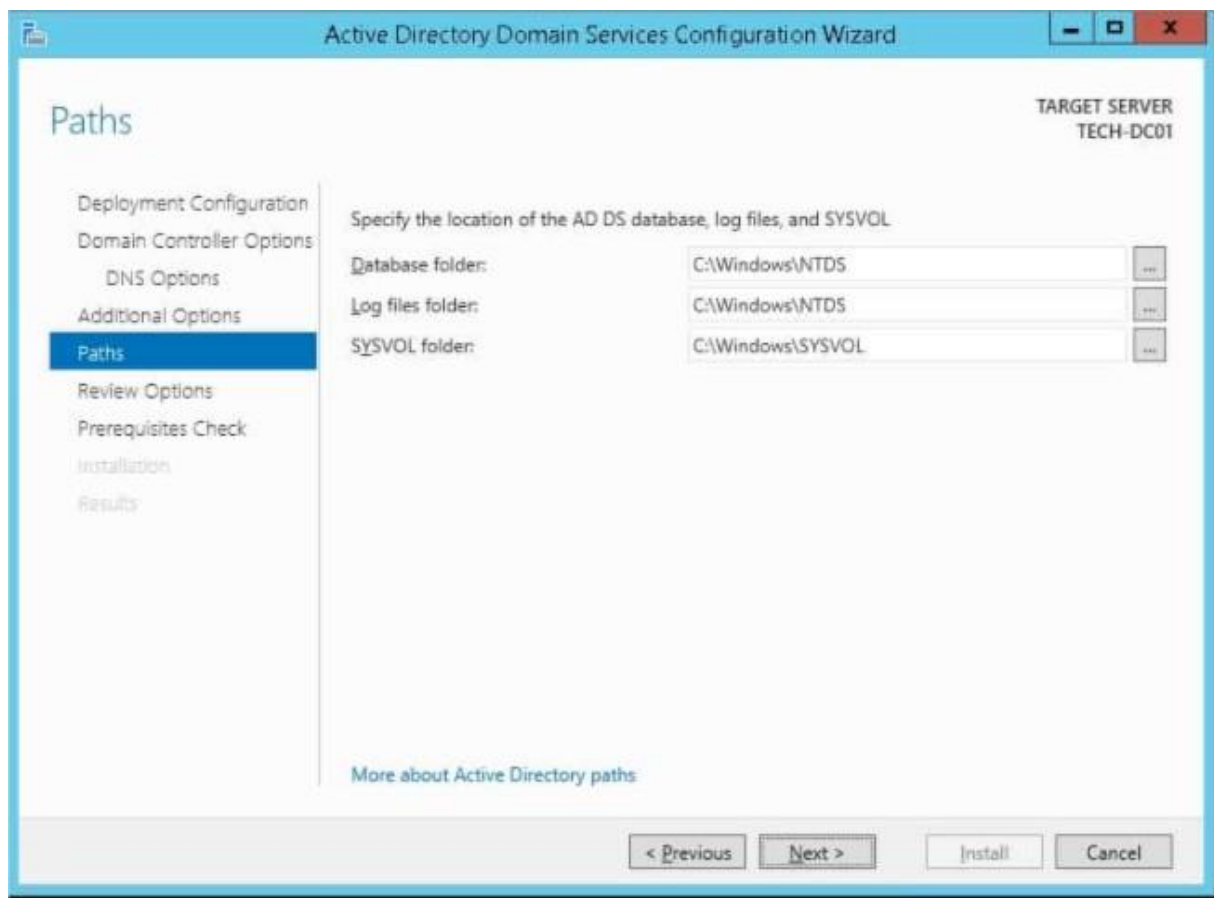
[More about domain controller options](#)

< Previous Next > Install Cancel

---

# RAPPORT TECHNIQUE

---

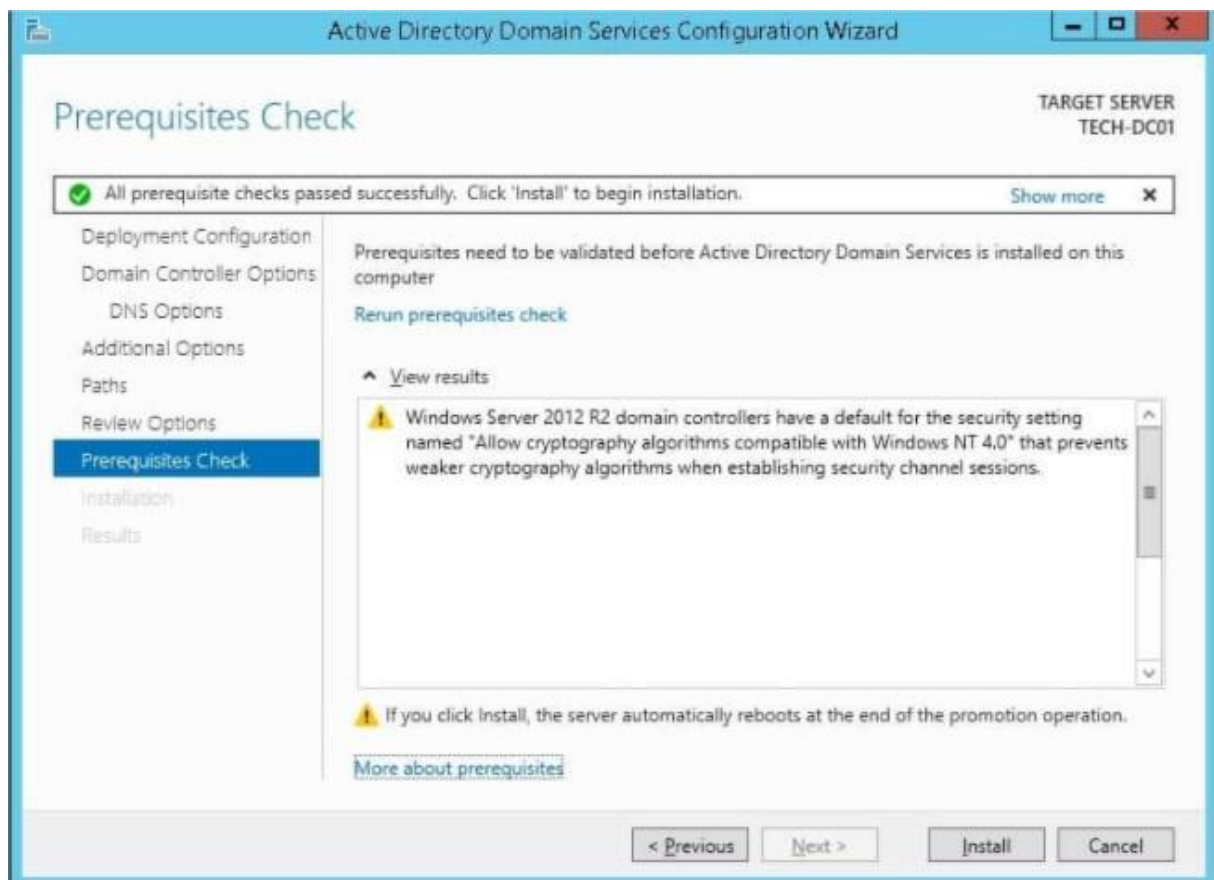


Sur la fenêtre de vérification des prérequis, cliquer sur **Installer**.

---

# RAPPORT TECHNIQUE

---



Attendre la fin de la configuration d'Active Directory.

L'ordinateur redémarrera automatiquement à la fin de la configuration.

## 3. Configuration du DHCP

Tout système informatique comportant plusieurs ordinateurs doit avoir un service DHCP pour l'adressage automatique de tous les ordinateurs connectés sur le réseau. L'installation du DHCP se fait de la manière suivante :

- ❖ Dans le gestionnaire de serveur, sélectionner « outil » puis valider « **DHCP** »
- ❖ Double-clic sur le nom du serveur, faire un clic droit sur « **IPv4** » et sélectionner « *Nouvelle étendue* ».
- ❖ Sélectionner « *Suivant* » jusqu'à la fenêtre suivante



---

# RAPPORT TECHNIQUE

---

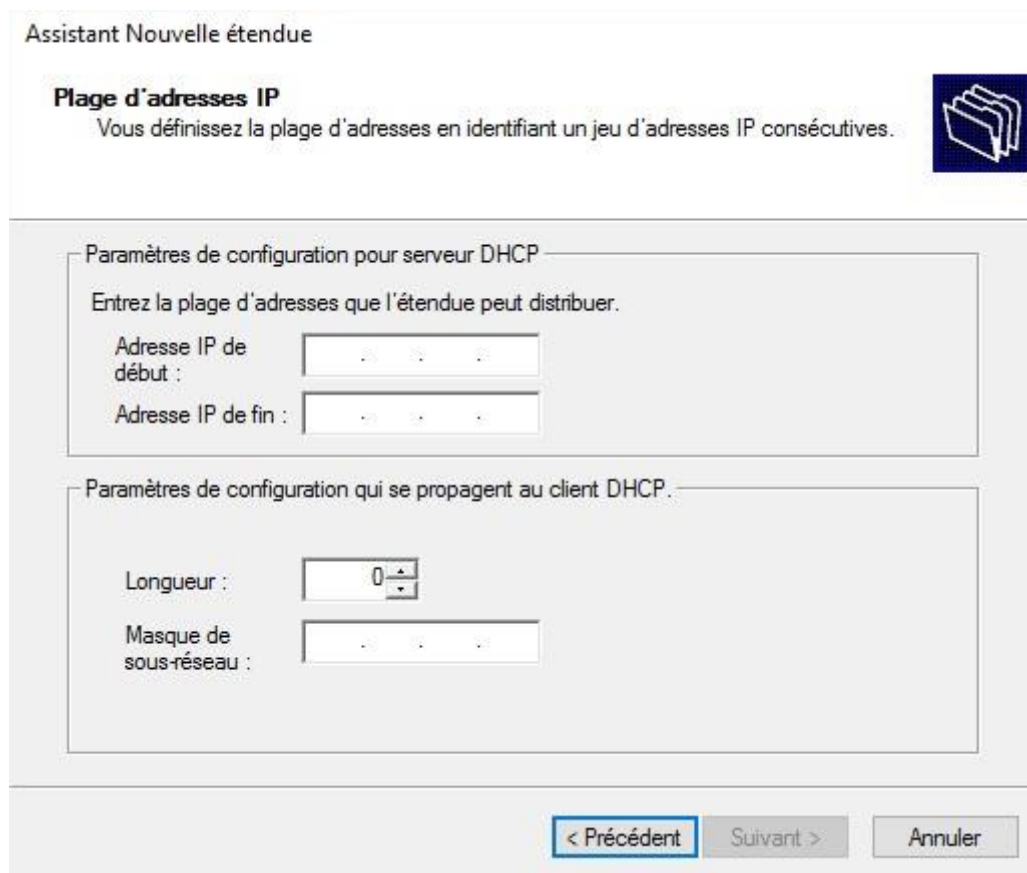


Figure 2: Plage d'adresses IP

Pour terminer et valider la configuration il suffit d'un clic sur « *Oui, je veux configurer ces options DHCP maintenant* ».

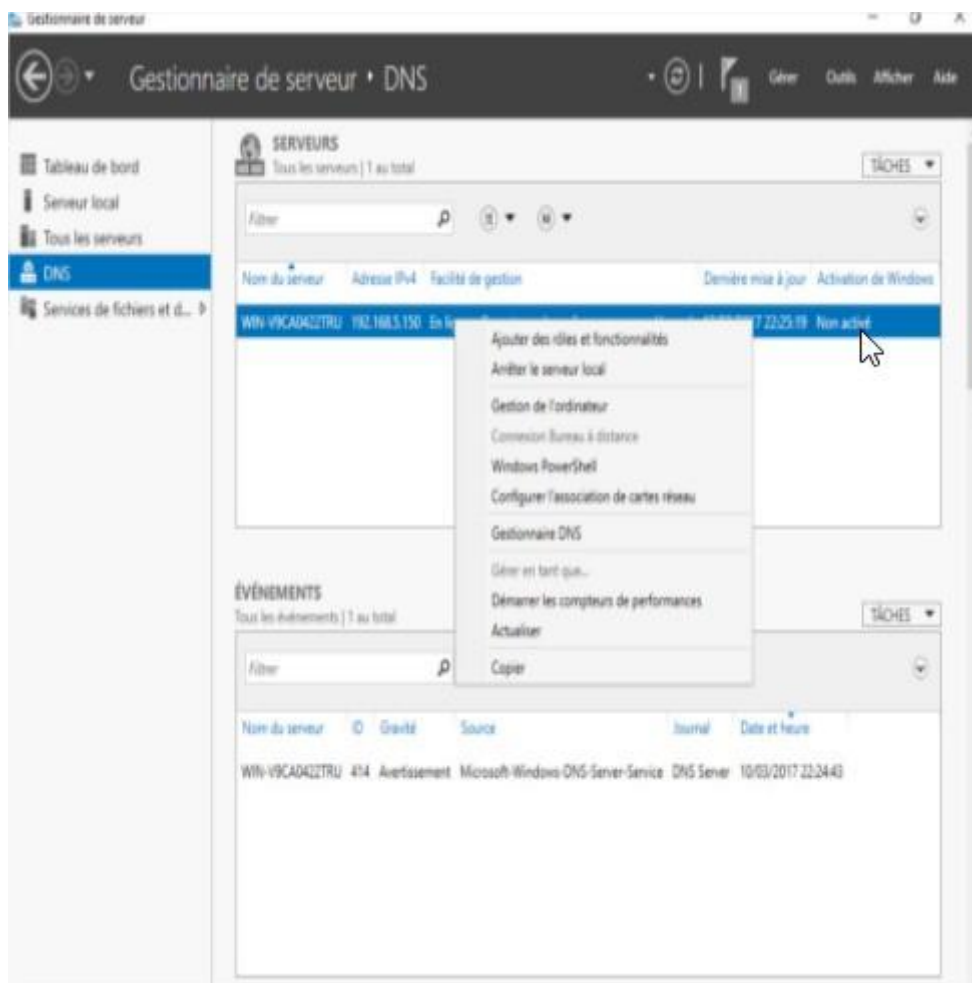
- ❖ Ajouter l'adresse IP de la passerelle par défaut (elle a été renseignée lors de du serveur)
- ❖ Et ensuite valider toutes les autres options jusqu'à la fin
- ❖ Activer la nouvelle étendue puis cliquer sur Suivant et Terminer

## 4. Configuration du DNS

Après avoir installé le service DNS sur Windows server, nous allons maintenant configurer la zone de recherche directe de notre serveur DNS.

Ouvrir le gestionnaire de serveur et cliquer sur « **DNS** ». Une fenêtre semblable à celle-ci s'ouvrira :

# RAPPORT TECHNIQUE

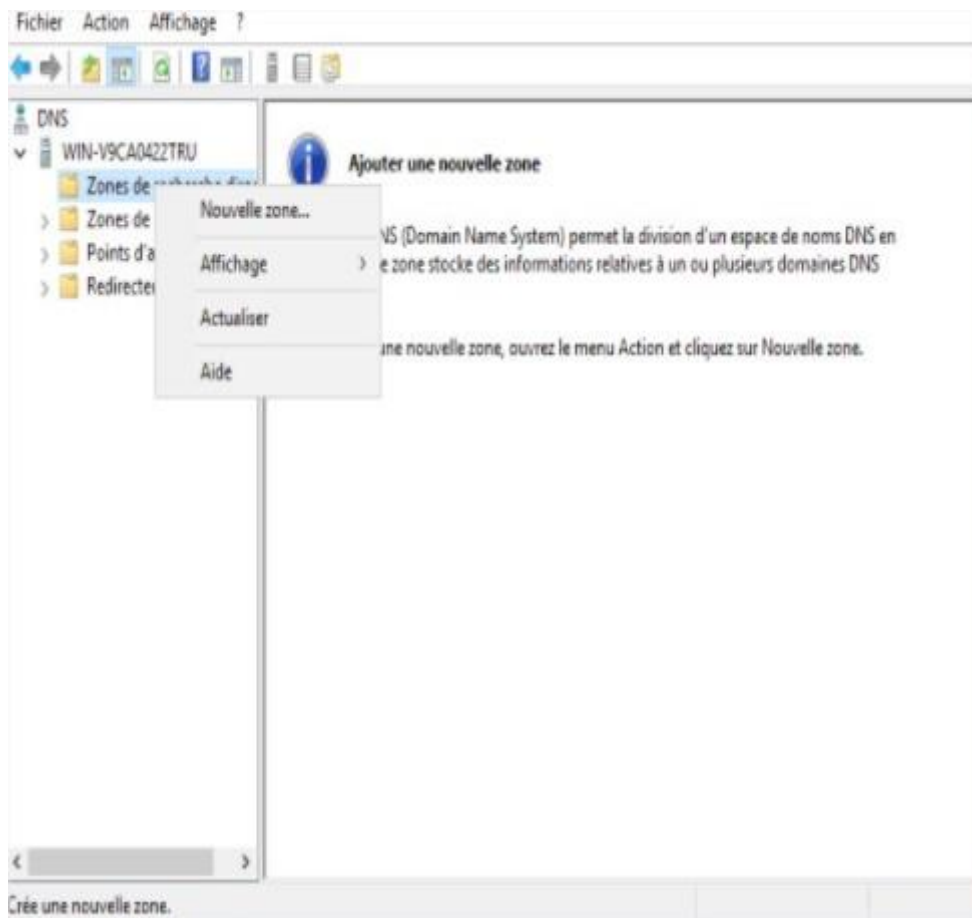


Faire un clic droit sur le serveur, puis cliquer sur « **Gestionnaire DNS** ». Nous avons la fenêtre ci-après :

---

# RAPPORT TECHNIQUE

---



Faire un clic sur le nom du serveur, puis un clic droit sur « **Zone de recherche direct** », puis cliquer sur « **Nouvelle zone** ».

---

# RAPPORT TECHNIQUE

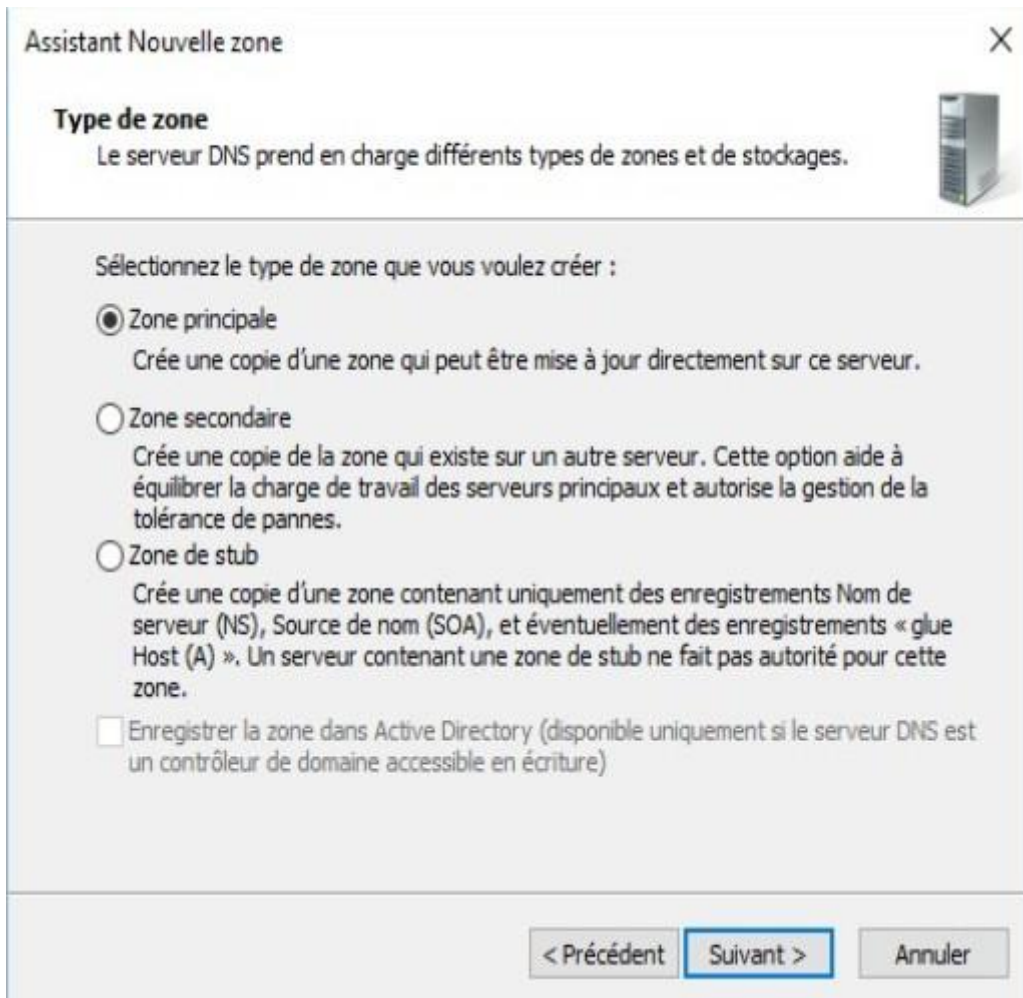
---



---

# RAPPORT TECHNIQUE

---



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)

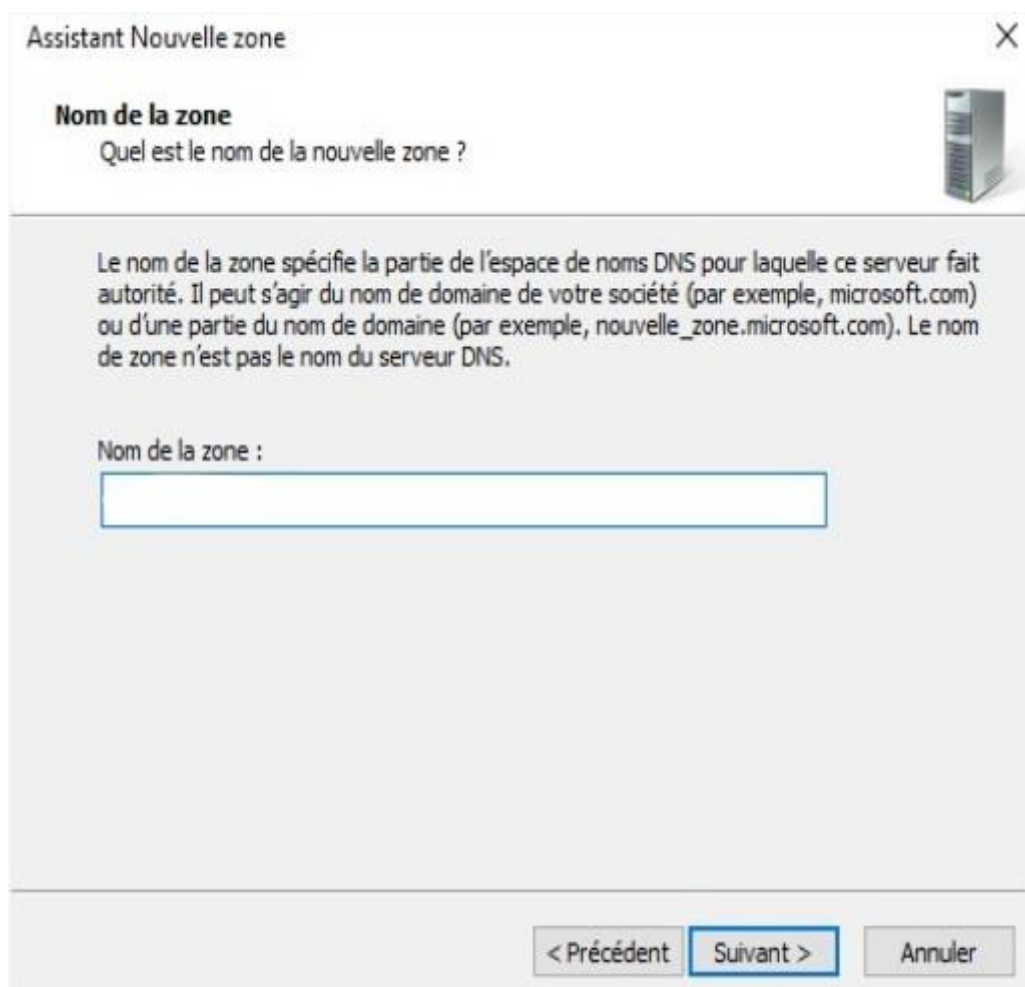
< Précédent   Suivant >   Annuler

Sélectionner « Zone principale » et cliquer sur « Suivant ».

---

# RAPPORT TECHNIQUE

---



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 :

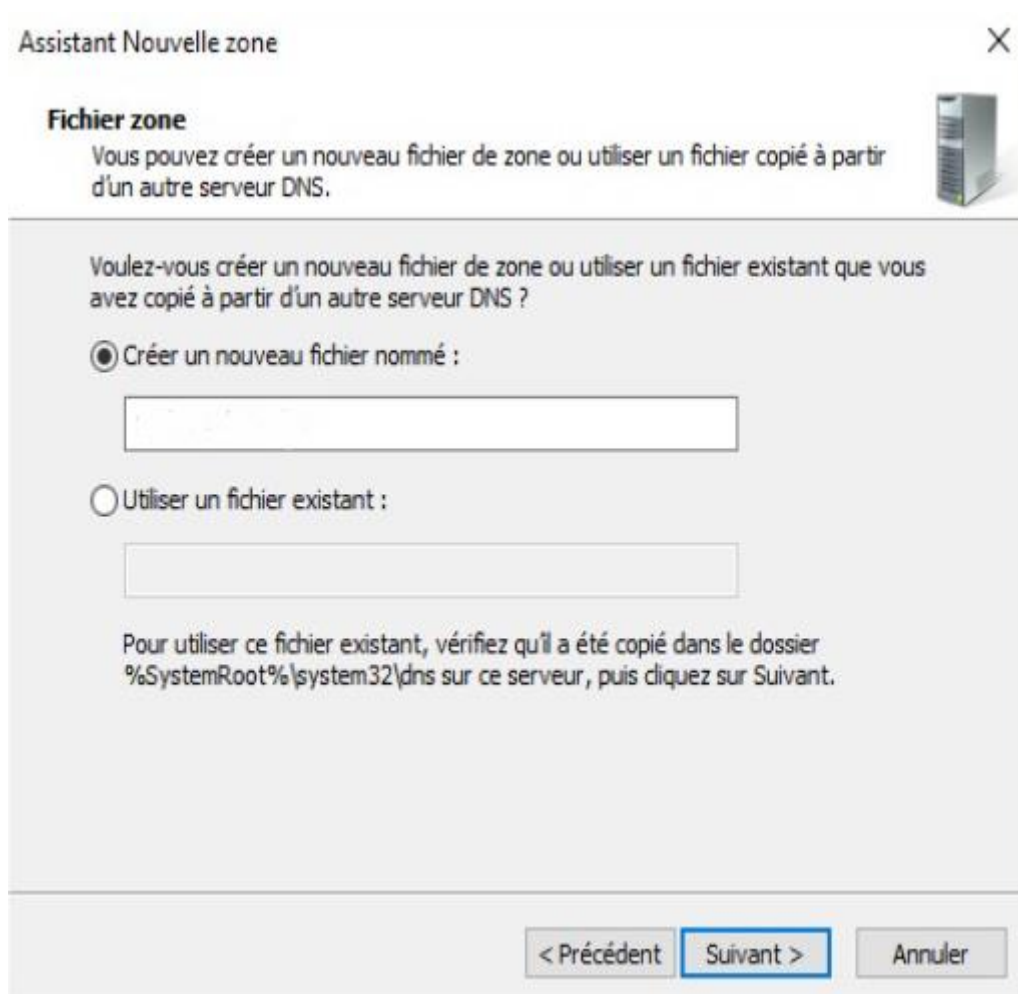
< Précédent Suivant > Annuler

Ici, il faut inscrire le nom du domaine souhaiter, dans notre cas il s'agit de : **isec-group.local**.

---

# RAPPORT TECHNIQUE

---



Assistant Nouvelle zone

**Fichier zone**

Vous pouvez créer un nouveau fichier de zone ou utiliser un fichier copié à partir d'un autre serveur DNS.

Voulez-vous créer un nouveau fichier de zone ou utiliser un fichier existant que vous avez copié à partir d'un autre serveur DNS ?

☒ Créer un nouveau fichier nommé :

☐ Utiliser un fichier existant :

Pour utiliser ce fichier existant, vérifiez qu'il a été copié dans le dossier %SystemRoot%\system32\dns sur ce serveur, puis cliquez sur Suivant.

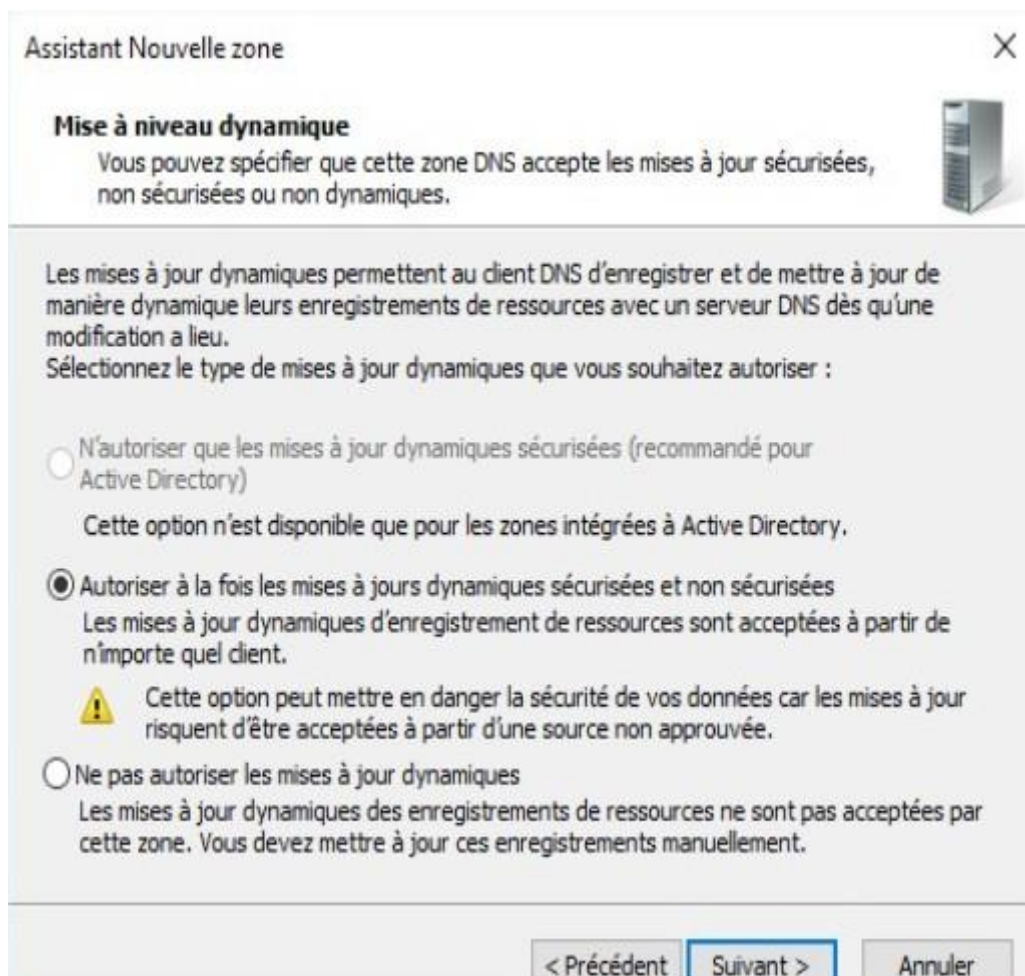
< Précédent Suivant > Annuler

A ce niveau, il faut sélectionner « Créer un nouveau fichier nommé : » ensuite le champ se remplira automatiquement sinon le remplir « **Nom du domaine.dns** ».

---

# RAPPORT TECHNIQUE

---



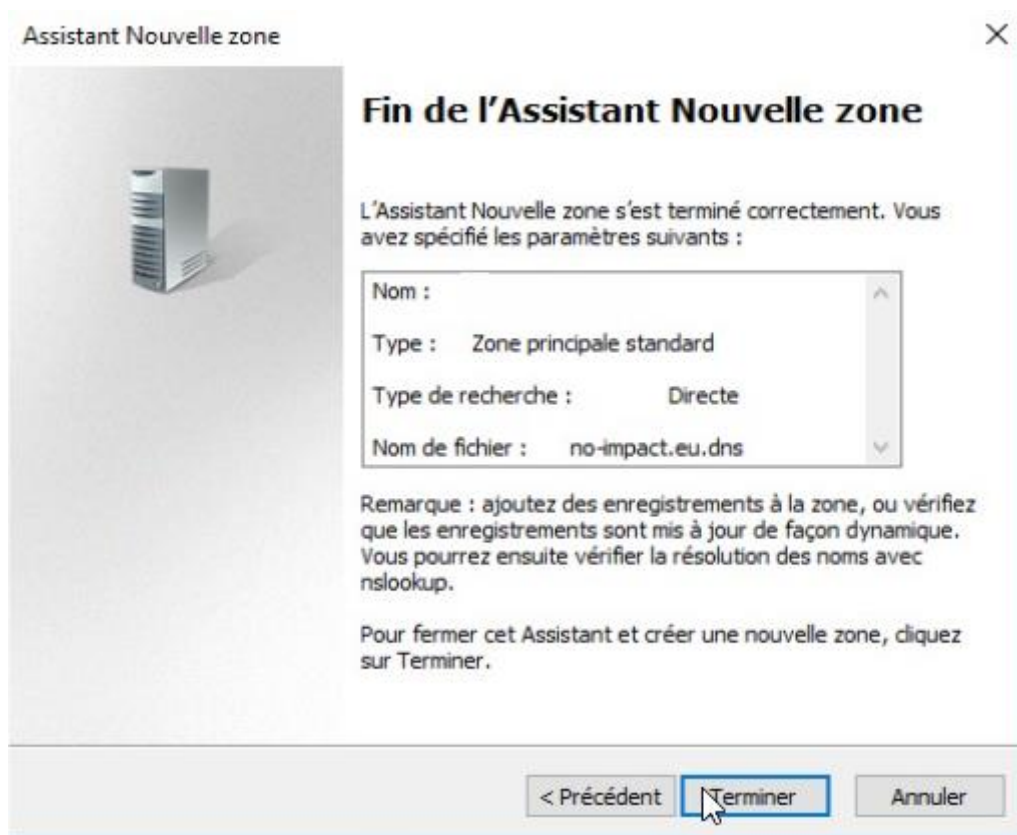
Cocher la case « **Autoriser à la fois les mises à jours dynamiques sécurisées et non sécurisées** ».



---

# RAPPORT TECHNIQUE

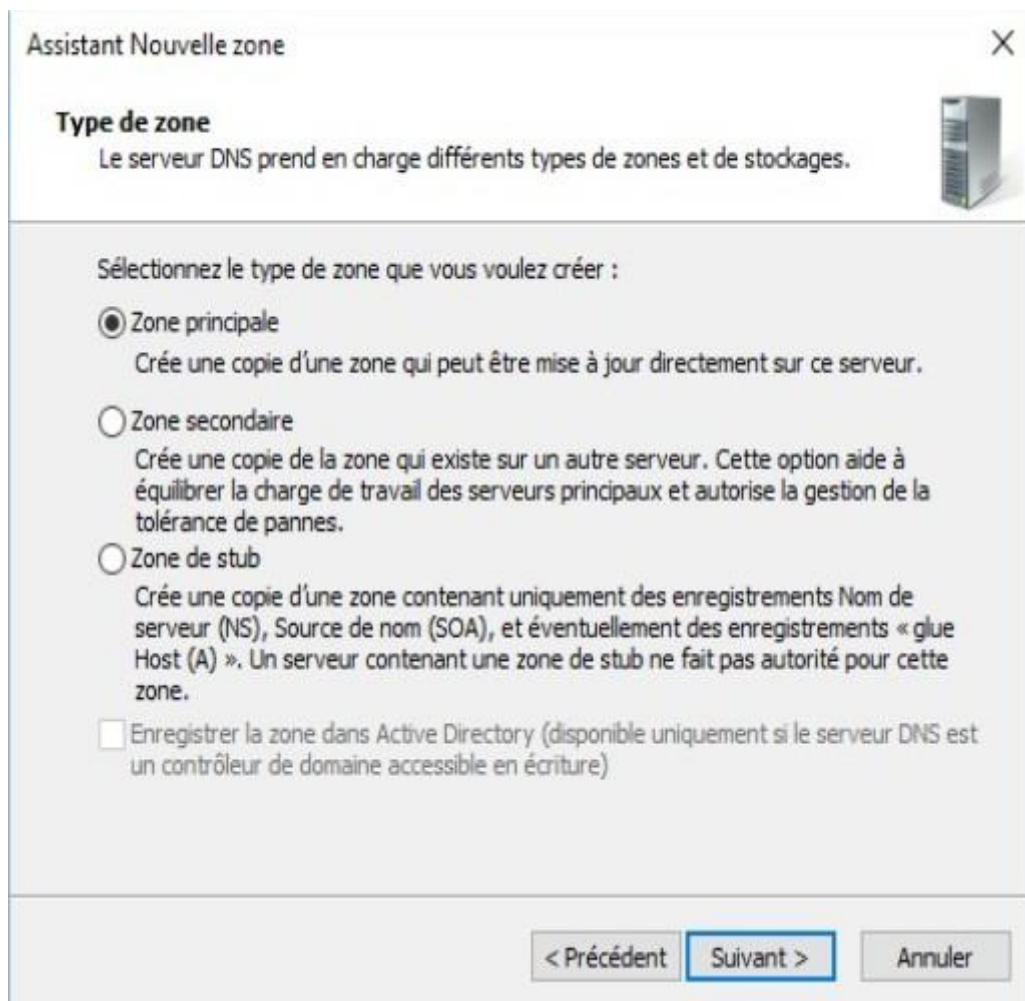
---



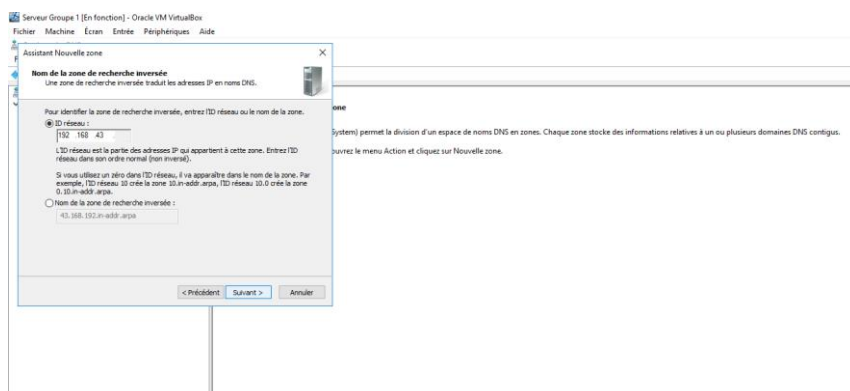
Maintenant nous allons configurer la zone de recherche inverse de notre serveur DNS.

Faire un clic droit sur « Zone de recherche inverse » ensuite cliquer sur « **nouvelle zone** ».

# RAPPORT TECHNIQUE

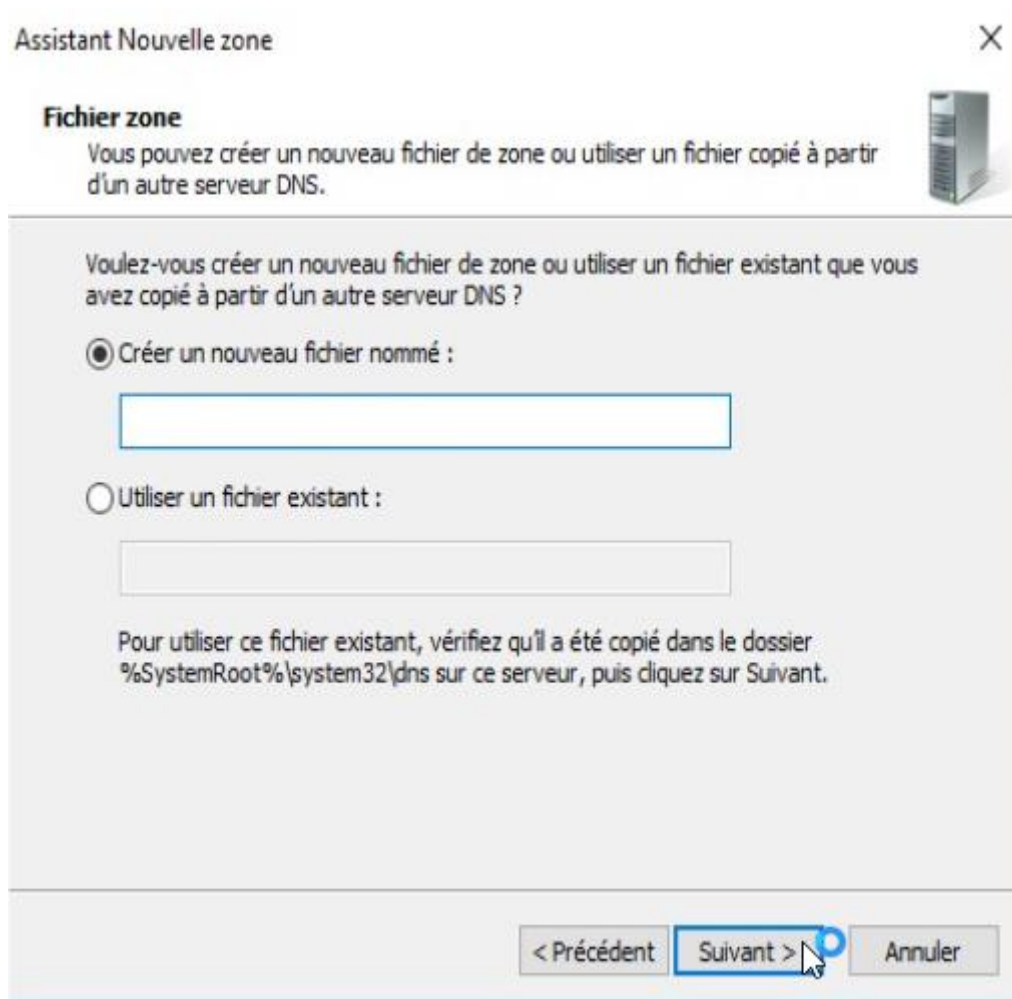


Sélectionner « **Zone principale** » et sur la prochaine fenêtre choisir « **Zone de recherche inversée IPV4** ».

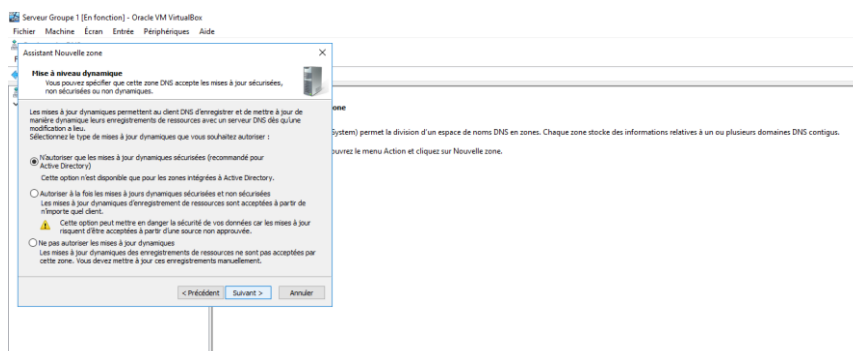


Sélectionner « ID réseau : » et y mettre l'adresse IP de notre réseau à savoir : 192.168.43

# RAPPORT TECHNIQUE

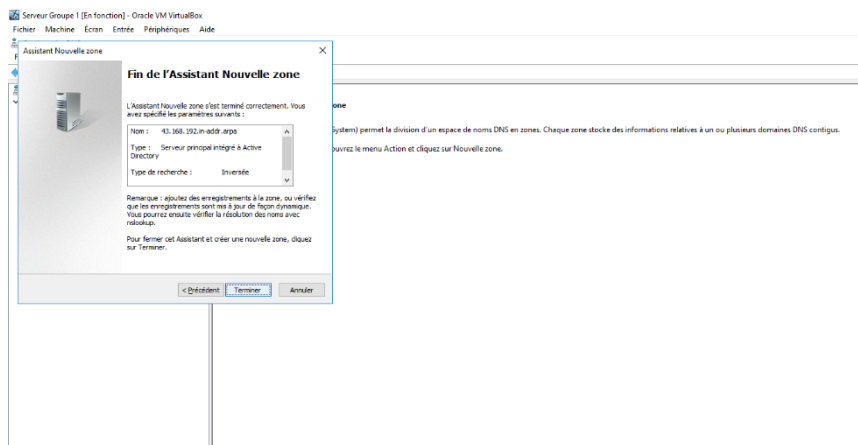


Sélectionner « Créer un nouveau fichier nommé : ». Le champ devrait se remplir automatiquement sinon mettre : **43.168.192.in-addr.arpa.dns**



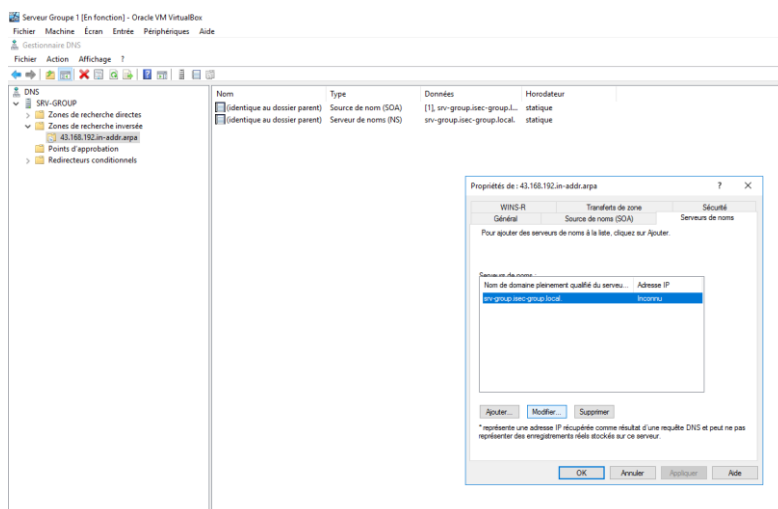
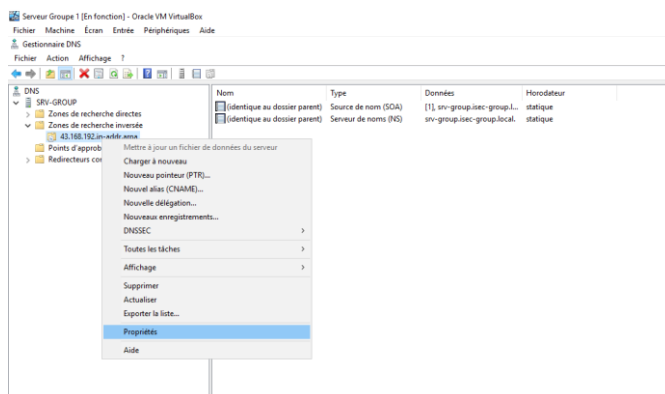
Cocher la case : « Autoriser à la fois les mises à jours dynamiques sécurisées et non sécurisées ».

# RAPPORT TECHNIQUE



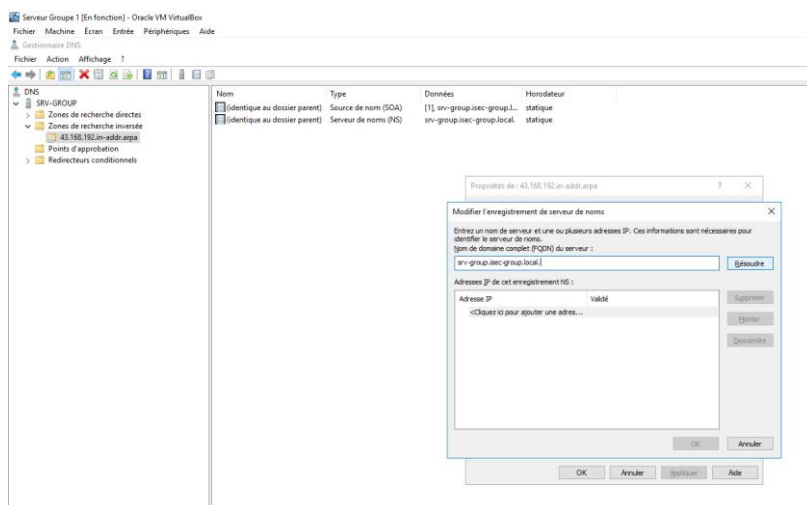
Nous allons maintenant configurer la redirection DNS.

Clic droit sur le fichier, puis « propriétés ».



Cliquer sur l'onglet « Serveur de nom », « modifier » et « résoudre ».

# RAPPORT TECHNIQUE



Les champs devraient se remplir automatiquement, ensuite appuyer sur « OK ».

La configuration du DNS en entier est terminée.

## 5. Création des « Organisation Units », des groupes et des utilisateurs

Pour créer un groupe ou encore un utilisateur, les étapes à suivre sont les suivantes :

- ❖ Dans le gestionnaire de serveur, cliquer sur « **Outil** »
- ❖ ensuite sur « **Utilisateurs et ordinateurs Active Directory** ».
- ❖ Sur le nom de notre serveur, effectuer un clic droit, ensuite sur groupe/utilisateur ou encore autre en fonction du besoin.
- ❖ L'interface de création apparaît, ensuite remplir les différents champs en fonction des informations des utilisateurs/ groupes et c'est terminé.

# RAPPORT TECHNIQUE

Nouvel objet - Utilisateur

Créer dans : isec-group.local/Isec Group

Prénom :  Initiales :

Nom :

Nom complet :

Nom d'ouverture de session de l'utilisateur :

@isec-group.local

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :

ISEC-GROUP0\

< Précédent Suivant > Annuler

Figure 3: Création d'un utilisateur

---

# RAPPORT TECHNIQUE

---

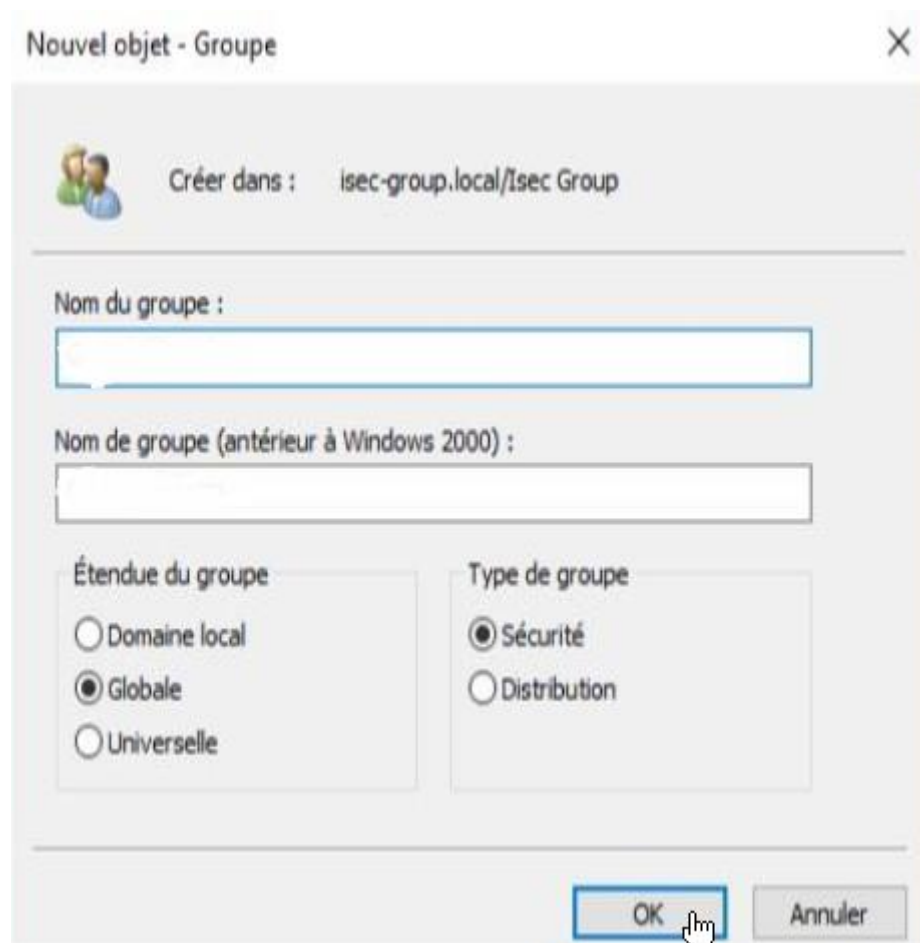


Figure 4: Création d'un groupe

Pour ajouter un utilisateur dans ce groupe, il faut :

- ❖ Aller dans les propriétés de l'utilisateur que l'on souhaite ajouter
- ❖ Dans l'onglet « **Membre de** », cliquer sur « **Ajouter** »
- ❖ Choisir le nom du groupe et valider

## 6. Ajouter un utilisateur dans un domaine

Après avoir créé des utilisateurs, nous devons les ajouter dans le domaine. Pour le faire, les étapes sont les suivantes :

## 7. Création des GPO « Stratégie de groupes »

- a) Création d'un répertoire partagé

---

# RAPPORT TECHNIQUE

---

Les Etapes à suivre sont les suivantes :

- ❖ Dans les propriétés du dossier à partager, aller à l'onglet « **partage** » et cliquer sur « **partager** »
- ❖ Ajouter les personnes et/ou les groupes qui auront accès au dossier partage ; et leur donner les droits en fonction du besoin. Nous attribuerons les droits en **lecture/écriture**.
- ❖ Valider en cliquant sur « Partager » (N'oublier pas de copier le chemin réseau du dossier partage).

## b) Création d'un GPO pour le lecteur réseau

Les étapes à suivre les étapes suivantes :

- ❖ Ouvrir « *Gestion de stratégie de groupe* » dans l'onglet « **outils** »
- ❖ Faire un clic droit sur le nom du serveur et créer un GPO et renseigner le nom du GPO.
- ❖ Ensuite aller dans « *Configuration Utilisateur* », puis « **Préférences** », puis Mappages de Lecteur

## c) Redirection du dossier « document »

Elle se fait de la manière suivante :

- ❖ Création d'un répertoire dossier et le partagé tel que précédemment expliqué ; cette fois ci appliqué le partage à tous les membres de la filiale puisque chacun d'eux aura son dossier « Documents » redirigés.
- ❖ Ensuite créer un nouveau GPO
- ❖ Aller dans **Configuration utilisateur /Stratégies /Paramètres Windows /Redirection de documents /Documents**
- ❖ Dans les propriétés de documents, choisissez comme paramètre « **De base** », dans emplacement du dossier cible choisir « *Créer un dossier pour chaque utilisateur sous le chemin d'accès racine* » et coller le chemin d'accès précédemment copié
- ❖ Valider la création et « **Appliqué** » le GPO

## d) Gestion de la stratégie de mot de passe

Pour configurer les mots de passe tel que spécifier dans le cahier de charge, il faut :

- ❖ Se rendre dans le « Centre d'Administration Active Directory situé dans « Outils »



---

# RAPPORT TECHNIQUE

---

Dans le paramètre du serveur,

- ❖ Ouvrir « *System > Password Containers Settings* »
- ❖ Choisir « *Nouveau > Paramètres de mot de passe* »
- ❖ Remplir les champs explicites en fonction de ce qui est demandé dans le cahier de charge.
- ❖ Cliquer sur « **Ajouter** » pour sélectionner les utilisateurs et/ou les groupes à qui s'appliqueront la stratégie de mot de passe. Et « **Valider** »

En cas de verrouillage d'un compte d'utilisateur, sera déverrouillé par l'administrateur en suivant les étapes suivantes :

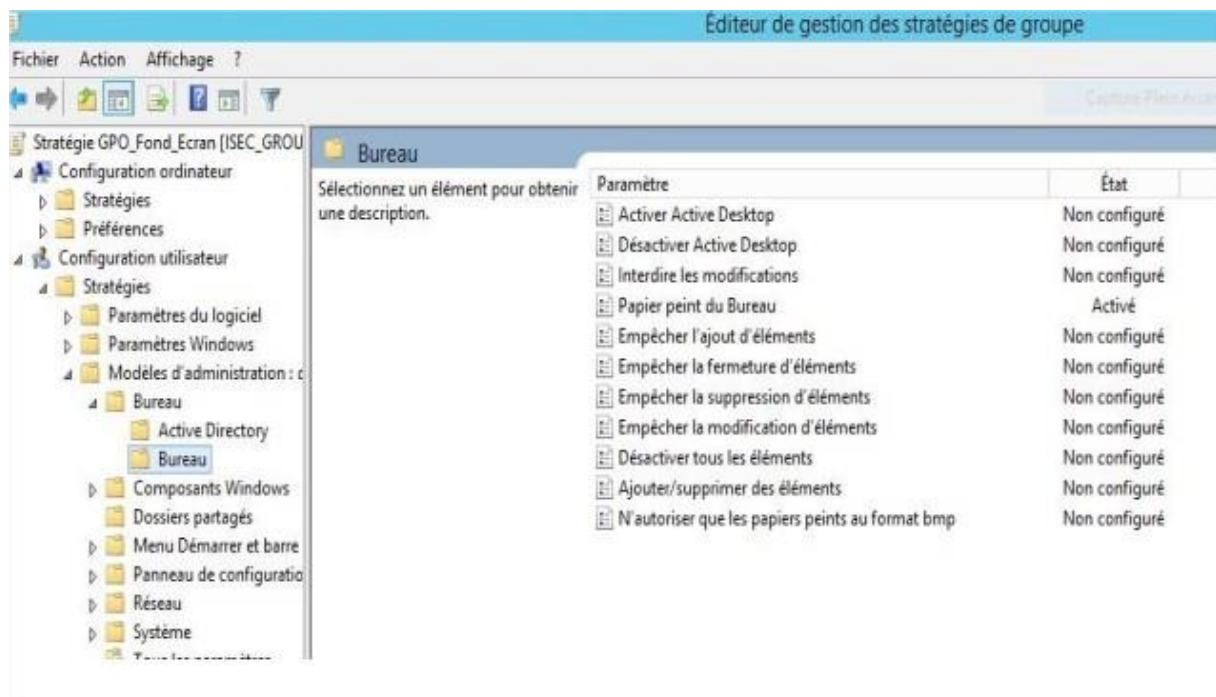
- ❖ Après l'ouverture du « Centre d'Administration Active Directory »
- ❖ Dans les paramètres du serveur choisir **Users** ou le nom de votre OU au lieu de System comme plutôt
- ❖ Sélectionner le nom du compte verrouillé et cliquer sur Déverrouiller.

## e) Gestion des Papiers Peints

Il est à noter ici que les images pour les fonds d'écran devraient être au **format .JPEG**, ensuite :

- ❖ Créer un répertoire contenant les images à appliquer en fond d'écran. Il sera partagé à tous les utilisateurs du groupe
- ❖ Créer un GPO, l'appliquer et ajouter les utilisateurs et/ou groupes qui auront le papier peint choisi en fonction de leur poste et leur service
- ❖ Modifier le GPO, aller dans */Configuration Utilisateur /Stratégies / Modèles d'administration /Bureau /Bureau / Papier peint.*
- ❖ Ouvrir papier peint et cocher la case « **Activé** »
- ❖ Dans le Nom du papier peint, indiqué le chemin d'accès du dossier images partage et y ajouter le nom de la photo à définir en papier peint avec l'extension **.jpg**
- ❖ Cliquer sur Paramètre suivant deux fois et cocher à nouveau Activé.
- ❖ Appliquer et valider

# RAPPORT TECHNIQUE



## f) Déploiement de l'application 7Zip

Il faut au préalable avoir un setup de 7-zip puis suivre les étapes suivantes :

- ❖ Copier le fichier 7-zip.msi dans un dossier qui aura son lecteur réseau créé sur les serveurs
- ❖ Créer une stratégie de groupe et y ajouter tous les utilisateurs puisqu'ils auront tous accès à l'application 7-ZIP et appliquer la stratégie de groupe
- ❖ Aller dans **Modifier > Configuration utilisateur > Stratégies > Paramètre du logiciel > Installation du logiciel**
- ❖ Clic droit **Nouveau > Package et choisir le setup de 7zip** dans le lecteur réseau et non le dossier puis valider
- ❖ Aller dans les propriétés du package (7zip) ; dans l'onglet **Déploiement**, cocher les cases Attribué et Installer cette application lors de l'ouverture de session
- ❖ Ensuite, appliquer et valider

## g) Gestion des Périphériques Amovibles

Nous n'avons pas besoin de créer un dossier partagé ensuite suivre les étapes suivantes

# RAPPORT TECHNIQUE

- ❖ Gérer une stratégie de groupe donner les droits à tous les membres du groupe et supprimer
- ❖ Utilisateurs authentifiés et appliquer la stratégie de groupe Modifier la stratégie ainsi créée et aller dans *Configuration ordinateur > Stratégies>Modèle d'administration >Composant Windows > Stratégies d'exécution automatique*
- ❖ Double-cliquer sur Désactiver l'exécution automatique puis cliquer sur Activé.
- ❖ Cliquer sur Paramètre suivant deux fois et cocher à nouveau Activé.
- ❖ Appliquer et valider

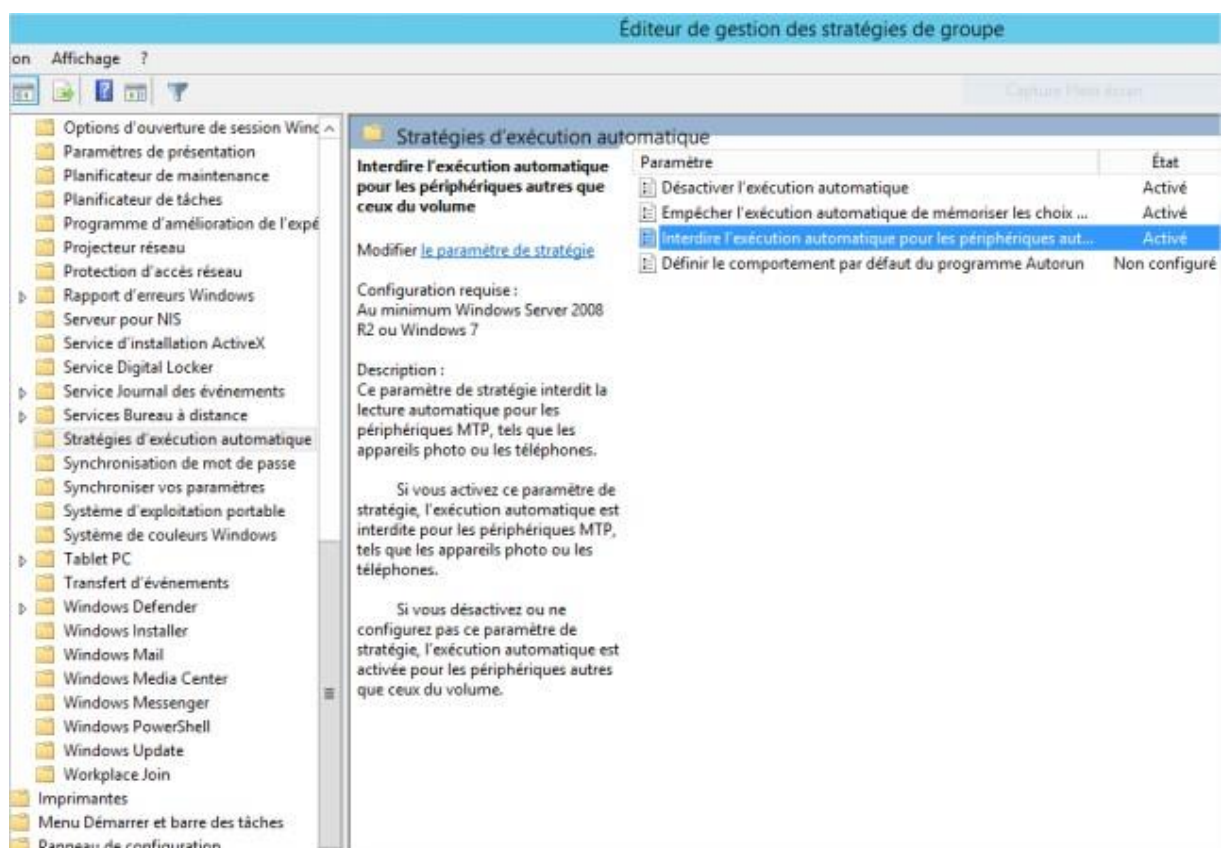


Figure 5: Périphériques amovibles

## h) Gestions des imprimantes

Puisque nous avons déjà installé les services d'impression, il faut :

- ❖ Aller dans « *Gestion de l'impression* » située dans « **Outils** »
- ❖ Aller dans *Serveurs d'impression > Nom de notre serveur > Imprimantes*

---

# RAPPORT TECHNIQUE

---

- ❖ Ajouter une imprimante, cocher Ajouter une imprimante via un port existant et choisir l'imprimante et les pilotes à installer.
- ❖ Dans les onglets *Nom de l'imprimante et Nom du partage*, renseigner le même nom.
- ❖ Renseigner une stratégie de groupe (celle par défaut), cocher les deux cases et cliquer sur ajouter.
- ❖ Terminer l'installation

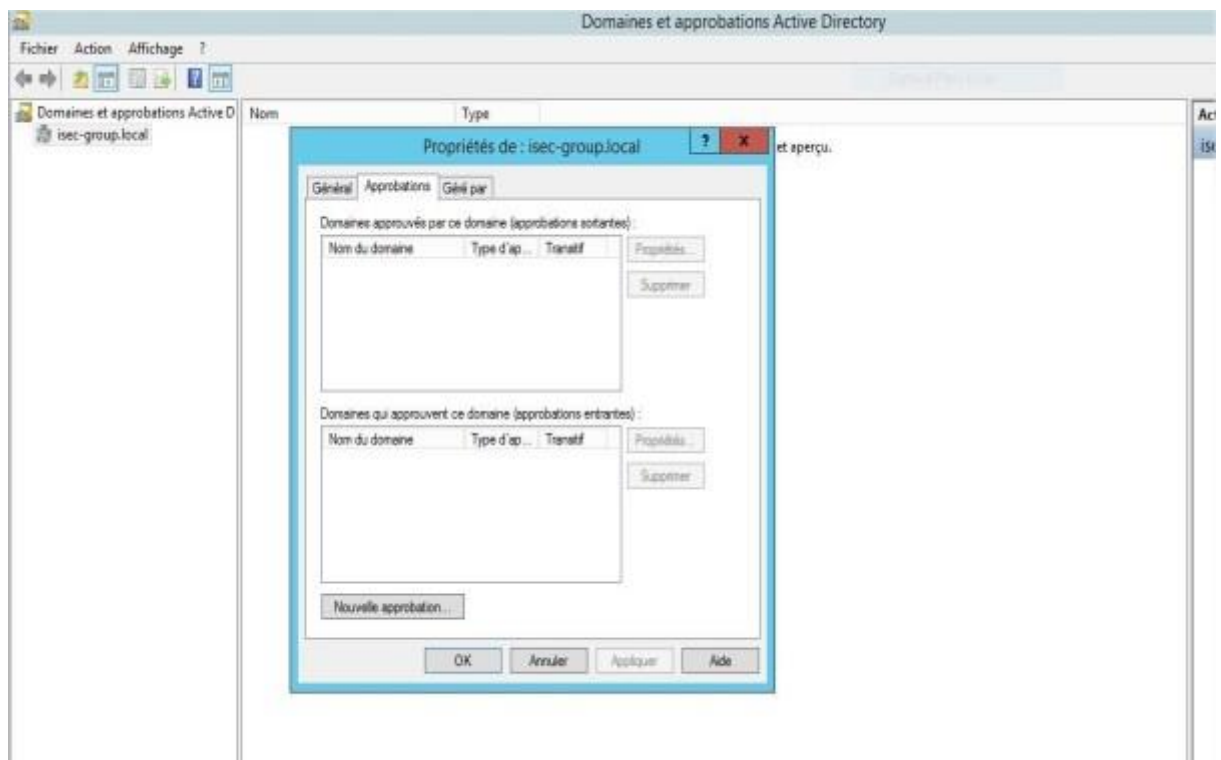


Figure 6: Création d'une nouvelle approbation

## 8. Supervision

**Zabbix** est une solution de surveillance distribuée open source de classe entreprise.

**Zabbix** est un logiciel qui surveille de nombreux paramètres d'un réseau ainsi que la santé et l'intégrité des serveurs, des machines virtuelles, des applications, des services, des bases de données, des sites Web, du Cloud et plus encore. Il est gratuit et est écrit et distribué sous la licence publique générale GPL version 2. Cela signifie que son code source est librement distribué et disponible pour le grand public.

### i) Configuration du serveur Zabbix

---

# RAPPORT TECHNIQUE

---

- On commence par installer les différents paquets requis pour le bon fonctionnement de Zabbix, notamment : **apache2**, **php**, **mysql**, **mariadb** :

```
# apt install apache2 php php-mysql php-mysqldb  
php-ldap php-bcmath php-mbstring php-gd php-pdo  
php-xml libapache2-mod-php
```

- On vérifie grâce à la commande **service apache2 status** pour vérifier qu'apache2 fonctionne correctement.

```
root@kali:~# service apache2 status  
● apache2.service - The Apache HTTP Server  
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: en  
   Active: active (running) since Tue 2020-10-27 15:26:17 CET; 35s ago  
     Docs: https://httpd.apache.org/docs/2.4/  
   Process: 2007 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)  
 Main PID: 2028 (apache2)  
    Tasks: 6 (limit: 2306)  
   Memory: 20.1M  
   CGroup: /system.slice/apache2.service  
           └─2028 /usr/sbin/apache2 -k start  
             └─2032 /usr/sbin/apache2 -k start  
               └─2033 /usr/sbin/apache2 -k start  
                 └─2034 /usr/sbin/apache2 -k start  
                   └─2035 /usr/sbin/apache2 -k start  
                     └─2036 /usr/sbin/apache2 -k start  
  
oct. 27 15:26:13 kali systemd[1]: Starting The Apache HTTP Server ...  
oct. 27 15:26:17 kali apachectl[2007]: AH00558: apache2: Could not reliably deter  
oct. 27 15:26:17 kali systemd[1]: Started The Apache HTTP Server.  
lines 1-19/19 (END)
```

- Pour la sauvegarde des données, Zabbix a besoin d'une base de données. Zabbix supporte **MySQL**, **MariaDB**, **Postgres** et **Oracle**. Nous allons utiliser **MariaDB** dans pour déploiement

```
root@kali:~# apt install mariadb-server mariadb-client
```

- Ensuite on vérifie que le service de **MariaDB** fonctionne correctement

```
root@kali:~# service mariadb status
```

---

# RAPPORT TECHNIQUE

---

```
root@kali:~# service mariadb status
● mariadb.service - MariaDB 10.3.24 database server
   Loaded: loaded (/lib/systemd/system/mariadb.service; disabled; vendor preset: disabled)
   Active: active (running) since Tue 2020-10-27 15:26:12 CET; 4min 46s ago
     Docs: man:mysqld(8)
           https://mariadb.com/kb/en/library/systemd/
   Process: 1875 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysql
   Process: 1876 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSITI
   Process: 1878 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= ||
   Process: 1956 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POSITI
   Process: 1958 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
  Main PID: 1925 (mysqld)
    Status: "Taking your SQL requests now..."
     Tasks: 56 (limit: 2306)
    Memory: 192.7M
    CGroup: /system.slice/mariadb.service
            └─1925 /usr/sbin/mysqld

oct. 27 15:26:04 kali systemd[1]: Starting MariaDB 10.3.24 database server ...
oct. 27 15:26:05 kali mysqld[1925]: 2020-10-27 15:26:05 0 [Note] /usr/sbin/mysqld (mysq
oct. 27 15:26:05 kali mysqld[1925]: 2020-10-27 15:26:05 0 [Warning] Could not increase
oct. 27 15:26:12 kali systemd[1]: Started MariaDB 10.3.24 database server.
oct. 27 15:26:12 kali /etc/mysql/debian-start[1960]: Upgrading MySQL tables if necessar
oct. 27 15:26:14 kali /etc/mysql/debian-start[2022]: Triggering myisam-recover for all
lines 1-23/23 (END)
```

- Ensuite on procède à la configuration de **MariaDB** :

```
root@kali:~# mysql_secure_installation

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!
```



---

# RAPPORT TECHNIQUE

---

```
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorisation.

Set root password? [Y/n] y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
... Success!

By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them. This is intended only for testing, and to make the installation
go a bit smoother. You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
... Success!

Normally, root should only be allowed to connect from 'localhost'. This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] y
... Success!
```

- Une fois le serveur de base de données est sécurisé on doit créer une base de données pour Zabbix

```
# mysql -u root -p
```

```
MariaDB [(none)]> create database zabbix character set
utf8 collate utf8_bin;
MariaDB [(none)]> grant all privileges on zabbix.* to
zabbix@localhost identified by 'admin@monit1';
MariaDB [(none)]> quit;
```

- Maintenant il faut installer **zabbix server,web frontend**

```
# apt -y install zabbix-server-mysql zabbix-frontend-php zabbix-agent
```

- Importer les données de départ pour le fonctionnement de **zabbix**  

```
# zcat /usr/share/doc/zabbix-server-mysql/schema.sql.gz | mysql -u zabbix -p
zabbix
```
- Maintenant que tout l'environnement est prêt il faut donc lancer le service **zabbix-server** sans toutefois oublier par la suite de vérifier le statut du service

# RAPPORT TECHNIQUE

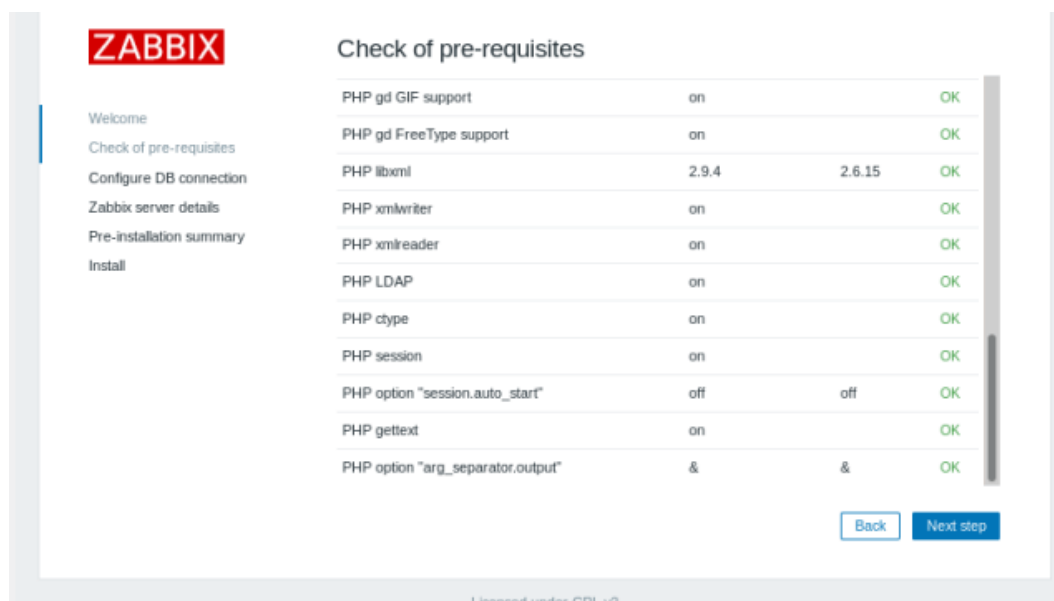
```
# systemctl start zabbix-server
# systemctl enable zabbix-server
```

```
root@tecmin1:~# systemctl start zabbix-server zabbix-agent
root@tecmin1:~# systemctl enable zabbix-server zabbix-agent
Synchronizing state of zabbix-server.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable zabbix-server
Synchronizing state of zabbix-agent.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable zabbix-agent
Created symlink /etc/systemd/system/multi-user.target.wants/zabbix-server.service → /lib/systemd/system/zabbix-server.service.
Created symlink /etc/systemd/system/multi-user.target.wants/zabbix-agent.service → /lib/systemd/system/zabbix-agent.service.
root@tecmin1:~#
```

- Rendez-vous maintenant dans votre navigateur à l'url **localhost/zabbix** pour accéder à l'interface d'administration de zabbix



- Vérifier les prérequis



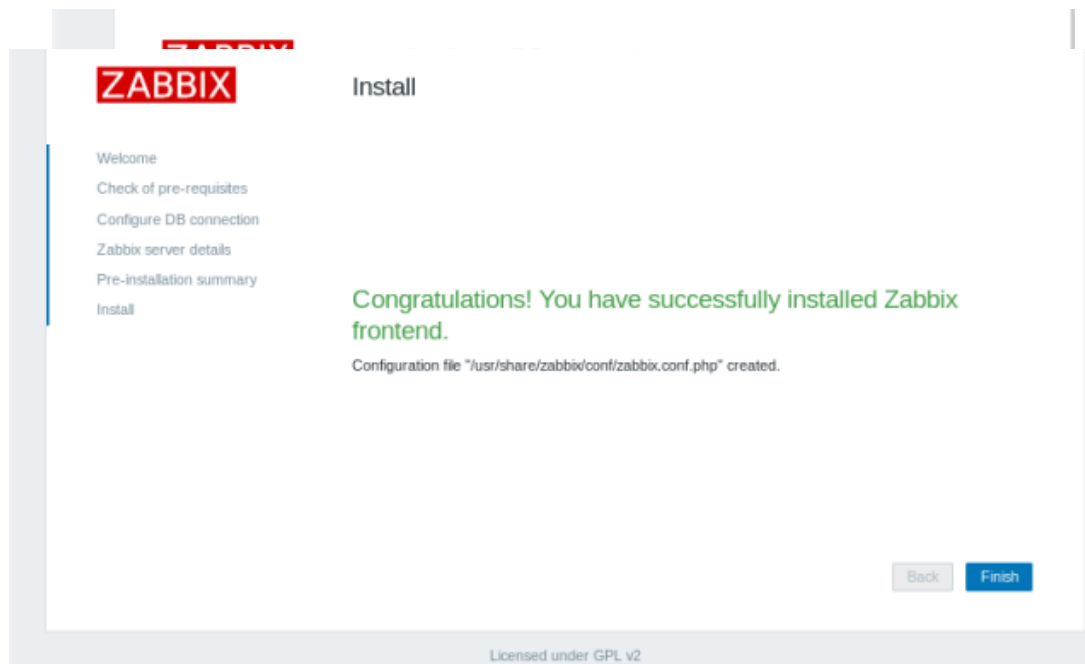


---

# RAPPORT TECHNIQUE

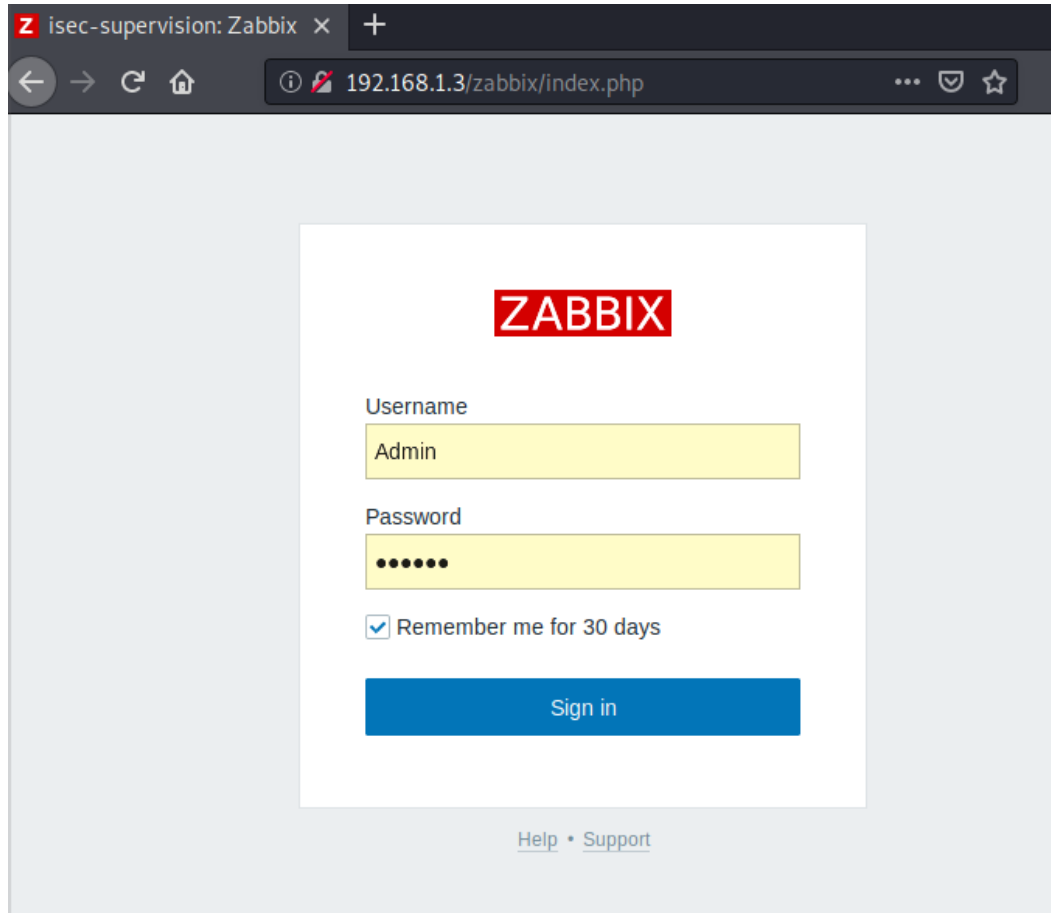
---

- Renseignement des informations pour la base de données



Au moment de se connecter, on utilise comme nom d'utilisateur **Admin** et comme mot de passe **zabbix**

# RAPPORT TECHNIQUE



isec-supervision: Zabbix x +

192.168.1.3/zabbix/index.php

**ZABBIX**

Username  
Admin

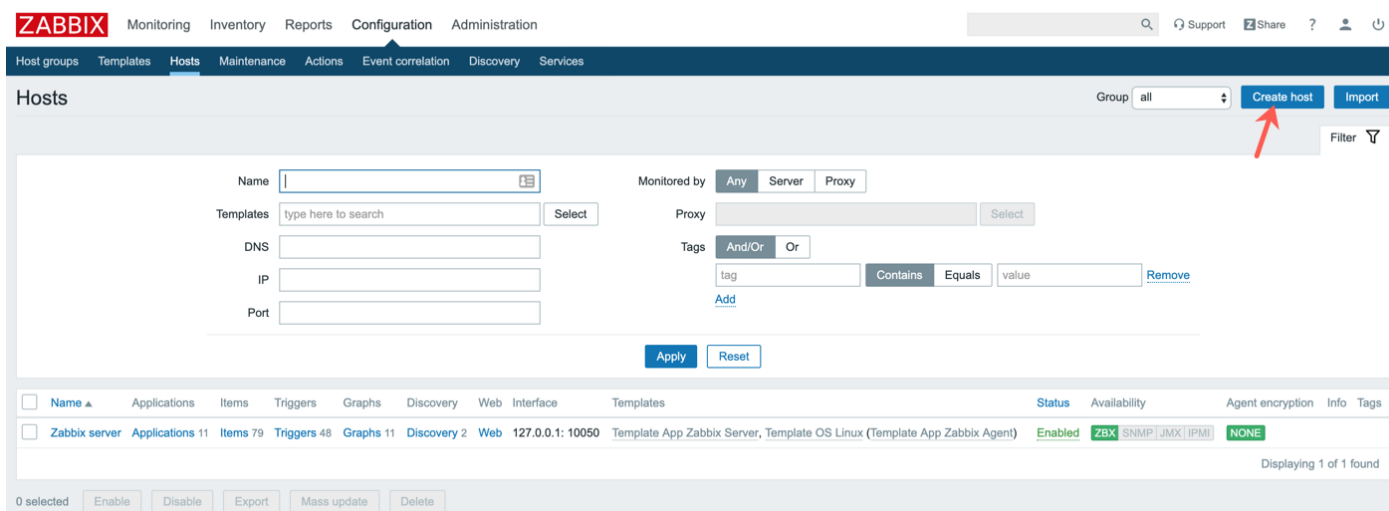
Password  
•••••

☒ Remember me for 30 days

Sign in

[Help](#) • [Support](#)

- Ensuite il faut ajouter des machines à monitorer. Aller sur le menu **configuration** ensuite **hôtes** et enfin cliquer sur **créer hôte**



**ZABBIX** Monitoring Inventory Reports Configuration Administration

Host groups Templates **Hosts** Maintenance Actions Event correlation Discovery Services

Hosts Group: all [Create host](#) [Import](#) Filter

Name:  Monitored by: ☐ Any ☐ Server ☐ Proxy

Templates:  Select Proxy:  Select

DNS:  Tags: ☐ And/Or ☐ Or

IP:  tag:  Contains Equals value:  Remove

Port:  Add

Apply Reset

<input type="checkbox"/>	Name	Applications	Items	Triggers	Graphs	Discovery	Web	Interface	Templates	Status	Availability	Agent encryption	Info	Tags	
<input type="checkbox"/>	Zabbix server	Applications 11	Items 79	Triggers 48	Graphs 11	Discovery 2	Web	127.0.0.1: 10050	Template App Zabbix Server, Template OS Linux (Template App Zabbix Agent)	Enabled	ZBX	SNMP	JMX	IPMI	NONE

0 selected Enable Disable Export Mass update Delete

Displaying 1 of 1 found

---

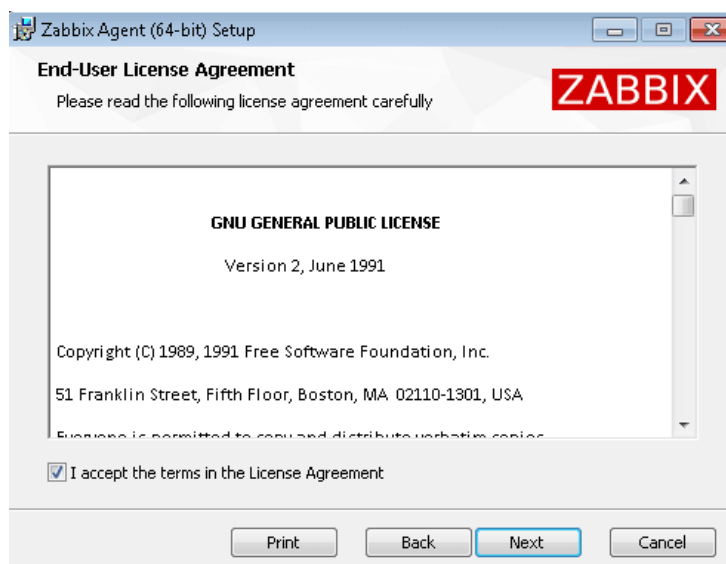
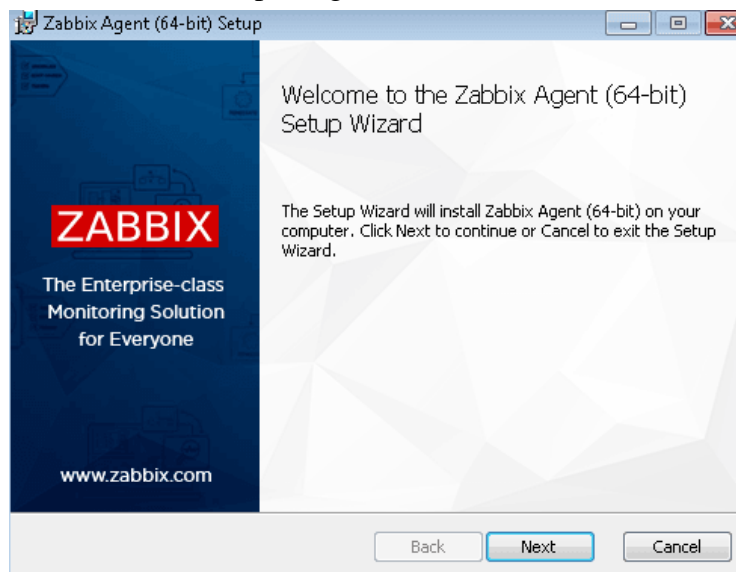
# RAPPORT TECHNIQUE

---

## Configuration du client Zabbix

La configuration du client Zabbix est assez simple, elle se fait avec un package .msi comme suit

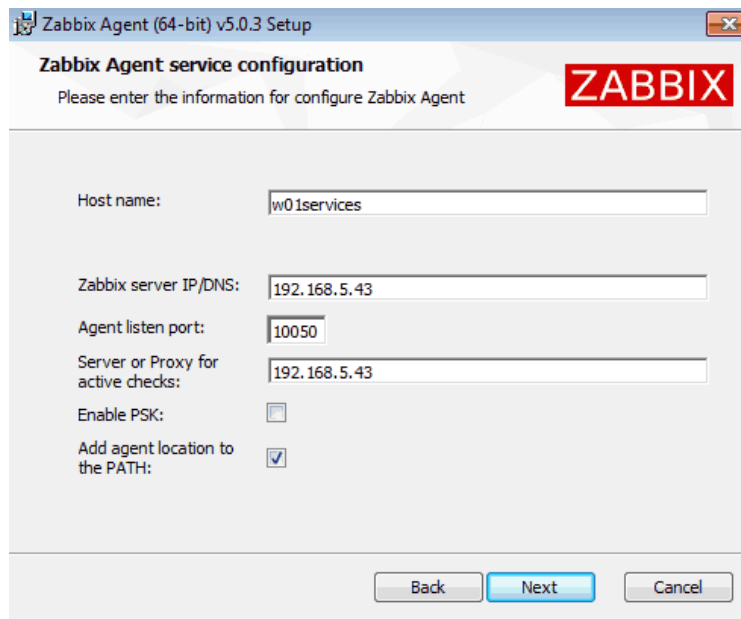
- Faire un double clic sur le package msi



---

# RAPPORT TECHNIQUE

---



**Zabbix Agent (64-bit) v5.0.3 Setup**

**Zabbix Agent service configuration**  
Please enter the information for configure Zabbix Agent

**Host name:** w01services

**Zabbix server IP/DNS:** 192.168.5.43

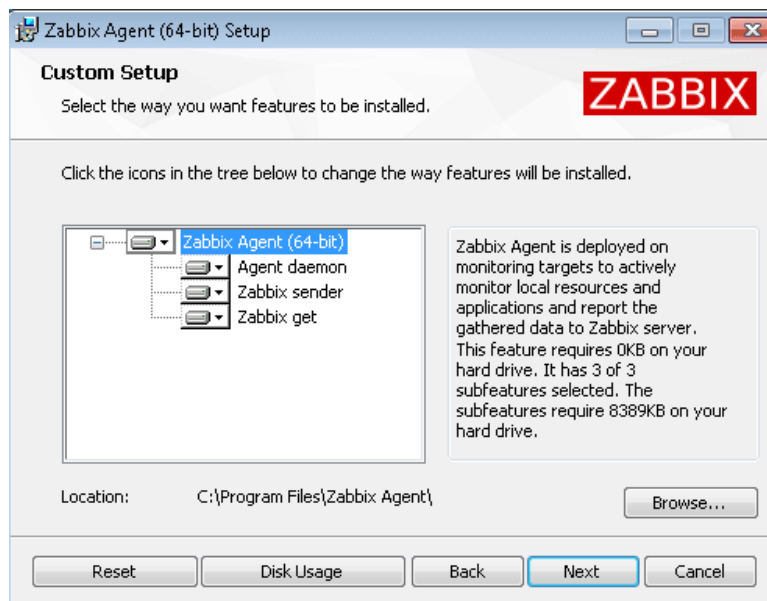
**Agent listen port:** 10050

**Server or Proxy for active checks:** 192.168.5.43

**Enable PSK:** ☐

**Add agent location to the PATH:** ☒

Back Next Cancel



**Zabbix Agent (64-bit) Setup**

**Custom Setup**  
Select the way you want features to be installed.

Click the icons in the tree below to change the way features will be installed.

**Feature Tree:**

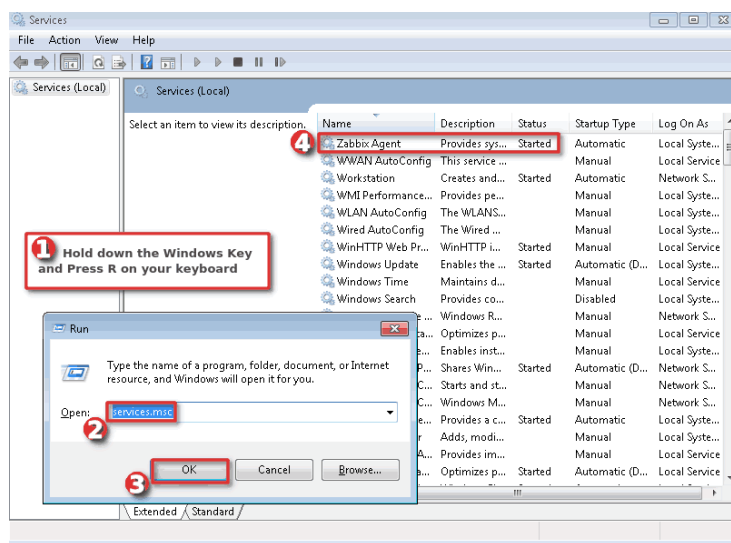
- Zabbix Agent (64-bit)
  - Agent daemon
  - Zabbix sender
  - Zabbix get

**Description:** Zabbix Agent is deployed on monitoring targets to actively monitor local resources and applications and report the gathered data to Zabbix server. This feature requires 0KB on your hard drive. It has 3 of 3 subfeatures selected. The subfeatures require 8389KB on your hard drive.

**Location:** C:\Program Files\Zabbix Agent\ Browse...

Reset Disk Usage Back Next Cancel

# RAPPORT TECHNIQUE



## 9. Création de la Relation d'approbation

Pour se faire nous avons suivi les étapes suivantes :

- ❖ Faire un clic droit sur le nom du serveur et choisir Propriétés
- ❖ Dans l'onglet Redirecteurs, ajouter l'adresse IP de l'autre machine et valider.
- ❖ Dans le Centre de domaine et approbations Active Directory, aller dans les propriétés du serveur.
- ❖ Créer une nouvelle approbation et renseigner le nom de domaine de l'autre machine
- ❖ Conserver la relation à sens unique

## 10. Installation et configuration de ISEC Groupe Réplica »

Le réplica comme l'indique son nom, Il s'agit de la copie du serveur principal d'ISEC **Groupe**. Il présente les mêmes fonctionnalités de ce dernier et servira de remplaçant en cas de pannes au niveau du serveur primaire.

Vu qu'il représente le serveur secondaire, il doit être mentionné lors de ses configurations plus précisément lorsqu'on va promouvoir le serveur en contrôleur de domaine.

## III. Justification des choix techniques

---

# RAPPORT TECHNIQUE

---

## 1. Choix des outils de supervision

Aussi appelée monitoring informatique (en abus de langage), la supervision permet de contrôler, surveiller et piloter le système d'information, élément central de l'activité des différents services de l'entreprise. Et pour être performante, toute TPE, PME ou grande structure est entièrement dépendante de son système informatique, notamment de son infrastructure informatique, qui doit fonctionner de façon optimale et permanente. La moindre anomalie peut ralentir sa progression, causer une perte de chiffre d'affaires ou même paralyser la production. Dans un monde en constante évolution, une perte d'efficacité n'est pas envisageable.

**La supervision informatique** est une technique mêlant :

- ❖ Surveillance,
- ❖ Suivi,
- ❖ Pilotage,
- ❖ Alertes,
- ❖ Rapports,

Elle doit répondre aux préoccupations suivantes :

- ❖ **Techniques** : surveillance de l'infrastructure informatique, dont :
  - Le réseau : disponibilité des services en ligne, débits, sécurité, contrôle des flux,
  - Les composants matériels,
  - Le système d'exploitation,
  - Le système de stockage des données,
- ❖ **Fonctionnelles (ou Services)** : surveillance des machines informatiques et de production, notamment de leur rendement, avec indicateurs, alertes, sondes, etc.,
- ❖ **Applications** : suivi des applications et de leur disponibilité.

Il existe alors de nombreux outils de supervision, parmi lesquels on peut citer :

- ❖ NAGIOS
- ❖ CENTREON
- ❖ CACTI
- ❖ MUNIN

---

# RAPPORT TECHNIQUE

---

## ❖ ZABBIX

Chacun de ses outils présente des avantages et des inconvénients. Le tableau ci-après présente un récapitulatif :

CRITÈRES DE COMPARAISON	MUNIN	CACTI	ZABBIX	CENTRON	NAGIOS
Gestion d'authentification et de rôles	NON	OUI	OUI	OUI	OUI
Création des graphes simple à partir des mesures	OUI	OUI	OUI	OUI	NON
Création des graphes complexes avec mise en relation des métriques des services monitorés	OUI	OUI	OUI	NON	NON
Utilisation d'agents sur les machines cibles	OUI	NON	OUI	OUI	OUI
Monitoring d'instances Windows	OUI	OUI	OUI	OUI	OUI
Reporting de la qualité de service en vue d'un rapport pour les SLA	NON	NON	OUI	OUI	OUI

---

# RAPPORT TECHNIQUE

---

Possibilité de mettre en place simplement un monitoring distribué	NON	NON	NON	OUI	NON
Fonctionnalité de supervision avancée : escalade, plages horaires	NON	NON	OUI	OUI	OUI
Utilisation de RRDtool	OUI	OUI	NON	OUI	NON

Notre choix est porté sur l'outil **ZABBIX** Pour tous ses avantages cités plus haut.

## 2. Choix de l'hyperviseur

Un hyperviseur est une plate-forme de virtualisation qui permet à plusieurs systèmes d'exploitation de travailler sur une même machine physique en même temps. Le choix de notre outil de supervision s'est fait entre **VMware** et **VirtualBox** dont le tableau comparatif ci-après.



---

# RAPPORT TECHNIQUE

---

CRITÈRE COMPARAISON	DE	VMWARE	VIRTUALBOX
Version		Player : gratuite, Workstation pro : payante	Gratuit, et Open Source
Performance		Performante notamment grâce à ses versions pro du logiciel, nécessite souvent plus en termes de ressources matérielle	Performance, moins gourmande en ressources matérielles
Interface utilisateur		Beaucoup plus compliqué les éléments menus sont nommés avec des termes technique	Interface simple et propre car les paramètres sont divisés.

**VirtualBox** est clairement le gagnant. Il est gratuit, sans tracas et riche en fonctionnalités. C'est la première chose à considérer pour les besoins de virtualisation des postes de travail. Bien que VMware domine le marché des entreprises, pour les cas d'utilisation strictement de bureau, il est facilement surpassé par **VirtualBox**.

## IV. Conclusion

En somme, notre travail qui consistait à mettre en place une architecture d'annuaire sous Windows server et une réplication sous WINDOWS server a été réalisée avec succès.

Nous avons pu réaliser l'architecture d'annuaire sous Windows Server et une réplication sur Windows également.