

Titre de l'activité N°2 : Installation des serveurs AD/DNS

Intitulé Activité Type de référence.		
Compétence(s) Evaluée(s).		
Durée effective de l'activité.		
Conditions de réalisation	En autonomie	En équipe
	X	

Description de l'activité.

I. Contexte :

Installation des serveurs Active Directory et DNS sur notre sandbox.

II. Matériel mis en œuvre :

MATERIEL	LOGICIELS ET DOCUMENTATIONS
<p>Serveur Lenovo ThinkStation P320 (Windows Server 2016)</p>	<p>Gestionnaire de serveur Gestionnaire Hyper-V Windows Server 2016 + ISO Documentation Msft PowerShell</p>

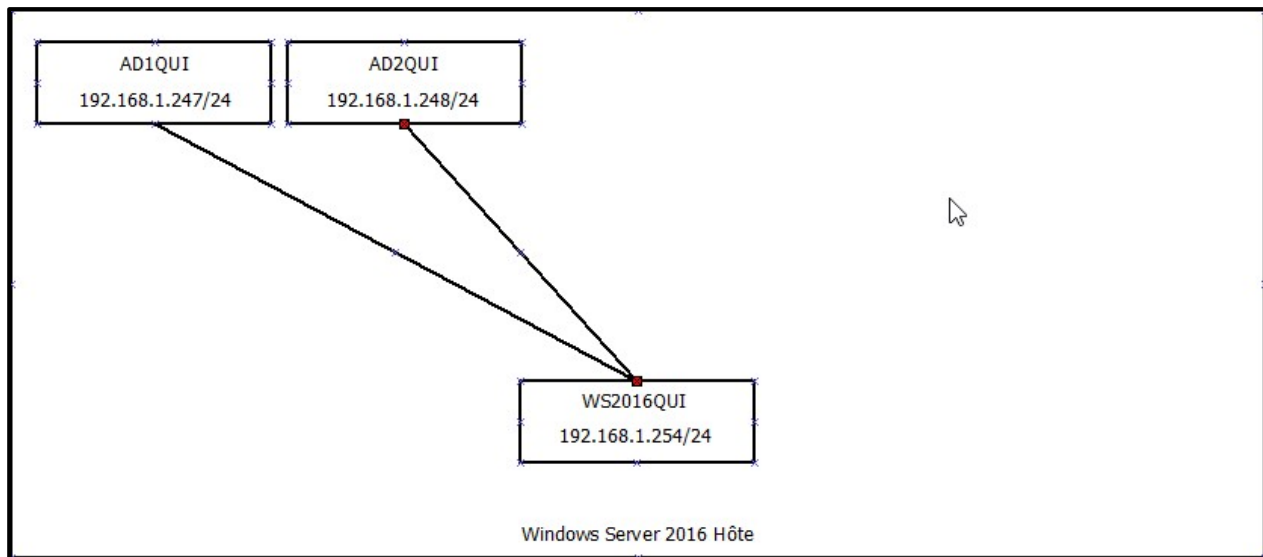
III. Consignes de réalisation :

Installer et configurer deux serveurs Active Directory et DNS qui travailleront de pair.

IV. Résultats attendus :

Pouvoir joindre un domaine sur nos VM et les gérer depuis un Windows Server 2016 en mode graphique.

V. Plan de l'infrastructure réseau mise en œuvre :



VI. Principales étapes de réalisation :

1 – Qu'est-ce que DNS ?

DNS est un service utilisé pour traduire des noms de domaines en adresse IP. C'est un composant essentiel d'Active Directory (qui travaille grâce aux noms de domaine).

2 – Qu'est-ce qu'Active Directory ?

Active Directory (AD) est un service d'annuaire Microsoft utilisant le protocole LDAP (Lightweight Directory Access Protocol). Il permet, entre autres, de centraliser l'identification et l'authentification des objets (ordinateurs, utilisateurs, etc...) d'un réseau informatique, améliorant ainsi la sécurité et la disponibilité des ressources du dit réseau.

3 – Préparation de l'environnement Active Directory :

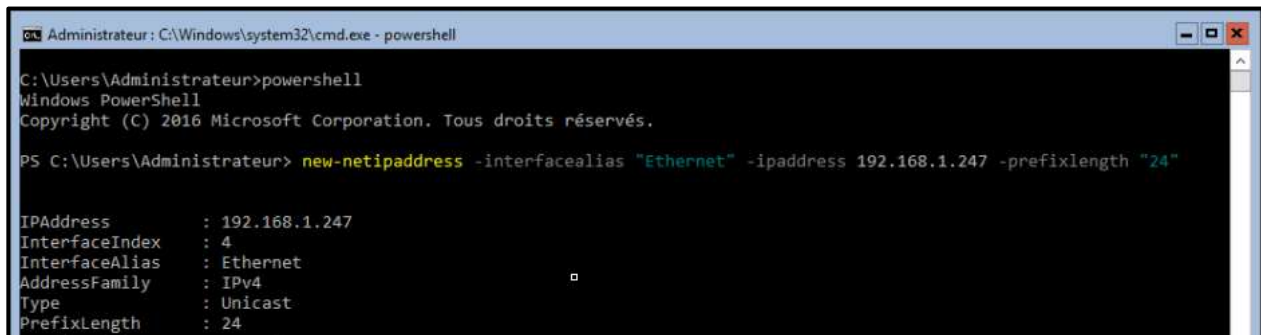
Notre environnement AD sera installé sur deux serveurs différents. L'un d'eux sera notre serveur AD/DNS principal, et sera répliqué sur l'autre de façon à assurer la continuité du service en cas d'indisponibilité du premier.

Nous allons pour ce faire créer deux VM sur notre machine hôte (*cf. FA 1 – Installation du rôle Hyper-V*), et installer Windows Server 2016 en mode **Core** (lors de l'installation, sélectionner une version sans **Expérience utilisateur**). Le mode Core est choisi afin d'optimiser les ressources de nos serveurs et de limiter leur surface d'attaque.

Une fois les deux VM fonctionnelles, en choisir une qui sera notre serveur principal et le configurer comme suit (penser à utiliser **Powershell** en tapant simplement *powershell* dans l'invite de commande) :

```
new-netipaddress -interfacealias "Ethernet" -ipaddress 192.168.1.247 -prefixlength "24"
```

Utiliser la commande *get-netipinterface* pour connaître le nom de l'interface réseau à configurer. Cette commande renseigne la configuration IPv4 de notre NIC en 192.168.1.247/24.



```
Administrateur: C:\Windows\system32\cmd.exe - powershell
C:\Users\Administrateur>powershell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. Tous droits réservés.

PS C:\Users\Administrateur> new-netipaddress -interfacealias "Ethernet" -ipaddress 192.168.1.247 -prefixlength "24"

IPAddress      : 192.168.1.247
InterfaceIndex  : 4
InterfaceAlias  : Ethernet
AddressFamily   : IPv4
Type            : Unicast
PrefixLength    : 24
```

```
set-dnsclientserveraddress -interfacealias "Ethernet" -serveraddresses ("192.168.1.247","192.168.1.248")
```



```
Administrateur: C:\Windows\system32\cmd.exe - powershell
SkipAsSource    : False
PolicyStore     : PersistentStore

PS C:\Users\Administrateur> set-dnsclientserveraddress -interfacealias "Ethernet" -serveraddresses ("192.168.1.247","192.168.1.248")
PS C:\Users\Administrateur> _
```

Nous renseignons ainsi les serveurs **DNS** de notre réseau.

Ouvrir ensuite le **Gestionnaire de serveur** grâce à *sconfig* et choisir l'option 7.

```

Administrateur: C:\Windows\system32\cmd.exe - sconfig
Inspection en cours du système...

=====
Configuration du serveur
=====

1) Domaine ou groupe de travail :      Domaine: rquinzio.lan
2) Nom d'ordinateur :                  ADIQUI
3) Ajouter l'administrateur local
4) Configurer l'administration à distance      Activé
5) Paramètres de Windows Update :          DownloadOnly
6) Télécharger et installer les mises à jour    Désactivé
7) Bureau à distance :
8) Paramètres réseau
9) Date et Heure
10) Paramètres de télémétrie              Renforcée
11) Activation de Windows
12) Fermer la session utilisateur
13) Redémarrer le serveur
14) Arrêter le serveur
15) Quitter pour revenir à la ligne de commande

Entrez un nombre pour sélectionner une option : 7
  
```

Puis **A** pour activer le **Bureau à distance**.

```

15) Quitter pour revenir à la ligne de commande

Entrez un nombre pour sélectionner une option : 7

(A)ctiver ou (D)ésactiver le Bureau à distance ? (Vide=Annuler) A
  
```

Enfin **1** pour sécuriser notre accès distant. Quitter ensuite sconfig avec **15**.

```

(A)ctiver ou (D)ésactiver le Bureau à distance ? (Vide=Annuler) A

1) Autoriser seulement les clients exécutant le Bureau à distance avec authentification NLA (plus sécurisé)
2) Autoriser les clients exécutant n'importe quelle version du Bureau à distance (moins sécurisé)

Entrez la sélection : 1
  
```

Nous allons ensuite modifier certaines règles du **Pare-feu Windows** afin de rendre gérable notre serveur depuis une autre machine grâce aux commandes suivantes :

```

set-netfirewallrule -displaygroup "Gestion à distance de Windows"
set-netfirewallrule -displaygroup "Bureau à distance"
  
```


```

Administrateur: C:\Windows\system32\cmd.exe - powershell
PS C:\Users\Administrateur> Enable-NetFirewallRule -DisplayGroup "Gestion à distance de Windows"
PS C:\Users\Administrateur> Enable-NetFirewallRule -DisplayGroup "Bureau à distance"
  
```

La commande *get-netfirewallrule* est très utile pour connaître les groupes à modifier.

Nous allons ensuite **renommer** notre machine avec :

rename-computer -newname "AD1QUI" -restart



```
Administrateur : C:\Windows\system32\cmd.exe - powershell
PS C:\Users\15admin> rename-computer -newname "AD1QUI" -restart
```

L'ordinateur redémarre automatiquement. Au prochain démarrage, son nom sera AD1QUI.

Appliquer la même méthode sur notre second serveur, avec une adresse IPv4 192.168.1.248, et en nom de machine AD2QUI.

4 – Installation d'Active Directory et jonction au domaine :

Retournons sur notre machine AD1QUI, sur laquelle nous allons installer **Active Directory** et notre première forêt de domaines. Pour ce faire, nous allons lancer **PowerShell** dans l'invite de commande ouverte, et entrer les commandes ci-dessous :

install-windowsfeature -name "ad-domain-services" -includemanagementtools
install-addsforest -domainname rquinzio.lan

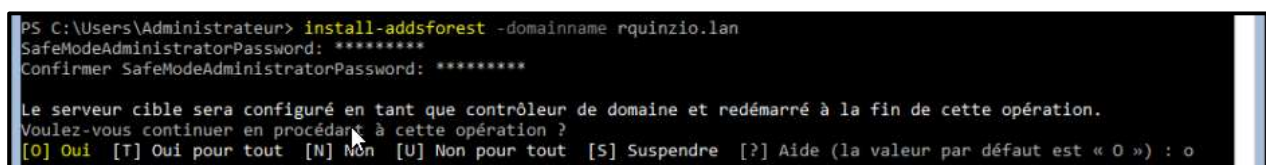


```
PS C:\Users\Administrateur> install-windowsfeature -name "ad-domain-services" -includemanagementtools
Success Restart Needed Exit Code      Feature Result
-----
True    No          Success      {Services AD DS, Gestion de stratégie de g...

PS C:\Users\Administrateur> install-addsforest -domainname rquinzio.lan
SafeModeAdministratorPassword: *****
```

Un mot de passe de récupération sera demandé (**SafeModeAdministratorPassword**). Ce mot de passe sera utilisé en cas d'utilisation du mode DSMR, pour, par exemple, mettre un serveur AD hors-ligne lors d'une maintenance d'urgence.

Valider l'installation de la forêt avec **O**. Le serveur redémarre automatiquement. L'installation d'AD/DNS et de notre forêt est terminée et notre serveur est automatiquement promu en **Contrôleur de domaine**.



```
PS C:\Users\Administrateur> install-addsforest -domainname rquinzio.lan
SafeModeAdministratorPassword: *****
Confirmer SafeModeAdministratorPassword: *****

Le serveur cible sera configuré en tant que contrôleur de domaine et redémarré à la fin de cette opération.
Voulez-vous continuer en procédant à cette opération ?
[O] Oui [T] Oui pour tout [N] Non [U] Non pour tout [S] Suspendre [?] Aide (la valeur par défaut est « O ») : o
```

Nous retournons ensuite sur notre machine AD2QUI pour la joindre au **domaine** avec la commande suivante :

add-computer -domainname rquinzio.lan -credential rquinzio.lan\administrateur -restart



Le mot de passe de l'**Administrateur du domaine** sera demandé. Comme l'installation d'AD s'est faite avec l'administrateur local d'AD1QUI, c'est ce compte qui est de facto Administrateur du domaine. Nous indiquerons donc son mot de passe. L'ordinateur redémarrera automatiquement et sera inscrit dans le domaine.

Enfin, nous passons sur notre première VM Windows Server créée (cf. FA 1 – *Installation du rôle Hyper-V*). C'est cette machine qui nous servira à gérer tous nos serveurs en mode graphique. Pratique, non ?

Pour ce faire, lui appliquer une configuration réseau en 192.168.1.254/24 avec pour serveurs DNS 192.168.1.247 et 192.168.1.248 grâce aux commandes vues précédemment. La renommer ensuite en WS2016QUI et la joindre au domaine rquinzio.lan.

5 – Installation du serveur AD/DS secondaire :

Sur WS2016QUI, se connecter avec le compte **Administrateur du domaine**.



Lancer une console **PowerShell**, puis entrer les commandes suivantes :

```
install-windowsfeature -name rsat-adds
install-windowsfeature -name rsat-dns-server
```



```

Administrateur : Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. Tous droits réservés.

PS C:\Users\administrateur.RQUINZIO> install-windowsfeature -name rsat-adds

Success Restart Needed Exit Code      Feature Result
-----
True      No             Success      {Outils d'administration de serveur distan...

PS C:\Users\administrateur.RQUINZIO> install-windowsfeature -name rsat-dns-server

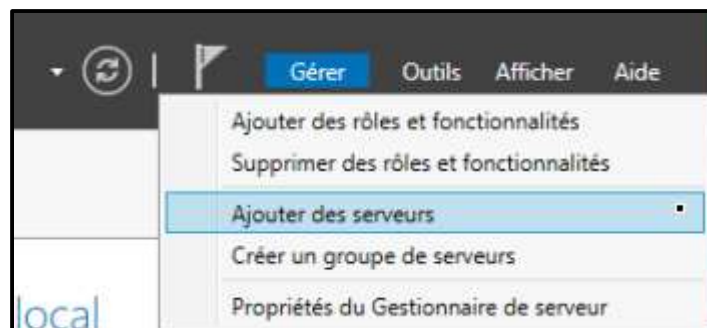
Success Restart Needed Exit Code      Feature Result
-----
True      No             Success      {Outils du serveur DNS}

PS C:\Users\administrateur.RQUINZIO>
  
```

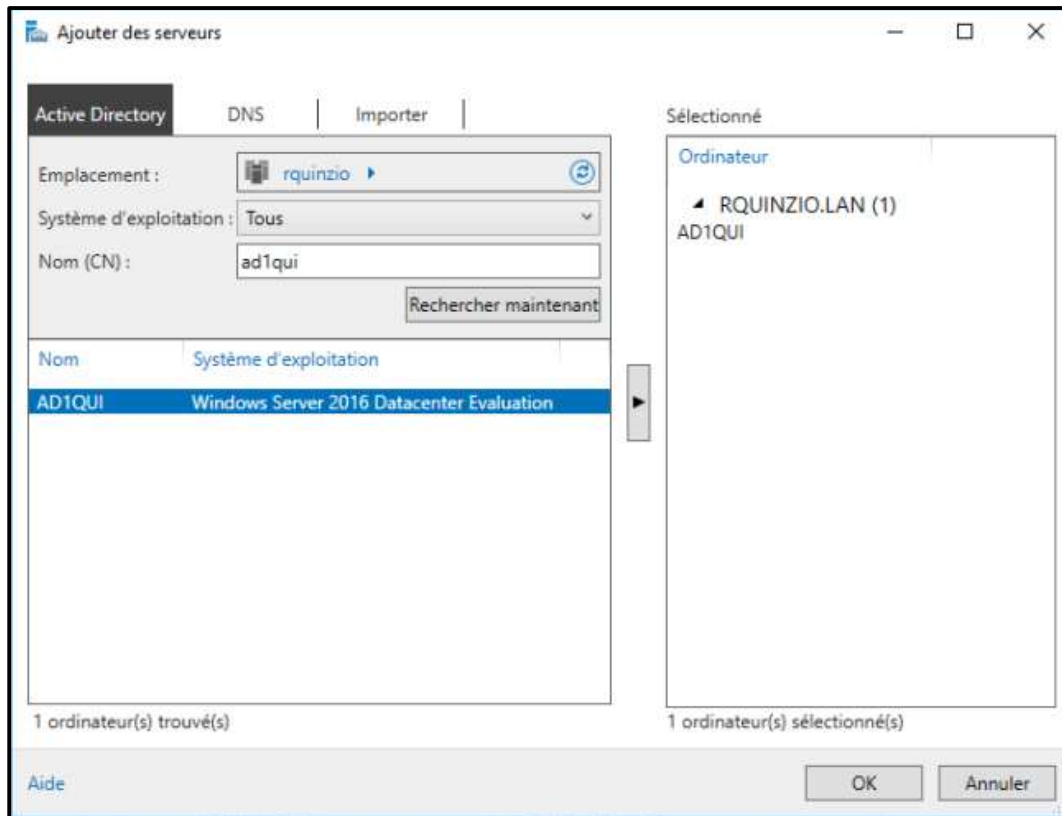
Ces commandes permettent l'installation des outils **RSAT** (Remote Server Administration Tools) pour AD et DNS.

Nous allons ensuite ajouter nos deux serveurs Core dans le Gestionnaire de serveur de WS2016QUI, afin d'y disposer d'un accès permanent.

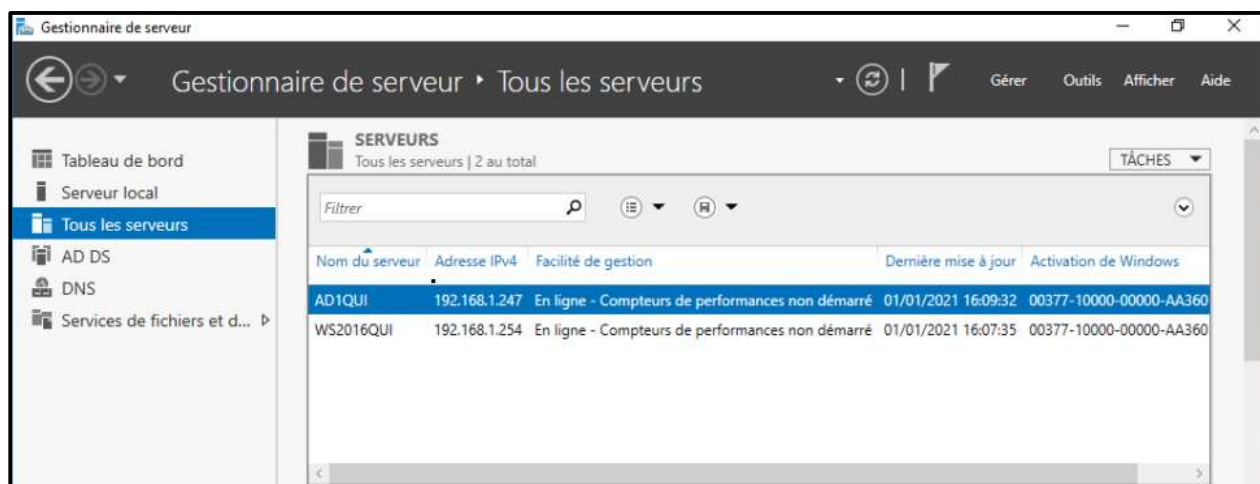
Dans le **Gestionnaire de serveur**, cliquer sur **Gérer > Ajouter des serveurs**.



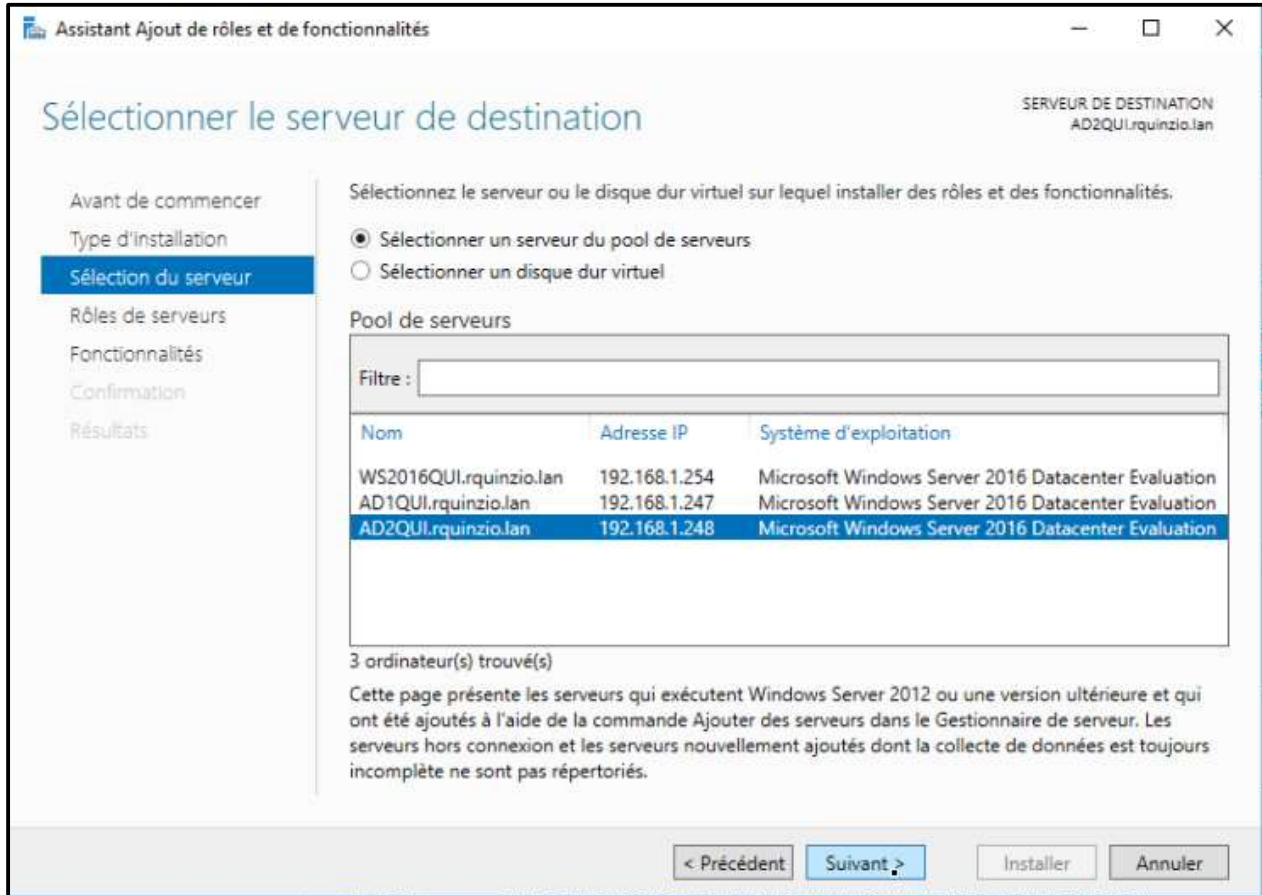
Dans la fenêtre nouvellement ouverte, onglet **Active Directory**, entrer le **nom canonique** (CN) de nos serveurs, dans notre cas AD1QUI, puis sélectionner le serveur et cliquer sur le bouton flèche du milieu pour l'ajouter. Procéder de la même façon pour AD2QUI et cliquer sur **OK**.



Nos serveurs apparaissent dans le panneau **Tous les serveurs** du Gestionnaire de serveur :



Nous allons ensuite installer AD et DNS sur AD2QUI. Pour ce faire, dans le **Gestionnaire de serveur** cliquer sur **Gérer > Ajouter des rôles et fonctionnalités**. Dans la liste des serveurs proposés choisir **AD2QUI**, puis cliquer sur **Suivant**.



Assistant Ajout de rôles et de fonctionnalités

Sélectionner le serveur de destination

SERVEUR DE DESTINATION
AD2QUI.rquinzio.lan

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats

Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.

☒ Sélectionner un serveur du pool de serveurs
☐ Sélectionner un disque dur virtuel

Pool de serveurs

Filtre :

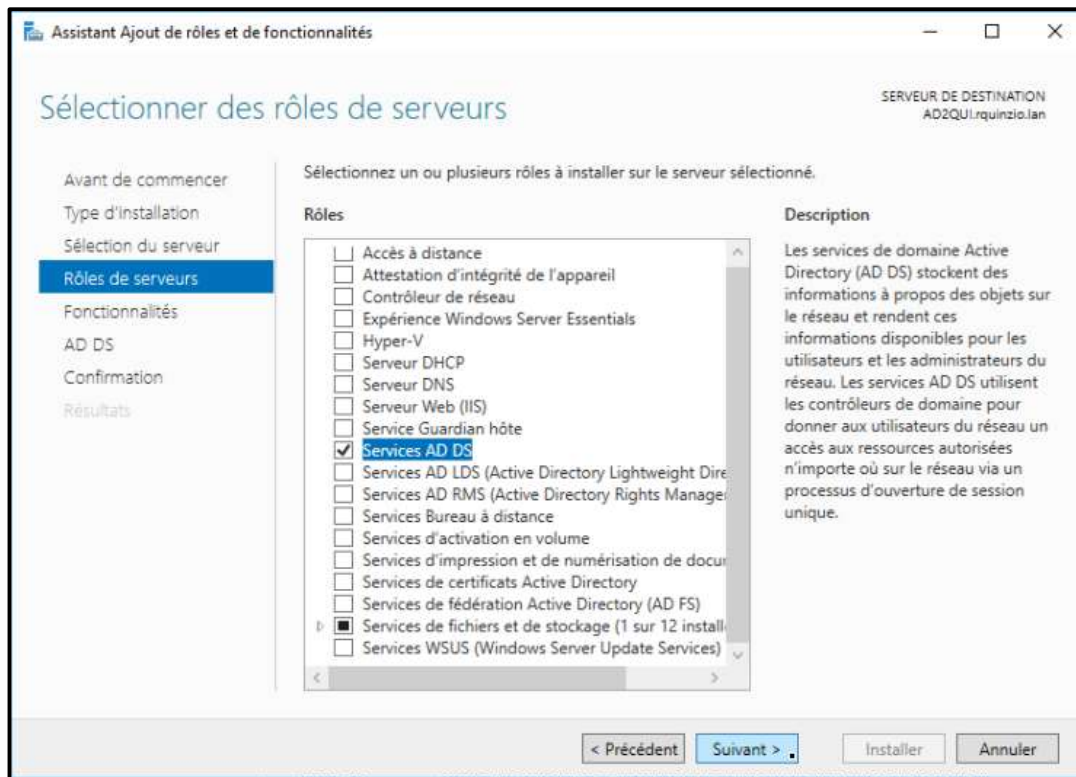
Nom	Adresse IP	Système d'exploitation
WS2016QUI.rquinzio.lan	192.168.1.254	Microsoft Windows Server 2016 Datacenter Evaluation
AD1QUI.rquinzio.lan	192.168.1.247	Microsoft Windows Server 2016 Datacenter Evaluation
AD2QUI.rquinzio.lan	192.168.1.248	Microsoft Windows Server 2016 Datacenter Evaluation

3 ordinateur(s) trouvé(s)

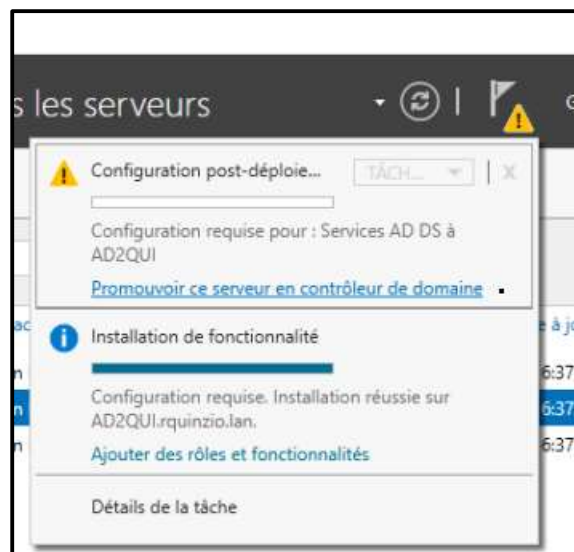
Cette page présente les serveurs qui exécutent Windows Server 2012 ou une version ultérieure et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors connexion et les serveurs nouvellement ajoutés dont la collecte de données est toujours incomplète ne sont pas répertoriés.

< Précédent Suivant > Installer Annuler

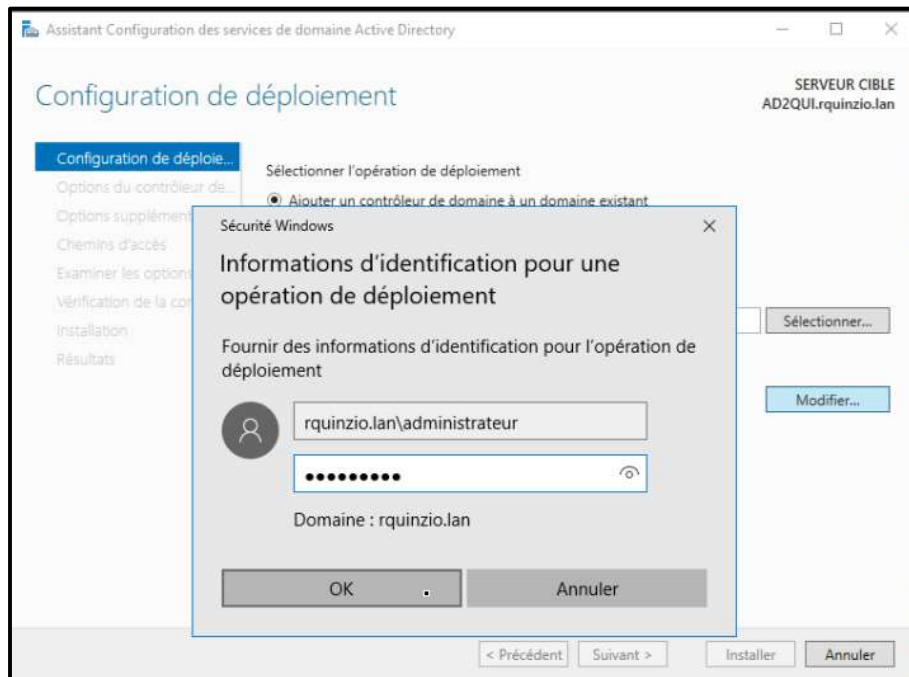
Sélectionner le rôle **Services AD DS** et cliquer sur **Suivant**.



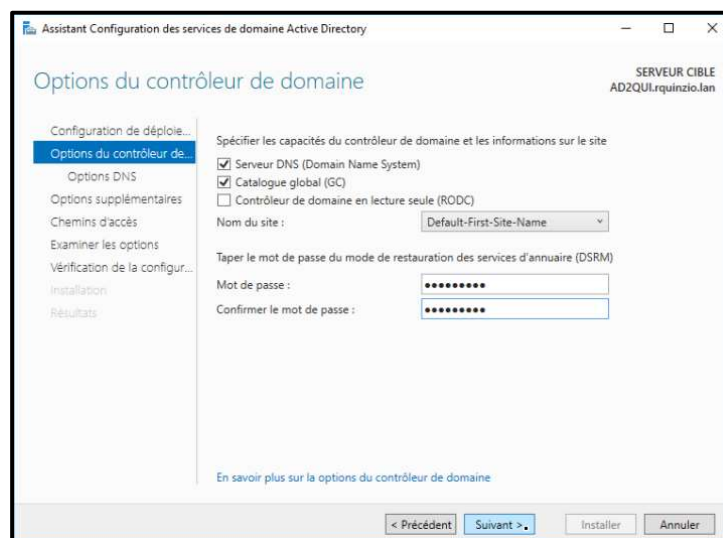
Une fois l'installation terminée, nous devons retourner sur notre **Gestionnaire de serveur** et cliquer sur l'**icône de notification** pour promouvoir ce serveur en **Contrôleur de domaine** (DC – Domain Controller).



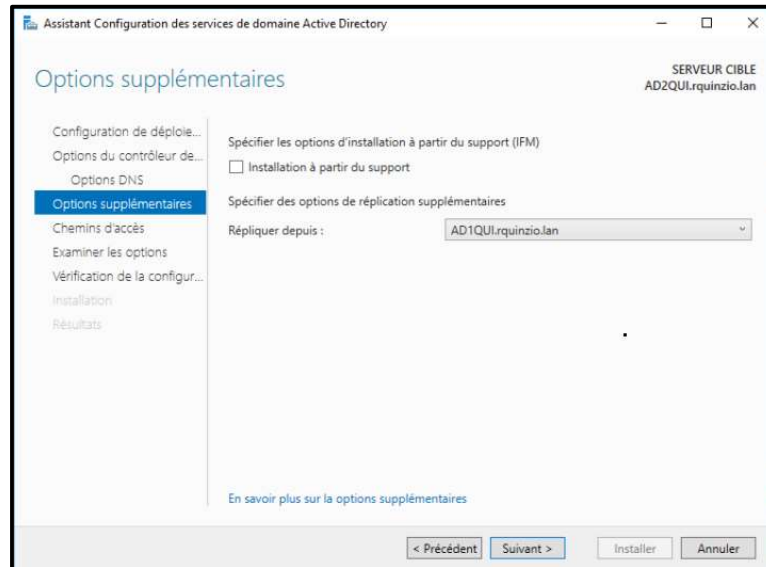
La fenêtre de Configuration de déploiement s'ouvre alors. Sélectionner **Ajouter un contrôleur de domaine à un domaine existant**, entrer le **nom de domaine** rquinzio.lan et modifier les informations d'identification pour qu'elles correspondent à celle de notre **Administrateur de domaine**. Cliquer sur **Suivant**.



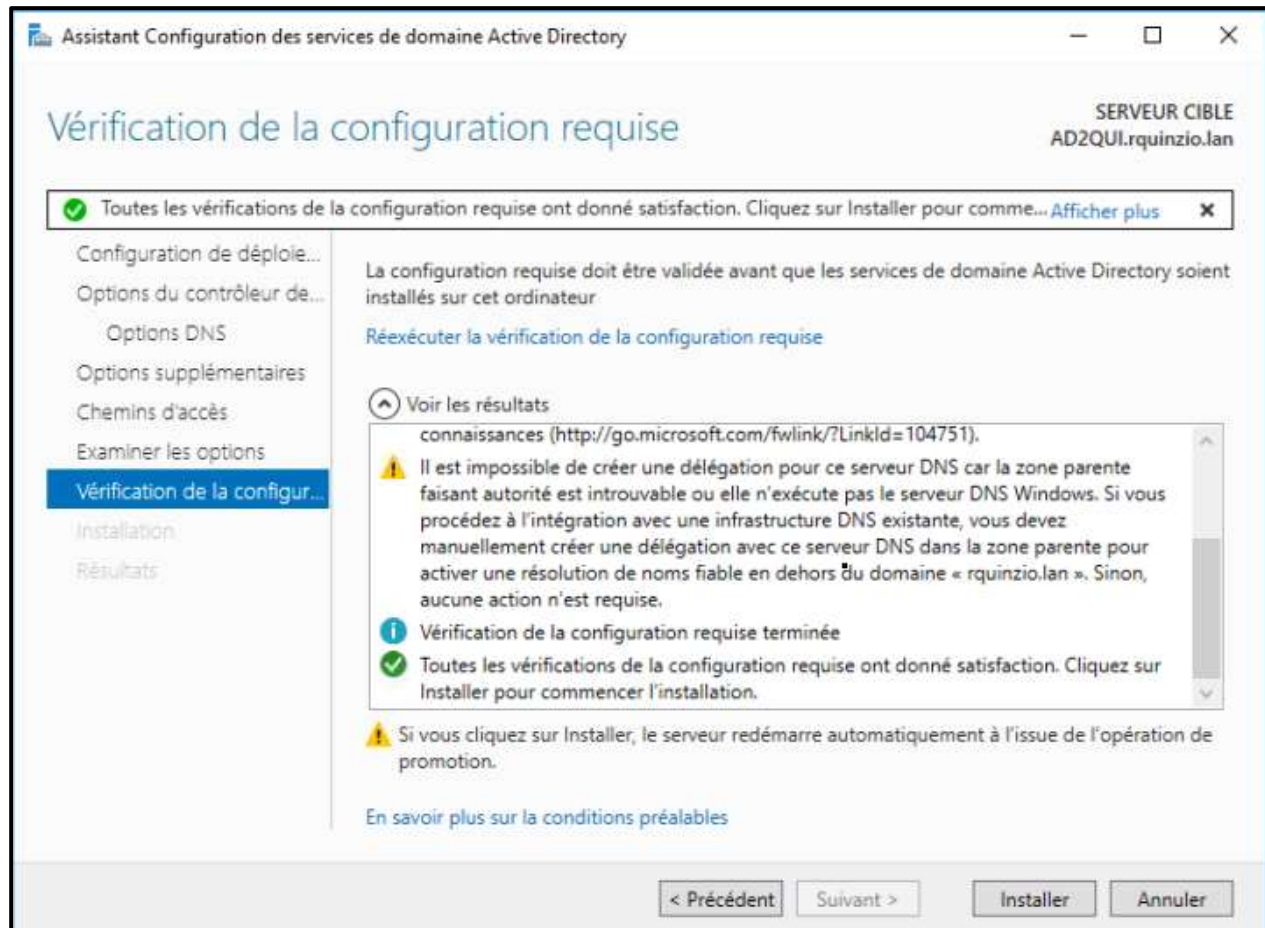
Dans les Options du DC, cocher **Serveur DNS** et **Catalogue global**. Dans notre cas, nous estimons que le serveur physique est protégé des utilisateurs indésirables et que nous serons seul administrateur réseau, il est donc inutile de mettre ce serveur en Lecture seule (RODC) et de se priver d'éventuelles facilités de gestion. Nous travaillons sur un seul site, nous pouvons donc laisser l'option par défaut dans Nom du site. Entrer un mot de passe pour **DSRM** et cliquer sur **Suivant**.



Dans les Options supplémentaires, choisir de **Répliquer depuis** notre **DC principal** et cliquer sur **Suivant**.



Laisser ensuite tous les paramètres **par défaut**. Une fois les vérifications de l'installation terminées, cliquer sur **Installer**. Le serveur AD2QUI redémarre automatiquement pour valider l'installation.

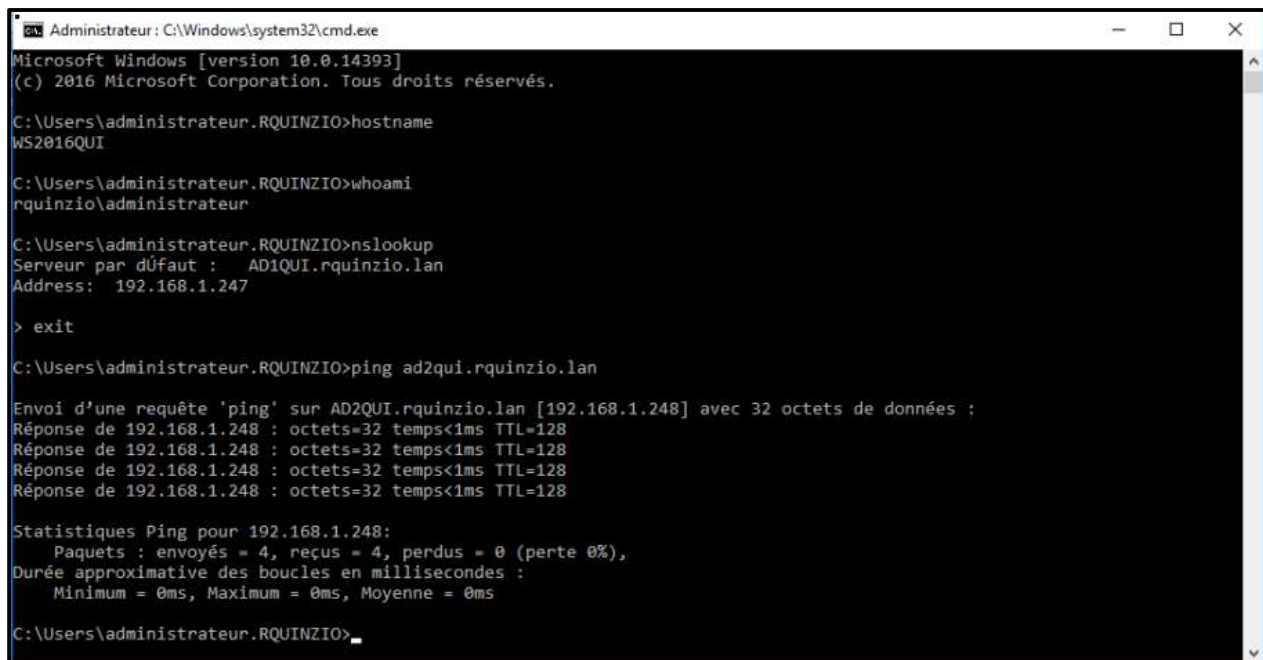


VII. Phase de validation :

Afin de valider l'installation, il faut s'assurer que le domaine soit bien fonctionnel en se connectant grâce à un compte utilisateur du domaine, et vérifier notre résolution DNS grâce à *nslookup*.

VIII. Bilan :

La connexion par le domaine et la résolution DNS sont fonctionnelles :



```
Administrateur: C:\Windows\system32\cmd.exe
Microsoft Windows [version 10.0.14393]
(c) 2016 Microsoft Corporation. Tous droits réservés.

C:\Users\administrateur.RQUINZIO>hostname
WS2016QUI

C:\Users\administrateur.RQUINZIO>whoami
rquinzio\administrateur

C:\Users\administrateur.RQUINZIO>nslookup
Serveur par défaut : AD1QUI.rquinzio.lan
Address: 192.168.1.247

> exit

C:\Users\administrateur.RQUINZIO>ping ad2qui.rquinzio.lan

Envoi d'une requête 'ping' sur AD2QUI.rquinzio.lan [192.168.1.248] avec 32 octets de données :
Réponse de 192.168.1.248 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.248 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.248 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.248 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.1.248:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\administrateur.RQUINZIO>
```




AFPA LORIENT



Nom : _____ Dates de réalisation : _____

Fiche d'évaluation.

Nom du tuteur	Fonction

CCP : N°

Evaluation de la compétence:...

Critères d'appréciation généraux		Validation	Critères d'évaluation spécifiques		Validation

V : validé. NV : Non validé. NE : Non évalué.

Observations du tuteur

--

Validation

<u>Entreprise</u>	<u>Centre de Formation AFPA</u>
Date : Signature du tuteur	Nom : Michel CHARRA Pris connaissance le : Signature du responsable pédagogique :

Observations du responsable pédagogique

--