

REMERCIEMENTS

Nous ne saurons entamer la rédaction de ce document toute fois sans exprimer notre profonde gratitude à toutes ses personnes avisées qui nous ont été d'une grande aide à quelque niveau que ce soit, personnes sans lesquelles l'élaboration de ce projet n'aurait pas eu lieu.

Nos remerciements vont tout d'abord à l'endroit de la Direction Exécutive du Programme PAC-CI, avec à sa tête le Dr Raoul MOH.

Ensuite, à l'endroit de :

- M. Célestin N'CHO, Chef du Service Informatique et Mme Adrienne ABOUA, Responsable des Ressources Humaines pour nous avoir permis d'intégrer l'entreprise et nous accordé leur confiance.
- M. Claude KORANDJI, notre encadreur pour la proposition du sujet, sa disponibilité, sa recommandation et ses précieux conseils.
- M. Dominique YAO, Responsable de la Hotline pour sa patience, son orientation et assistance.

Ainsi qu'à tout l'ensemble du personnel de PACCI, plus précisément le Service Informatique pour leur chaleureux accueil et encouragement.

DEDICACE

Du profond de mon cœur, je dédie ce travail à tous ceux qui me sont chers.

A MA CHÈRE MÈRE

Aucune dédicace ne saurait exprimer mon respect, mon amour éternel et ma considération pour les sacrifices que tu as consenti pour mon instruction et mon bien être.

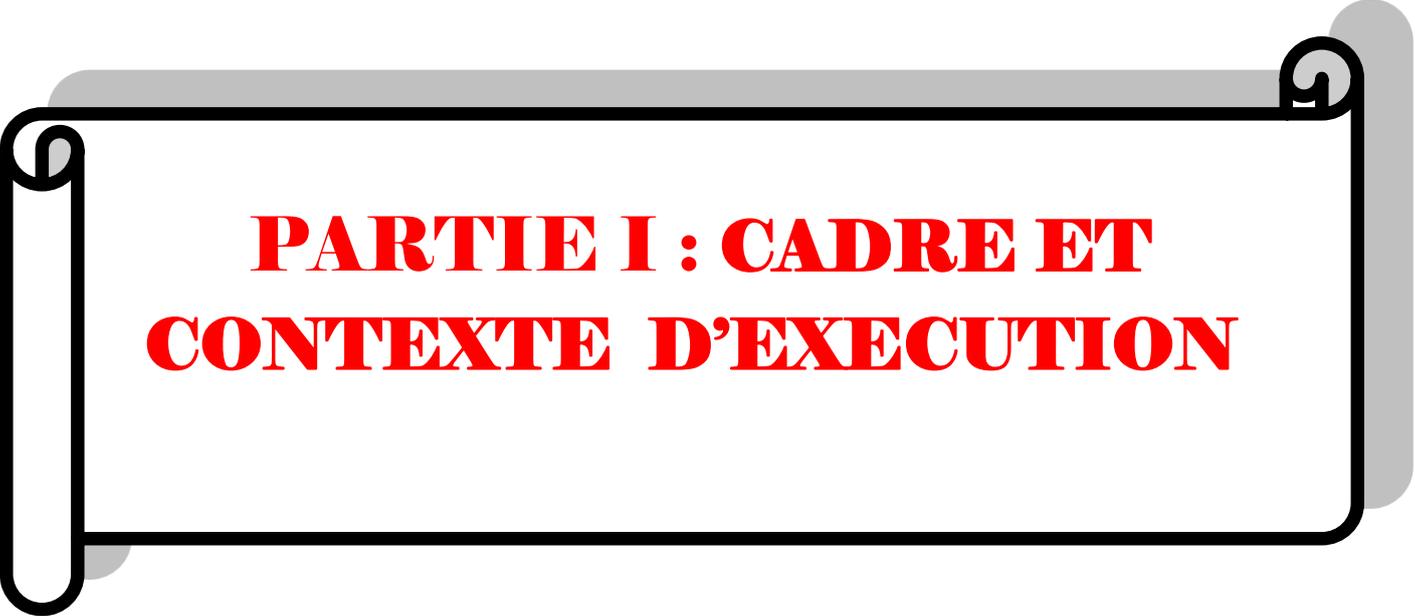
Je te remercie pour tout le soutien et l'amour que tu me porte depuis l'enfance et j'espère que ta bénédiction m'accompagne toujours. Que ce modeste travail soit l'exaucement de tes vœux tant formulés, le fruit de tes innombrables sacrifices.

Puisse Dieu, le très haut, t'accorder santé, bonheur et longévité.

A LA MEMOIRE DE MON PÈRE

Ce travail est dédié à mon père, électronicien et électrotechnicien, décédé trop tôt, qui m'a toujours poussé et motivé dans mes études. J'espère que, du monde qui est sien maintenant, il apprécie cet humble geste comme preuve de reconnaissance de la part d'un fils qui a décidé de suivre ces traces qu'il a laissé.

Puisse Dieu, le très haut, l'avoir en sa sainte miséricorde



**PARTIE I : CADRE ET
CONTEXTE D'EXECUTION**

CHAPITRE I : PRESENTATION DU CADRE D'ACCUEIL

I- HISTORIQUE

Le programme « PACCI/site ANRS de Côte d'Ivoire » a été ouvert en 1995, puis formalisé en 1996 par convention entre le Ministère ivoirien de la Santé, le Ministère ivoirien de l'Economie et des Finances, le Ministère français de la Coopération et l'ANRS. Cette convention fondatrice fixait deux objectifs :

- La formation du personnel de santé à la recherche médicale sur le VIH/SIDA ;
- La mise en œuvre de recherches médicales sur le VIH/SIDA dont les résultats devraient rapidement utiles aux personnes affectées par la maladie.

En 2010, les partenaires ivoiriens et français, jugent le bilan positif et consolident le programme PACCI par une révision de la convention élargit les missions du programme PACCI, dont l'objectif est maintenant de développer la recherche scientifique et médicale non seulement sur le VIH/SIDA mais aussi sur les autres maladies infectieuses.

En 2013, le développement institutionnel de PAC-CI s'est poursuivi de façon substantielle. Ainsi une convention de coopération a été signée le 6 novembre 2013 entre les différents partenaires suivants pour créer le tout premier Laboratoire International Associé (LIA-INSERM) en Afrique subsaharienne.

II- MISSIONS

Ses tâches sont basées sur trois thèmes prioritaires de recherche que sont :

- La prévention de la transmission du VIH de la mère à l'enfant,
- L'amélioration de la prise en charge de l'adulte infecté par le VIH,
- L'amélioration de la prise en charge de l'enfant infecté par le VIH.

Sur ceux-ci, les outils de recherche ont été d'abord épidémiologiques, cliniques et biologiques. Ensuite des années après, d'autres disciplines sont venues

appuyer les recherches sur ces thèmes, notamment la sociologie, l'anthropologie, l'économie et la modélisation.

III- ORGANISATION ET ROLES DES SERVICES

Le Programme PACCI est composé d'une « équipe centrale » inter-projets, et « d'équipes partenaires ».

A. EQUIPE CENTRALE

Hébergée dans les locaux du programme PACCI, dans l'enceinte du CHU de Treichville, elle est sous la coresponsabilité de deux Coordonnateurs (un ivoirien, dit Coordonnateur « Sud », et un français, dit Coordonnateur « Nord »), de deux Coordonnateurs adjoints, d'un Directeur Exécutif et d'un Directeur Exécutif adjoint.

Le Directeur est appuyé dans ses tâches par un comité administratif et une équipe de chercheurs :

❖ LE COMITE ADMINISTRATIF

- Un responsable administratif et financier
- Une responsable administrative
- Un responsable logistique
- Un responsable informatique

➤ Le Département Administratif et Financier

Ce département est dirigé par M. Abdoulaye CISSE, il pilote et participe aux missions, de planification, de gestion et de coordination des tâches administratives financières et comptable de la structure. Il est aidé dans ces tâches par Mlle Madikona DOSSO (Chef comptable). Il a pour rôle principal de :

- Contrôler de la comptabilité de l'entreprise ;
- Gérer la trésorerie ;
- Prévoir le financement des investissements et/ou Projets ;
- Assurer une veille sur l'évolution des lois et réglementations ;
- Superviser les relations avec les services fiscaux ;

- Assurer une permanence juridique et sociale ;
- Participer à l'administration du personnel ;
- Participer à la gestion des systèmes d'informations de l'entreprise.

➤ Le Département Ressources Humaines

La gestion des ressources humaines est la fonction organisationnelle du Programme PAC-CI. Elle est présidée par Mme Adrienne ABOUA, qui s'occupe du recrutement, de la gestion, du perfectionnement et de la motivation du personnel. Elle fournit de même du soutien, des systèmes fonctionnels et spécialisés pour favoriser la participation des employés ainsi que des systèmes de gestion pour favoriser le respect réglementaire des normes liées à l'emploi et aux droits du personnel.

➤ Le Département Logistique et Achats

Cette section est dirigée par M. Romuald KONAN. Il est épaulé dans l'exécution des tâches qui incombent à la section par une assistante Mlle Sylvie KONAN. Son rôle premier est de mettre à la disposition du personnel les moyens nécessaires pour arriver à travailler dans les conditions optimales. En plus de cela, il assure toutes les tâches qui composent la fonction achat dans une entreprise normale depuis la réception de l'expression des besoins jusqu'à satisfaction du demandeur. En effet il établit les demandes d'achat, lance les commandes, sélectionne-le(s) fournisseur(s) après confrontation des offres, réceptionne les commandes, procède à la vérification avant de les transmettre au service concerné.

➤ Le Département Informatique et Télécommunication

Cette section dirigée par M. Célestin N'CHOT, constitue l'un des piliers essentiels sur lequel repose la structure. La performance de son système lui permet

d'effectuer l'échange des données informatisées entre toutes les structures de recherche rattachées. La maintenance de ce système est assurée par le service informatique. Cette direction a en charge, le suivi, l'évolution et l'adaptation aux solutions informatiques implémentées par le groupe.

❖ **UNE EQUIPE DE CHERCHEUR**

- Deux chercheurs seniors de l'équipe, les chefs de projet appuyer eux aussi par :
- Quatre médecins moniteurs d'étude clinique
- Un biologiste, moniteur d'étude biologique
- Une équipe spécialisée en Gestion des données
- Cinq gestionnaires de bases de données/développeurs d'applications
- Un responsable technicien d'études clinique
- Une traductrice

B. EQUIPE PARTENAIRE

➤ **En Côte d'Ivoire**

- **Les trois CHU d'Abidjan** : le CHU de Treichville, le CHU de Yopougon et le CHU de Cocody.
- **Les quatre grands centres de soins extrahospitaliers spécialisés dans le VIH** :
 - Le Centre de Prise en charge et de Formation
 - Le Centre Médical de Suivi des Donneurs de Sang
 - Le Centre Intégré de Recherches Biocliniques d'Abidjan
 - L'Unité de Soins Ambulatoires et de Conseil
- **Des structures de soins générales autres que les CHU** : les hôpitaux généraux de Yopougon et d'Abobo Nord.

➤ **En France**

- **A Bordeaux** : Le Centre Inserm, Institut de Santé Publique Epidémiologie et Développement

- **A Montpellier** : L'Université de Montpellier
- **A Nantes** : L'Hôpital Laennec

➤ **En Afrique**

Burkina Faso: CHU Salado Ouédraogo, CHU Souro Sanou Bobo-Dioulasso

Cameroun : Hôpital Centrale de Yaoundé

Guinée : CHU Donka

Mali : CHU du Point G

Sénégal : le Centre Régional de Recherche et Formation

Ouganda: Mbarara University of Science and Technology

Tanzanie : NIMR

Togo : Le Laboratoire BIOLIM, Université de Lomé, CHU Sylvanus Olympio

➤ **En Asie**

Vietnam: Clinical research unit Pham Ngoc Thach Hospital

Cambodge: National Center for HIV/AIDS

➤ **En Amérique Latine**

Brésil: Laboratory on Clinical research on STD/AIDS – IPEC/FIOCRUZ

IV- ORGANIGRAMME

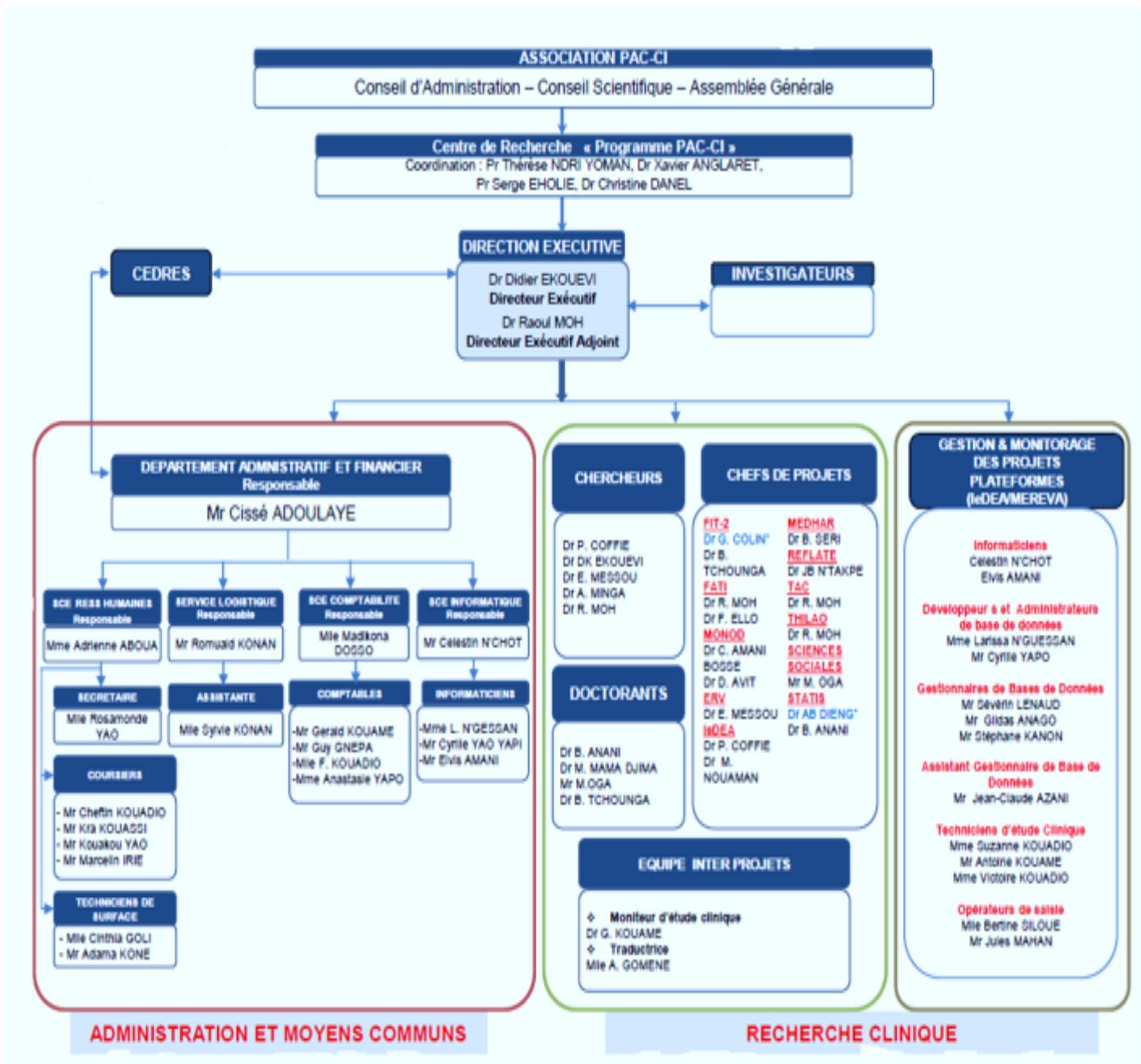


FIGURE I.1 : Organigramme générale du Programme PAC-CI

V- PRESENTATION DU SERVICE D'ACCUEIL

Notre travail a été effectué au sein du service informatique. Ce service est chargé d'automatiser les tâches des différents services pour une gestion plus fine de l'entreprise et aussi permettre aux travailleurs d'être plus efficace dans le travail. Elle est subdivisée comme suite :

✓ **Le pole réseaux et sécurité** chargé de :

- Maintenir le parc informatique, planifier les interventions d'installation, de configuration et de dépannage de matériels,
- Gérer le réseau informatique et faire évoluer l'infrastructure matérielle dans tous les bâtiments,
- Gérer la messagerie électronique, le réseau sans fil,
- Gérer les équipements audiovisuels et les systèmes de visioconférence,
- Mettre en place les mécanismes concernant la sécurité informatique et assurer la veille sur l'évolution des risques,
- Administrer et exploiter les serveurs administratifs, etc.

✓ **Le pole développement et gestion des bases de données** chargé de :

- Mettre en place une politique de sauvegarde et d'archivage des données,
- Maintenir et faire évoluer le système d'information,
- Mise en place de nouvelles solutions applicatives.

Sa **représentation hiérarchique** est la suivante :

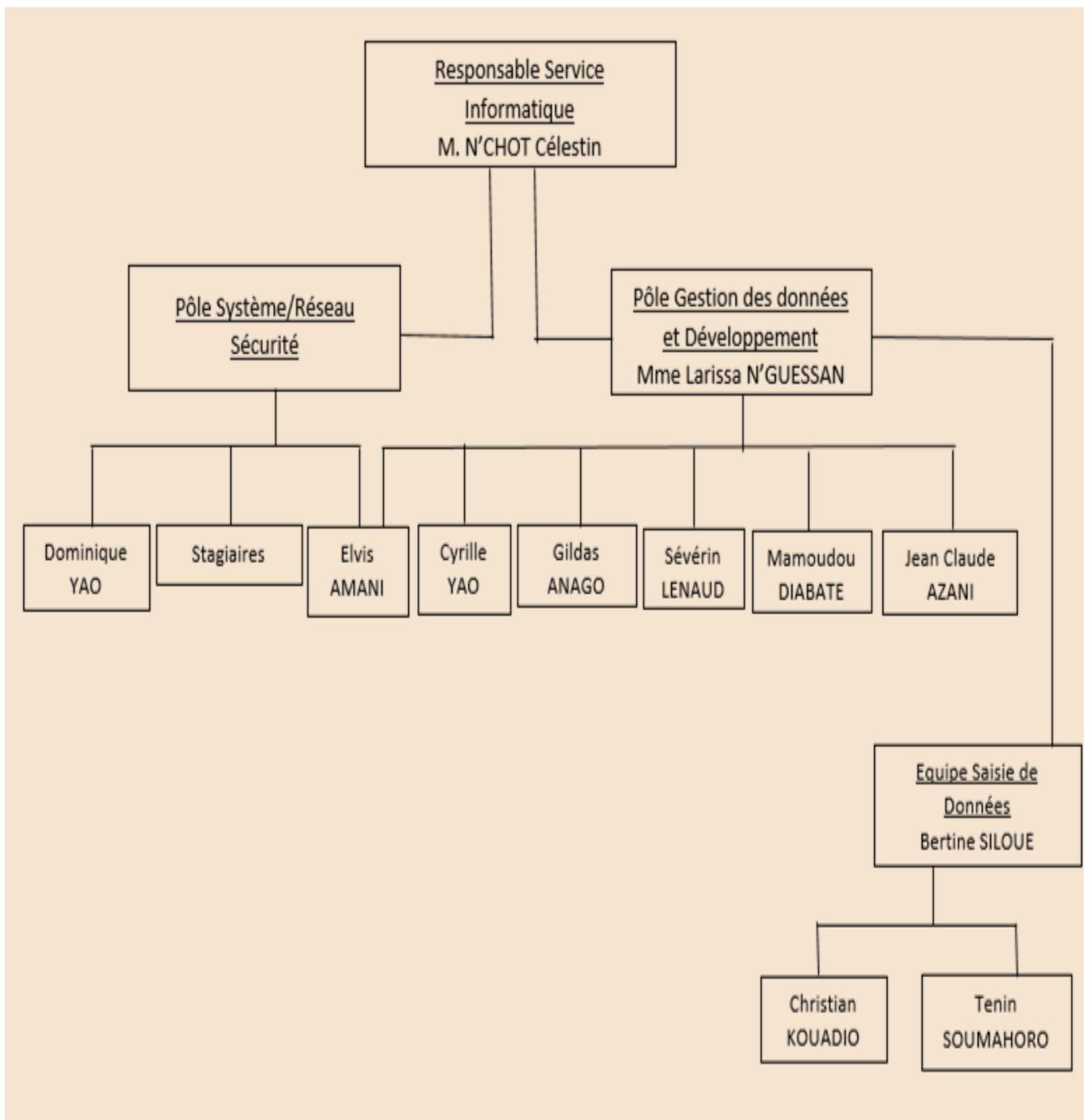


FIGURE I.2 : Organigramme du Service Informatique du Programme PAC-CI

CHAPITRE II : CONTEXTE D'EXECUTION

I) PRESENTATION DU THEME

L'Objectif principal d'un contrôleur de domaine, est de pouvoir régler les accès aux ressources du réseau tant à partir du réseau local qu'à l'extérieur, tout en essayant au maximum de limiter les failles d'éventuelles attaques ou vols d'informations.

II) CADRE DE MISE EN PLACE

Au sein de l'organisation PAC-CI, les ressources sont partagées par de nombreux utilisateurs et applications. Pour permettre à ceux-ci d'accéder à des ressources et aux informations les concernant, une méthode de gestion des données est donc nécessaires . A cet effet, l'installation d'un domaine est donc l'option idéale dans la mesure où l'on veut gérer en même temps les données, les utilisateurs et les accès utilisateurs à ces données.

PAC-CI adopte alors cette idée de domaine par la mise en place d'un contrôleur de Domaine sous Windows serveur 2008.

Avec l'avènement des Nouvelles Technologie de l'information, l'administration informatique ne cesse de s'améliorer. Etant disponible et accessible en tout temps, les outils d'échange de données et de partage d'information doivent être en mesure d'offrir une confidentialité maximale et une sécurité à toute épreuve.

C'est à la recherche de solutions pouvant pallier aux problèmes de sécurité, de mobilité, d'ergonomie, et de modernisation que l'organisation PAC-CI décide de migré vers un nouveau domaine sous un serveur plus performant. D'où l'origine du thème : « **Mise en place d'un contrôleur de domaine sous Windows serveur 2016** ». Notre stage au sein de cette organisation consiste donc à l'installation de Windows Server 2016 et à la configuration de l'Active Directory et de ces services. Puis d'ajouter les ordinateurs du réseau au domaine et créer, configurer les comptes utilisateurs, a l'objectif de mettre en place un serveur contrôleur de domaine qui sera en mesure de répondre aux critères demandé par un administrateur réseau.



**PARTIE II : ETUDE
TECHNIQUE**

CHAPITRE I : GENERALITE SUR LES SERVEURS

I. DEFINITION D'UN SERVEUR

Un serveur est un ordinateur qui fournit des services à d'autres ordinateurs en réseau intranet et internet. En d'autre terme, c'est une unité centrale qui exécute des opérations selon les requêtes envoyées par un ordinateur appelé « **client** », d'où la relation « **client/serveur** ».

La plupart des réseaux informatiques prennent en charge un ou plusieurs serveurs traitant des tâches spécialisées. En règle générale, plus le nombre de clients connectés au réseau est important, plus il est probable que plusieurs serveurs jouent un rôle, chacun étant dédié à un objectif spécifique.

Parmi ces taches, les plus importantes sont :

- **La Messagerie** : logiciel de transfert de messages électroniques d'un serveur à un autre. L'exécution de ce service par un utilisateur, demande l'installation d'un *client de messagerie* sur sa station de travail. Le rôle du client de messagerie est de contacter le serveur pour envoyer ou recevoir les messages.
- **Le World wide web** : abrégé *www*, c'est une technologie qui permet de consulter, avec un navigateur, des pages accessibles sur des sites.
- **La Base de donnée** : c'est une collection d'informations organisées afin d'être facilement consultables, gérables et mises à jour.
- **L'Authentification** : technique de sécurité consistant à définir les utilisateurs, les programmes et les ressources autorisé dans un environnement informatique.

II. LES DIFFERENTS TYPES DE SERVEUR INFORMATIQUE

- **Serveur de messagerie** : il permet l'envoi et la livraison du courrier électronique aux ordinateurs.
- **Serveur web** : logiciel utilisé sur le serveur pour accéder à une page web .
- **Serveur de fichiers** : Ce serveur stock les fichiers partagés par plusieurs ordinateurs dans un emplacement commun. Un utilisateur peut accéder à un document depuis un ordinateur quelconque, grâce à ce serveur.
- **Serveur d'applications** : il permet de partager des données d'un logiciel accessibles depuis tous les postes reliés au serveur informatique. Ce serveur est identique au *serveur de fichier*, mais différent au point où celui est spécialisé dans le stockage de donnée pour logiciel (Sécurité, Comptabilité,...) et l'autre dans le stockage de donnée personnel (images, vidéos,...).
- **Serveur d'impression** : il gère le partage des imprimantes dans le réseau.

III. ARCHITECTURE RESEAU

1) Peer to Peer

Une architecture **Peer to Peer** en français *égal à égal*, est une architecture réseau dans laquelle chaque ordinateur est un peu serveur et un peu client. Un **poste client** est un ordinateur qui envoie des demandes vers un autre ordinateur. Chaque poste du réseau est **libre** de partager ses ressources. Cela signifie qu'il n'y a pas **d'administrateur central**.

Ce type de réseaux présente d'énormes inconvénients que d'avantages :

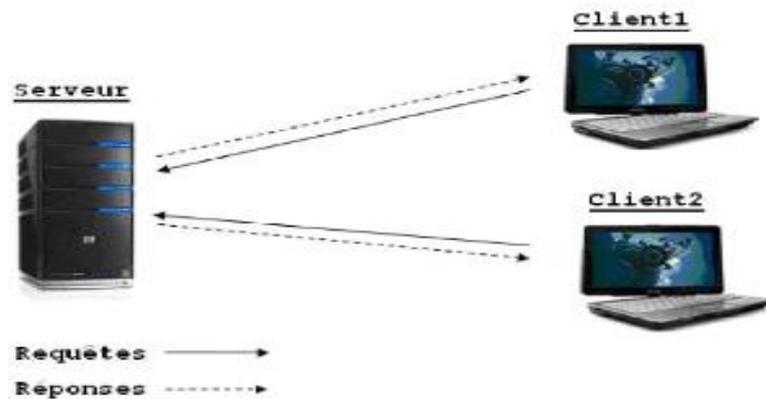
- Il comporte peu de postes (moins d'une dizaine de postes.)
- Un système non centralisé
- Un niveau de sécurité faible

Néanmoins c'est une architecture facile à installer et moins coûteuse.

2) Client-serveur

L'architecture **Client-serveur** désigne un mode de communication dans lesquels un poste client envoie des requêtes à un autre poste appelé serveur, qui lui à son tour répond à cette requête. Le serveur est la machine la plus puissante en matière de stockage et de traitement de tâches dans un environnement

informatique. Elle est indispensable dans une Entreprise car elle centralise et fiabilise la Sécurité du système informatique.



IV. FORMAT DE SERVEUR

1) Le Serveur Tour



Son Format est identique à l'unité centrale d'un ordinateur. Sa particularité est qu'il peut être installé dans n'importe quelle pièce de l'entreprise, contrairement aux serveurs racks ou lames, qui nécessitent un emplacement spécifique pour fonctionner.

Ces serveurs proposent souvent des performances d'entrée de gamme, et leur prix sont proche de celui d'un ordinateur. Installation facile et résistant. L'utilisateur peut ajuster le volume

NB : un serveur tour peut en moyenne accueillir 6 disques durs, et deux processeurs.

2) Le Serveur Rack

Le serveur rack est conçu pour être disposé dans des **racks**, armoires spécialement conçu pour installer du matériel informatique. Ceux-ci vont être empilés dans le rack, avec l'avantage de pouvoir faciliter **les différentes connexions**. Au moyen du rack tous les équipements informatiques nécessaires à la vie de l'entreprise seront regroupés au même endroit.



Plusieurs serveurs physiques peuvent être positionnés sur un seul et même rack, afin par de répartir les services (messagerie, impression,) . Sur le marché, les serveurs racks, sont plus couteux que les serveurs tours, mais possèdent des capacités de stockage bien plus importantes, et ils sont également bien plus évolutifs.

3) Le Serveur Lame

Les serveurs lame ou blade sont les derniers modèles de serveur. Compact, et mince comme une lame, ils sont insérer verticalement dans un chasier dédié.



Certains éléments matériels des serveurs lames sont mutualisés, ce qui permet une efficacité et une réduction de coût à partir d'une certaine masse critique de matériel, et de besoins informatiques. Un chasier accueille un certain nombre de serveur qui doivent être alimenté. La particularité de ces serveurs lames est qu'ils utilisent une alimentation unique, positionnée sur le chasier d'accueil. Au final, les serveurs lame assurent une puissance de traitement plus importante, un encombrement réduit et une consommation énergétique moindre que les autre formats, à usage équivalent. Du coté investissement se sont les plus couteux, et aussi les plus performant.

CHAPITRE II : PRESENTATION D'UN CONTROLEUR DE DOMAINE

I. DEFINITION DES CONCEPTS

1) Active directory

Active Directory essentiellement conçu pour les systèmes d'exploitation Windows , est un magasin d'identités centralisé de tous les membres d'un domaine. Il stocke des informations sur les utilisateurs, les groupes, les ordinateurs et autres enregistrements. Et permet également à l'administrateur de contrôler l'utilisation des ressources répertoriées grâce à des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation des accès.

Les différentes fonctions d'un active directory sont listées ci-dessous :

- Services ADDS (Active Directory Domain Services)
- Services ADLDS (Active Directory Lightweight Directory Services)
- Services ADCS de (Active Directory certificats Services)
- Services ADRMS (Active Directory Right Management Services)
- Services ADFS (Active Directory Fédération Services)

Hébergé par un serveur jouant le rôle d'un contrôleur de domaine, Active directory exécute une seule fonction : **Services ADDS** (Active Directory Domain Services) traduit service de domaine Active Directory.

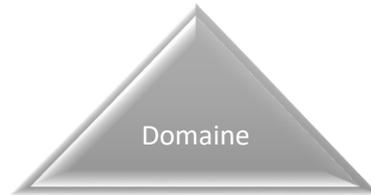
2) Un Domaine

Un **domaine** est un ensemble d'ordinateurs reliés au sein d'un réseau et possédant une caractéristique commune. Par exemple, un domaine nommé "SECU" désigne l'ensemble des ordinateurs et périphériques du réseau du service *sécurité*, et les comptes utilisateurs qui sont autorisés à s'y connecter. Composé d'un ou de plusieurs contrôleurs de domaine, il constitue le contexte dans lequel sont créés les objets suivants :

– **Le compte utilisateur** qui permet de définir les droits d'accès aux différentes ressources partagées.

– Le **compte ordinateur** qui permet d'identifier un ordinateur sur laquelle l'utilisateur se connecte à son compte.

– **les groupes** qui permettent de regrouper des comptes utilisateurs et ordinateurs dans le but de leur autoriser l'accès à une ressource.



Symbole d'un Domaine

3) Une Arborescence

Le terme **arborescence** définit un ensemble de données structuré en **arbre**. Elle sous-entend la notion de **hiérarchie**, dans laquelle les utilisateurs et les ordinateurs sont organisés en *groupes et sous-groupes* afin de faciliter l'administration des comptes utilisateurs.

Cette hiérarchie part d'une racine appelé le **niveau 1 de l'arborescence**. Une racine peut contenir autant de **répertoires**, chaque répertoire pouvant lui-même contenir autant de **sous-répertoires** que nécessaire, et ainsi de suite. Les domaines d'un même arbre partagent un espace de noms juxtant comme l'exemple ci-dessous :

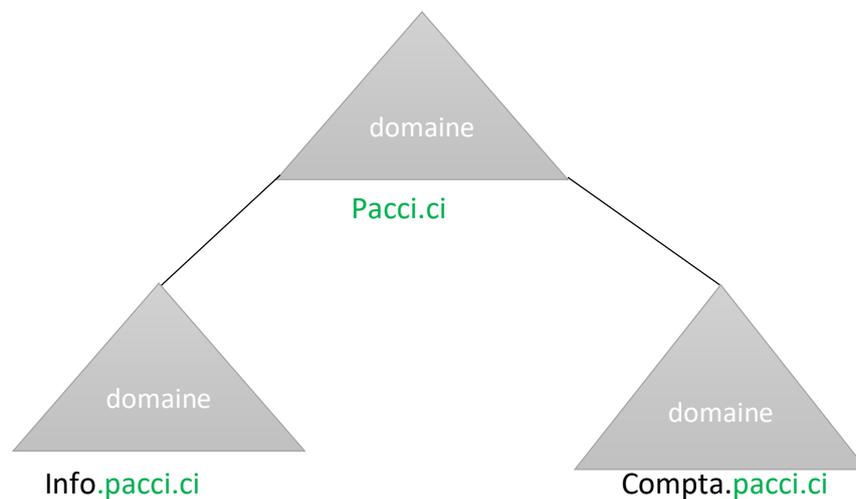


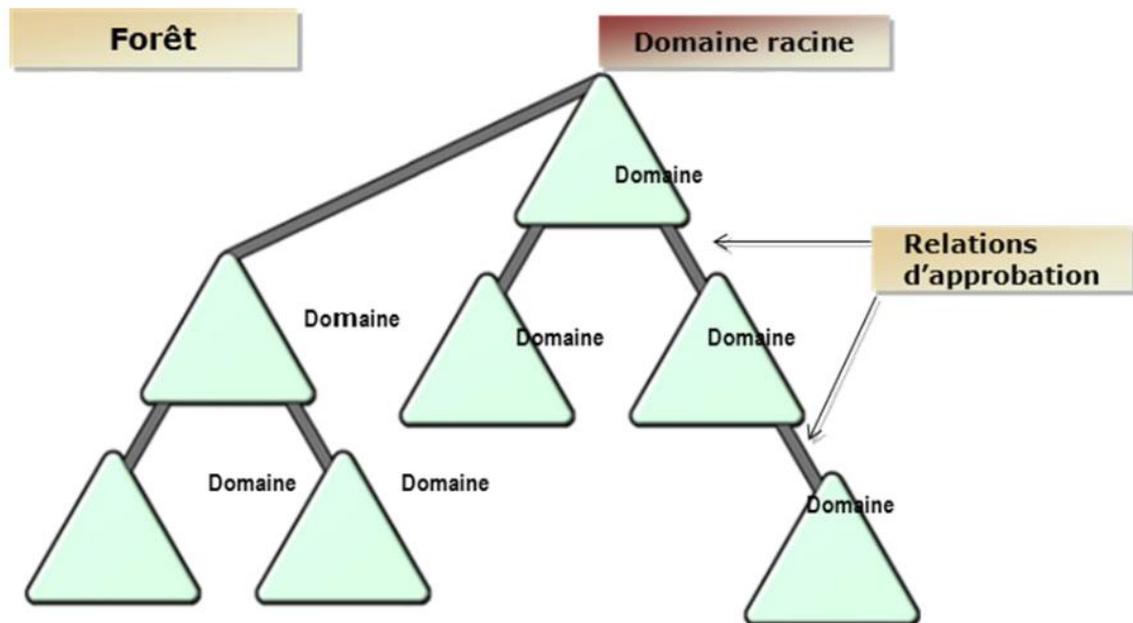
Schéma d'une arborescence

4) Forets

Une forêt est composée d'une suite de domaines appelée *arborescence de domaines*.

Dans une forêt le premier domaine est appelé **domaine racine**, elle porte le nom de ce dernier. L'ensemble des contrôleurs de domaine présents dans une forêt partagent une seule configuration et un seul schéma. La relation entre les domaines d'une même arborescence est de type parent/enfant.

NB : Un domaine qui dispose d'un espace de noms différent fait partie d'une arborescence différente.



5) Contrôleur De Domaine

Un contrôleur de domaine est un serveur exécutant **Active Directory**.

La principale responsabilité de ce serveur consiste à authentifier et à valider l'accès des utilisateurs sur le réseau. Lorsque les utilisateurs se connectent à leur domaine, le contrôleur de domaine vérifie leur nom d'utilisateur, leur mot de passe et leurs autres informations d'identification pour autoriser ou refuser l'accès .

II. GESTION A BASE DE STRATEGIE

1) Définition

Les **stratégies de groupe** ou **GPO** sont stratégies de gestion centralisée des ordinateurs et des utilisateurs appartenant à un domaine Active Directory.

Ils permettent la configuration des restrictions d'utilisation ou des paramètres à appliquer soit sur un ordinateur donné, soit un compte utilisateur donné.

Les stratégies de groupe sont enregistrées dans le répertoire **SYSVOL** disponible sur chaque contrôleur de domaine.

Ils ont pour avantages :

- La mise en place d'une politique de sécurité commune à des utilisateurs et ordinateurs.
- Déploiement des applications sur des postes de travail ciblés.
- Gestion centralisée et dynamique des ressources.
- Contrôle efficace des actions des utilisateurs.
- Renforcement de la sécurité dans un domaine Active Directory

2) Différents types de stratégies importantes

a. Stratégie de mot de passe

Les stratégies de mots de passe correspondent à des objets : Paramètres de mots de passe, et sont également appelées **PSO** (*Password Settings Object*).

- **Nom** : il s'agit du Nom du PSO

- **Priorité** : une Valeur supérieure à 0 qui servira à faire l'arbitrage en cas de conflit entre deux PSO qui s'appliquent sur un même objet.

- **Appliquer la longueur minimale du mot de passe** : Chiffre entier pour définir la longueur minimale que doit faire le mot de passe

- **Appliquer l'historique des mots de passe** : Permet de définir le nombre d'anciens mots de passe qu'un utilisateur ne peut pas réutiliser,

- **Le mot de passe doit respecter des exigences de complexité** : Indiquez si oui ou non le mot de passe doit respecter ces exigences .

- **Protéger contre la suppression accidentelle** : protéger contre une éventuelle suppression involontaire.

- **Appliquer l'âge minimal de mot de passe** : Durée de vie minimale d'un mot de passe,

- **Appliquer l'âge maximal de mot de passe** : durée de vie maximale d'un mot de passe.

- **Nombre de tentatives échouées autorisé** : verrouillez le compte automatiquement Une fois le nombre de tentatives autorisées est dépassé,
- **Réinitialiser le nombre de tentatives de connexion échouées après (min)** : Une fois ce délai écoulé, le nombre de tentatives échouées et remis zéro.
- **Le compte va être verrouillé** : Lors du verrouillage d'un compte, ce dernier peut être verrouillé :
 - *Pendant une durée de (min)* : Définissez un temps de verrouillage du compte qui sera automatiquement déverrouillé une fois le délai terminé.
 - *Jusqu'à ce qu'un administrateur déverrouille manuellement le compte* : Une action d'un administrateur est requise pour déverrouiller le compte.

b. Stratégie de verrouillage du compte

Le verrouillage des comptes permet de bloquer un compte pendant un certain temps si un nombre défini de tentatives de connexion n'ont pas réussi pendant une certaine période.

- **Seuil de verrouillage de comptes** : cette valeur définit le nombre d'échecs d'ouverture de session autorisé avant que le compte ne soit bloqué. La valeur « 0 » indique qu'il n'y a pas de verrouillage de compte.
- **Réinitialiser le compteur de verrouillages du compte après** : cette valeur définit l'intervalle de temps pendant lequel le nombre de tentatives d'échec ont eu lieu. Si les tentatives de connexion se font à un intervalle supérieur à cette valeur le compte ne sera pas verrouillé.
- **Durée de verrouillage des comptes** : cette durée indique la durée pendant laquelle le compte est considéré comme verrouillé, une fois ce temps dépassé les compteurs repartent à 0.

c. Stratégie d'audit

La Stratégie d'audit permet de contrôler et de connaître l'accès aux objets, tels que les fichiers et dossiers, et pour gérer les comptes d'utilisateur, les groupe et les ouvertures et fermetures de session. Les Stratégies d'audit peuvent spécifier les catégories d'événements à auditer, définir la taille, le comportement du journal de sécurité et déterminer le type de surveillance d'accès à un objet.

III. ENVIRONNEMENT DE L'ACTIVE DIRECTORY

1) Les Unité Organisationnelle

Les unités d'organisation sont des conteneurs dans lesquels l'on peut placer des utilisateurs, des groupes, des machines et d'autres unités d'organisation (*sous unités organisationnelle*). Elles ne peuvent contenir que des objets de leur domaine parent. En d'autre terme des objets ayant les mêmes tâches administratives. Elles servent également de frontière pour la délégation d'autorisation administrative et permet d'appliquer la stratégie de groupe.

2) PowerShell

PowerShell est un module consolidant un groupe d'applets de commande permettant l'automatisation des tâches nécessaire pour gérer les domaines Active Directory, [les jeux de configuration AD LDS \(Active Directory Lightweight Directory Services\)](#) et [les instances de l'outil de montage](#) de base de données Active Directory dans un seul package autonome.

PowerShell montre toute les informations concernant un domaine. l'applet de commande [Get-Command](#) présente toutes les applets de commande disponible.

3) Catalogue global

Un catalogue global (**GC**)est un répertoire qui contient des copies de tous les objets Active Directory de la forêt.il permet aux utilisateurs et aux applications de rechercher des objets dans une arborescence de domaine Active Directory, en fonction d'un ou de plusieurs attributs de l'objet cible.

Le catalogue global est créé automatiquement par le système de réplication des services de domaine Active Directory. La topologie de réplication du catalogue global est générée automatiquement. Les propriétés répliquées dans le catalogue global incluent un ensemble de base défini par Microsoft.

Aussi, Les administrateurs peuvent spécifier des propriétés supplémentaires pour répondre aux besoins de leur installation.

4) La Réplication

La réplication Active Directory garantit la mise à jour et la cohérence des informations entre les contrôleurs de domaine ; C'est la réplication qui garantit que les informations hébergées par les contrôleurs de domaine sont synchronisées entre chaque contrôleur de domaine. Elle est indépendante de la structure de la forêt, de l'arbre ou du domaine, et c'est cette flexibilité qui est au cœur de la bonne performance d'Active directory.

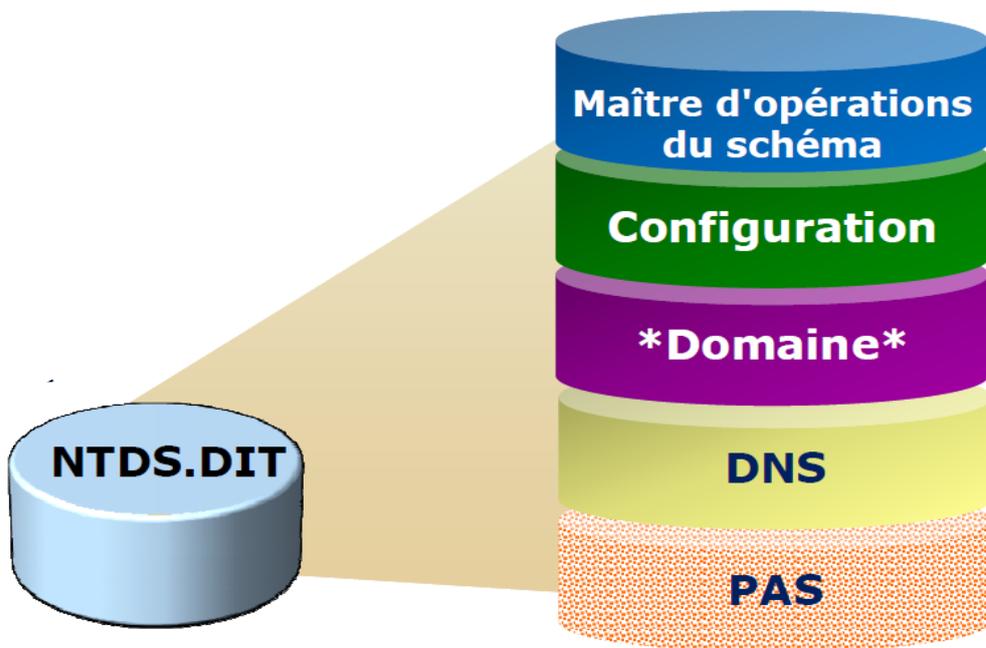
5) Relation d'approbation

les relations d'approbation sont des liens de confiance permettant aux utilisateurs authentifiés dans leur domaine d'accéder aux ressources d'un autre domaine

VI. STRUCTURE DE LA BANQUE DE DONNEE ACTIVE DIRECTORY

1) NTDS.DIT

L'ensemble des informations d'un domaine Active Directory est contenu dans un fichier de base de données nommé NTDS.DIT accessible via le dossier `%racinesystème%\NTDS\ntds.dit`. Ce fichier inclut également les hachages de mots de passe pour tous les utilisateurs du domaine. Il est organisé comme le présente le schéma suivant :



a. PAS

Partial Attribut Set (PAS) est un sous-ensemble d'attributs du schéma Active Directory qui sont répliqués sur le catalogue global. Chaque contrôleur de domaine possède une réplique complète en écriture du domaine dans lequel

réside le contrôleur de domaine. S'il s'agit également d'un serveur de catalogue global, il dispose également d'une réplique partielle en lecture seule de tous les autres contextes de dénomination de la forêt. Les répliques partielles incluent tous les objets, mais uniquement les attributs sélectionnés pour ces objets. Les attributs sélectionnés sont ceux du jeu d'attributs partiel.

b. DNS

Le DNS, **Domain Name System**, traduit en français : *système de noms de domaine* est le service utilisé pour traduire les noms de domaine Internet en adresse IP. L'accès aux hôtes sur un réseau IP, se fait par la mise en place d'un mécanisme associant un nom à une adresse IP. Ce nom, plus simple pour l'homme est appelé « nom de domaine ».

Dans le cas d'Active Directory, le DNS constitue l'élément primordial pour son fonctionnement. Il maintient une base de données de services qui s'exécutent sur ce réseau. Les services de domaine Active Directory (AD DS) utilisent les services de résolution de noms DNS (Domain Name System) pour permettre aux clients de localiser les contrôleurs de domaine et aux contrôleurs de domaine hébergeant le service d'annuaire de communiquer entre eux. En d'autre terme le DNS représente l'adresse du domaine sur le réseau.

c. Maître d'opération du schéma

Le Maître d'opérations ou maître d'attribution des noms de domaine représente un contrôleur de domaine dans Active Directory, unique dans une forêt. Il se charge de contrôler l'ajout ou la suppression de domaines dans la forêt. En effet, lorsqu'on ajoute des contrôleurs de domaine dans une forêt, le maître d'attribution des noms de domaine est le seul contrôleur de domaine capable d'ajouter le nouveau domaine. De part cette fonction, il permet d'éviter l'insertion de domaine ayant le même nom dans la forêt.

2) SYSVOL

Le volume système (Sysvol) est un répertoire partagé qui stocke la copie de serveur des fichiers publics du domaine qui doivent être partagés pour un accès commun et la réplication dans un domaine. Le terme SYSVOL fait référence à un ensemble de fichiers et de dossiers qui résident sur le disque dur local de chaque contrôleur de domaine d'un domaine et qui sont répliqués par le

service de réplique de fichiers (FRS). Les clients réseau accèdent au contenu de l'arborescence SYSVOL à l'aide des dossiers partagés NETLOGON et SYSVOL. Plus précisément, voici les éléments principaux que l'on trouvera dans le partage SYSVOL :

- [Scripts d'ouverture de session](#)
- [Stratégies de groupe](#)

CHAPITRE III : PRESENTATION DE WINDOW SERVER 2016

I. ETUDE DU "SYSTEME D'EXPLOITATION"

Pour qu'une application puisse utiliser les ressources matérielles d'un ordinateur, un composant ne doit impérativement pas manquer : le système d'exploitation.

Un **système d'exploitation** abrégé OS : *Operating System*, est un ensemble de programmes qui dirige l'utilisation des ressources d'un ordinateur par des logiciels applicatifs.

Après le programme d'amorçage (en anglais *bootloader*), l'OS est le principal programme exécuté lors de la mise en marche de l'ordinateur. Il fournit un ensemble de services généraux facilitant la communication entre le logiciel et le matériel informatique, apporte commodité, efficacité et capacité d'évolution, permettant l'introduction de nouveaux périphériques et de nouvelles tâches sans remettre en cause les logiciels.

On retrouve les systèmes d'exploitation dans toutes les machines ayant un processeur tels que : les ordinateurs, les téléphones, etc. Dans le domaine de l'informatique, précisément chez les serveurs, il existe plusieurs systèmes d'exploitation dédiés : [Linux](#), [Redah Enterprise](#), [Windows Server ...](#)

II. POURQUOI WINDOWS SERVER 2016 ?

1) Présentation de Windows server 2016

Windows Server 2016, aussi connu sous le nom [Windows Server vNext](#), un système d'exploitation pour serveurs [x64](#) de Microsoft, appartenant à la famille [Windows NT](#) destinée aux serveurs d'entreprise. Il utilise le noyau Windows NT 6.4, au même titre que *Windows 10*, ce qui fait qu'il ressemble visuellement à *Windows 10*. Parmi les nouvelles fonctionnalités figurent l'utilisation de *containers (avec fonction d'isolation)*, *les microservices et le cloudhybride*.

2) Les différentes éditions

Le système d'exploitation Microsoft Windows Server 2016 est disponible en trois éditions :

- **L'édition Essentials** : Cette édition est adaptée aux structures de petites tailles comptant jusqu'à 25 utilisateurs et 50 périphériques clients.
- **L'édition Standard** : édition conçue pour des environnements comptant plus de 25 stations dans laquelle toutes les fonctionnalités sont activées.
- **L'édition Datacenter** : Cette édition est plus adaptée aux infrastructures Cloud ou complexe. C'est la plus complète, car toutes les fonctionnalités du nouvel OS Cloud sont disponibles et le nombre de processeurs ou machines virtuelles est illimité

3) Les nouveautés de Windows Server 2016

Dans la vision d'améliorer le cloud, Les développeurs Microsoft, ont amélioré *Windows Server 2012 R2* pour produire *Windows Server 2016* afin d'enrichir l'expérience utilisateur.

Ce Système orienté Cloud apporte tout une série d'avantage par rapport à son prédécesseur tels que :

- **Une interface graphique**, avec le retour du menu Démarrer.
- **Les services de domaine Active Directory, amélioration** de la sécurité, du monitoring et aide au déploiement vers une infrastructure AD Cloud ou hybride avec Azure AD.
- **Les services de certificats Active Directory**, meilleur support de puces TPM et de lecteur de carte KSP pour l'attestation de clés.
(Une puce TPM est un module de plateforme sécurisé pouvant aider à sécuriser la clé privée d'un certificat),
- **Les périphériques hors domaine** peuvent désormais obtenir un certificat en utilisant l'inscription NDES, dont les clés pourront être attestées par un TPM.
- **Windows Defender** : système de sécurité permettant de protéger un serveur Windows Server 2016 .

4) Avantages pour l'entreprise

a. Sécurité

Windows server 2016 est doté d'un système de sécurité capable de détecter toute activité suspecte allant contre les systèmes d'une entreprise. Il permet aussi de réduire les dommages dans un environnement en cas d'incident. Windows server 2016 offre les différentes fonctionnalités de sécurité suivantes :

- Protection des machines virtuelles
- Sécurisation des informations d'identification de l'administrateur :
- Amélioration de la capacité de détection des

b. Evolution d'infrastructure

Windows Server 2016 permet de libérer les ressources informatiques pour planifier une stratégie utilisant des solutions Cloud pour les applications et les systèmes.

- Amélioration efficace d'infrastructures
- facilité à déployer de nouvelles applications
- Automatiser la gestion des serveurs :

c. Innovation d'application

Les applications représentent l'environnement de travail des Entreprises. Il est donc impératif, pour de nouvelles tâches, d'améliorer ou de créer de nouvelles applications. A cet effet Windows Server 2016 prendra en charge l'innovation des applications à l'aide de la technologie des **conteneurs et du micro services**. Les conteneurs ont pour rôle de :

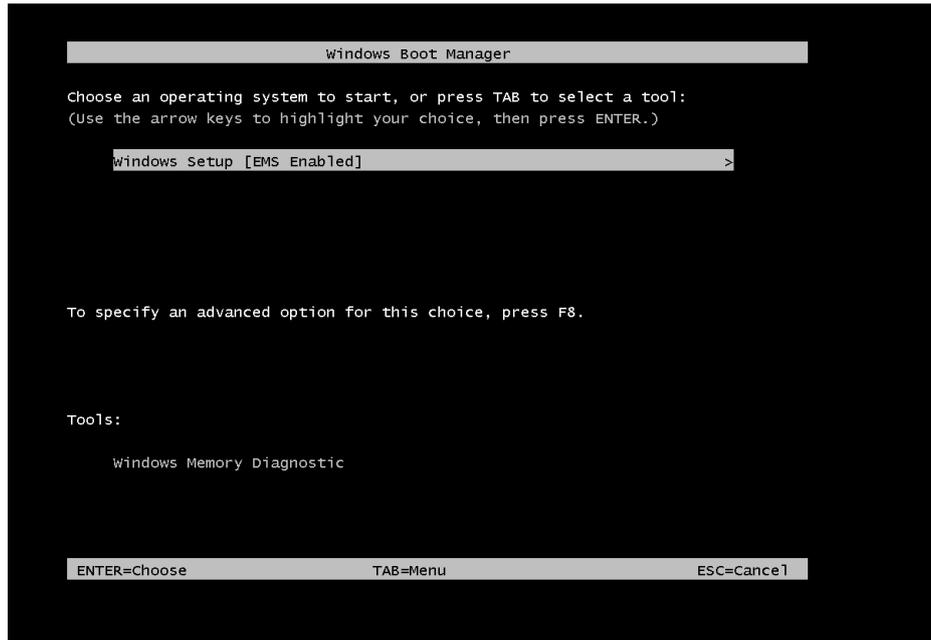
- sécuriser les applications:
- Création d'applications cloud natifs et hybrides



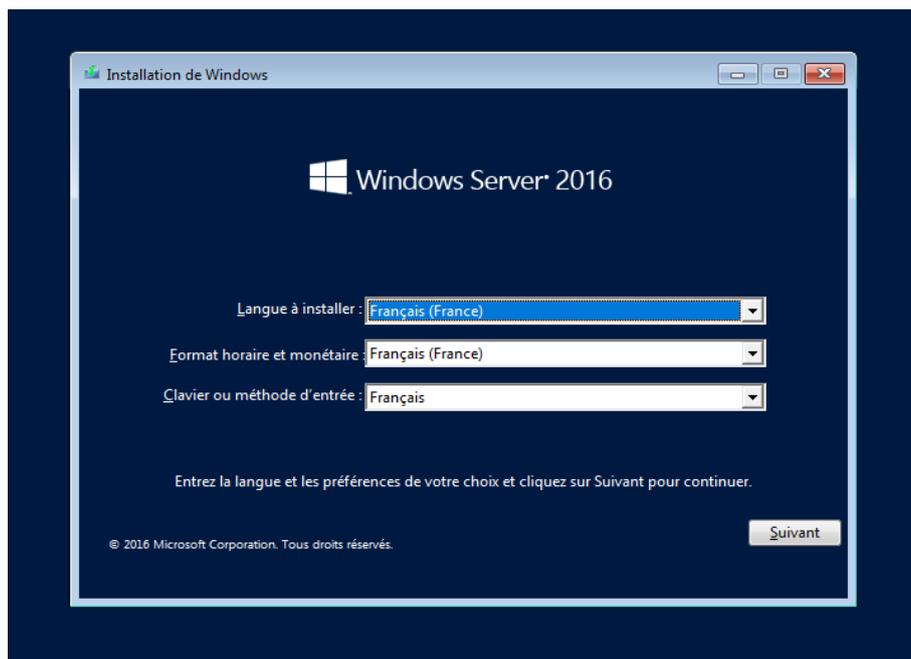
**PARTIE III : MISE EN
ŒUVRE DU CONTROLEUR
DE DOMAINE**

CHAPITRE I : INSTALLATION DE WINDOW SERVER 2016

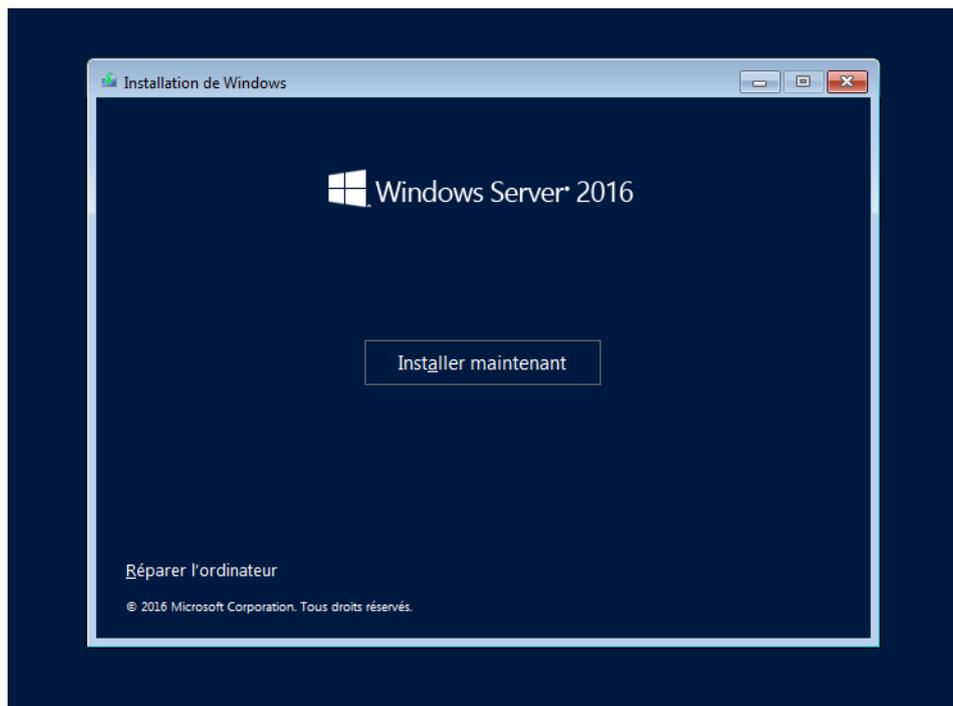
Etape 1: Menu Windows Boot manager



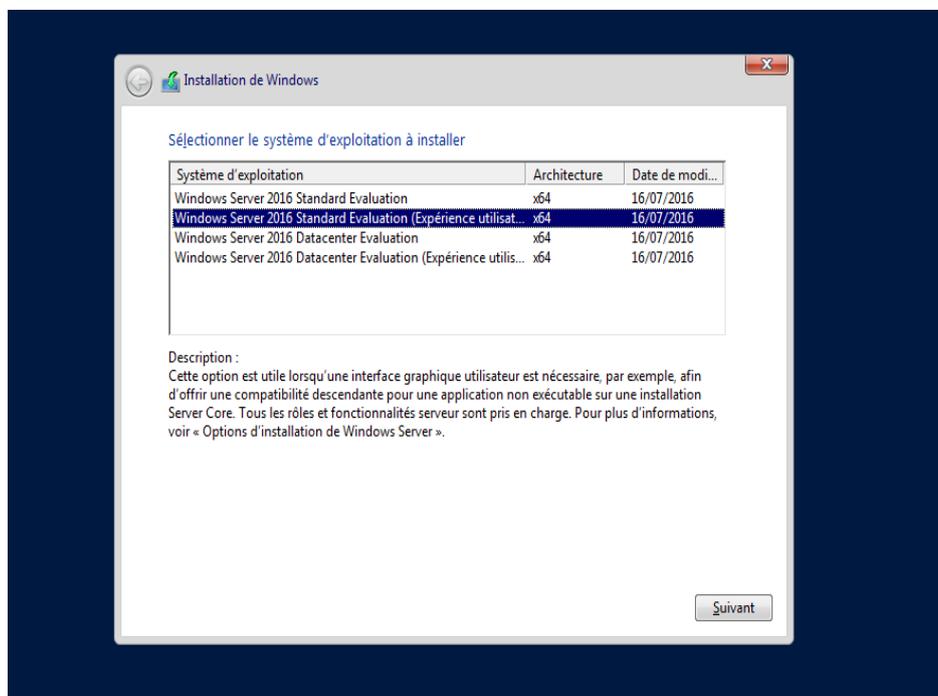
Etape 2: Fenêtre de configuration des langues



Etape 3 : Fenêtre d'installation

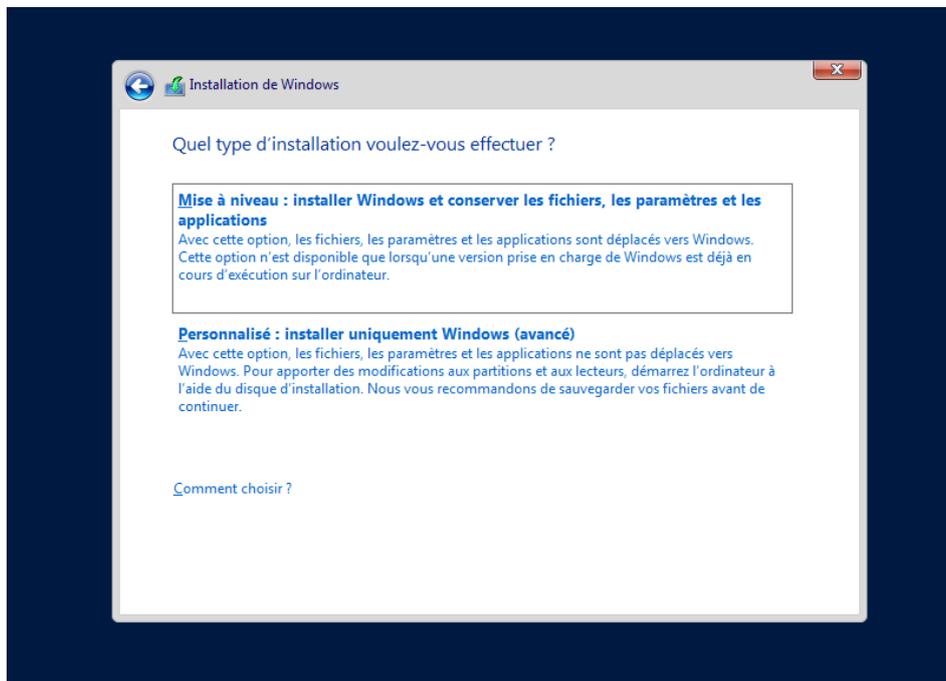


Etape 4: Choix du type du Système à installer

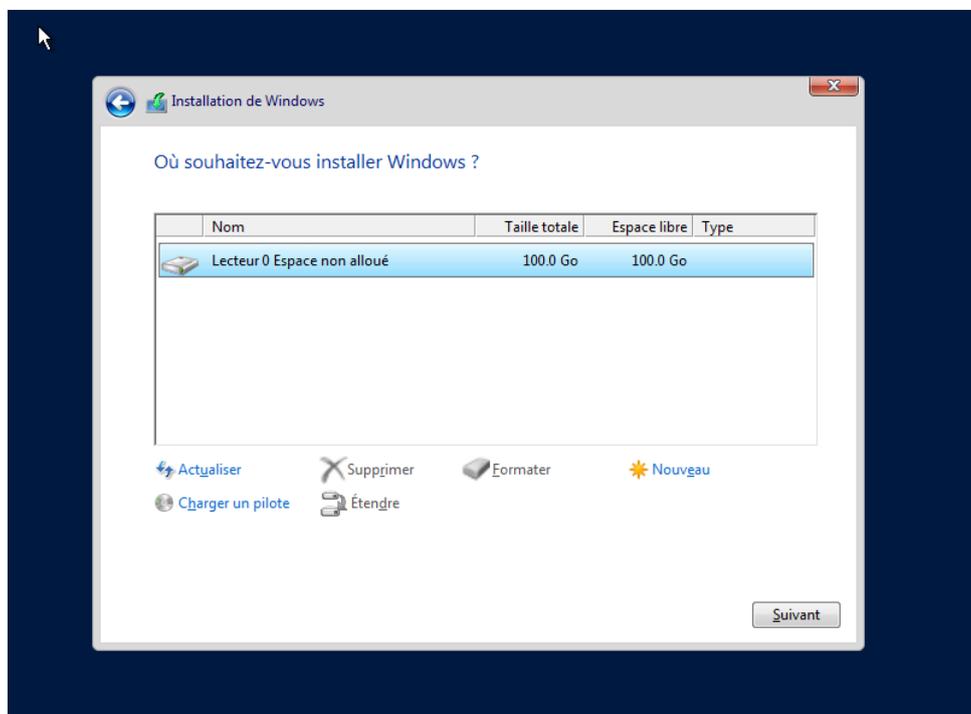


Etape 5 : Accepter le contrat d'utilisation

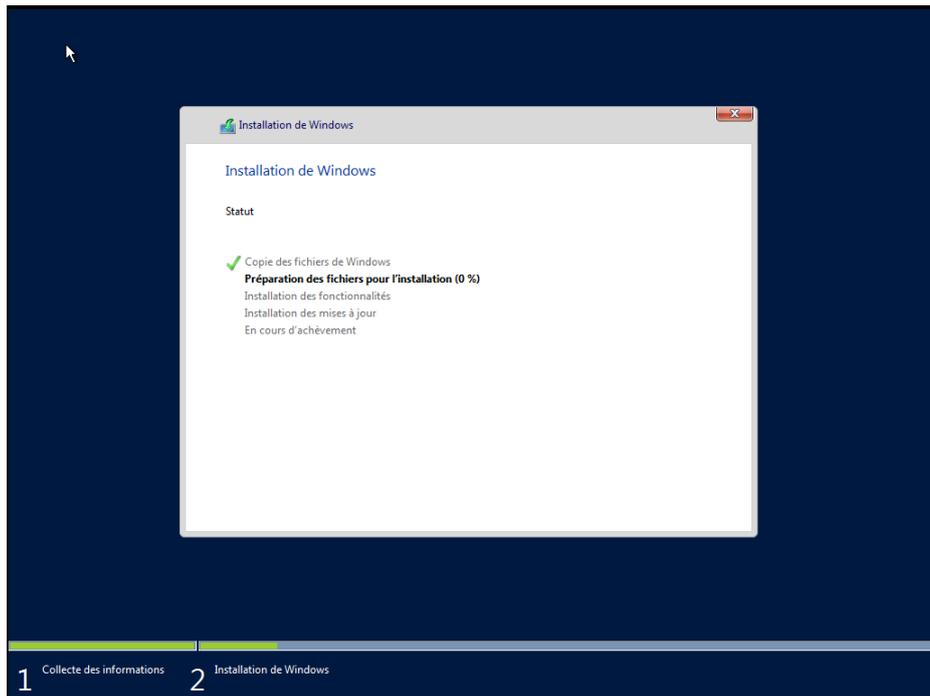
Etape 6 : Personnalisation de l'installation



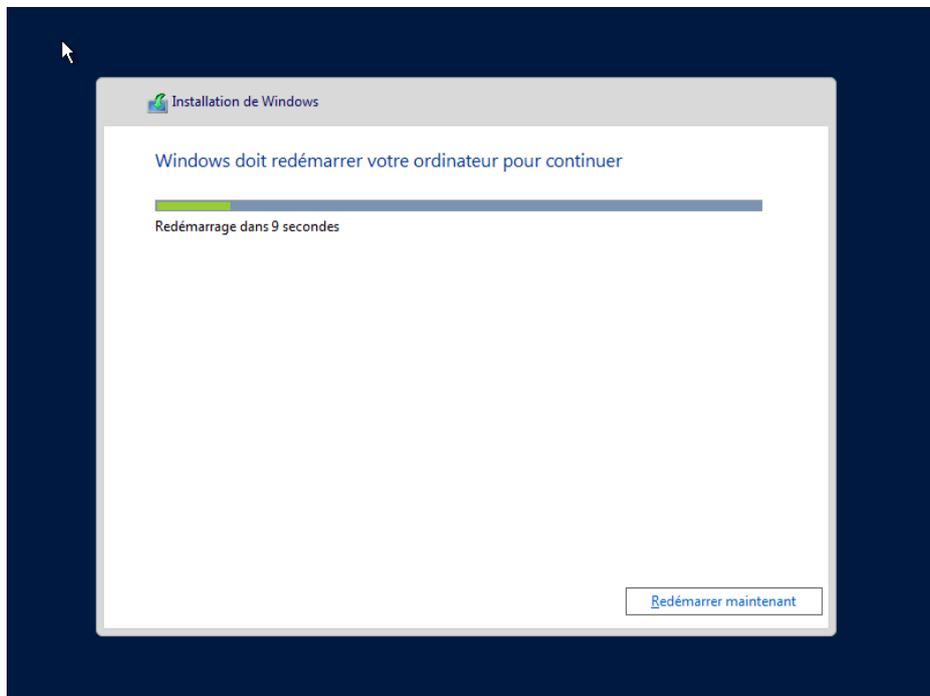
Etape 7 : Choix de la mémoire



Etape 8 : Installation du système



Etape 9 : Message de redémarrage



Etape 10: Redémarrage en cours...

Etape 11 : Paramètre de sécurité du compte administrateur

Paramètres de personnalisation

Tapez un mot de passe pour le compte Administrateur intégré que vous pouvez utiliser pour vous connecter automatiquement à cet ordinateur.

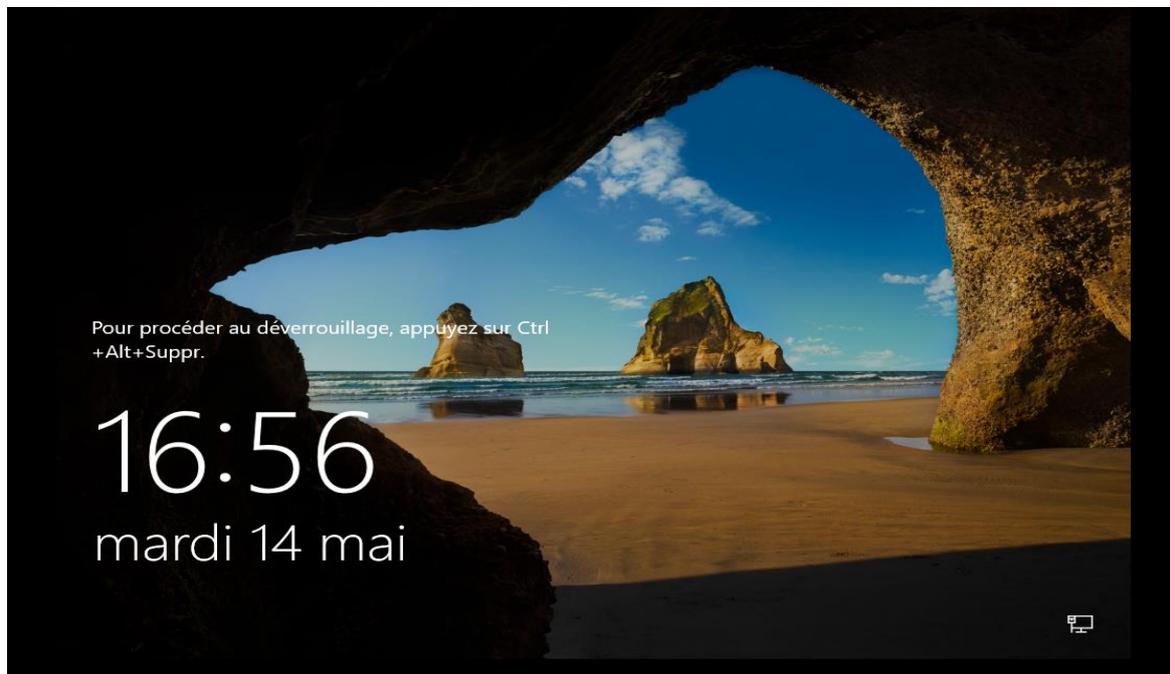
Nom d'utilisateur

Mot de passe

Entrez de nouveau le mot de passe 

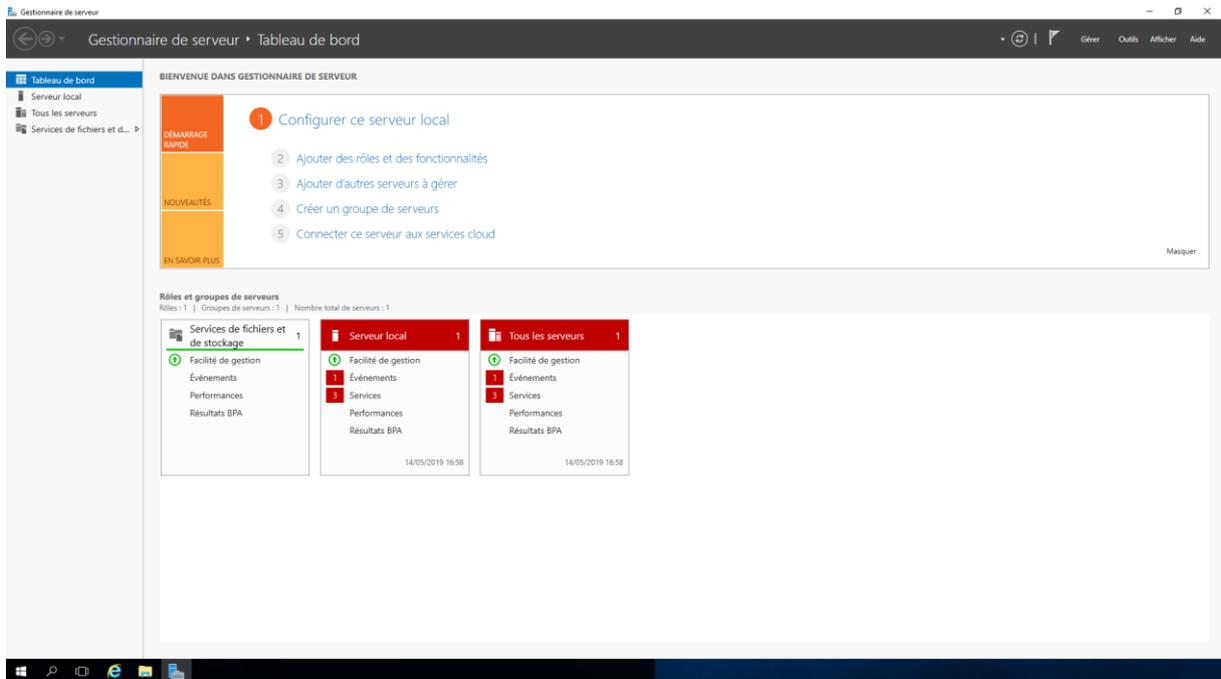
 Terminer

Etape 12 : Première page d'accueil du Système et Fin de l'installation

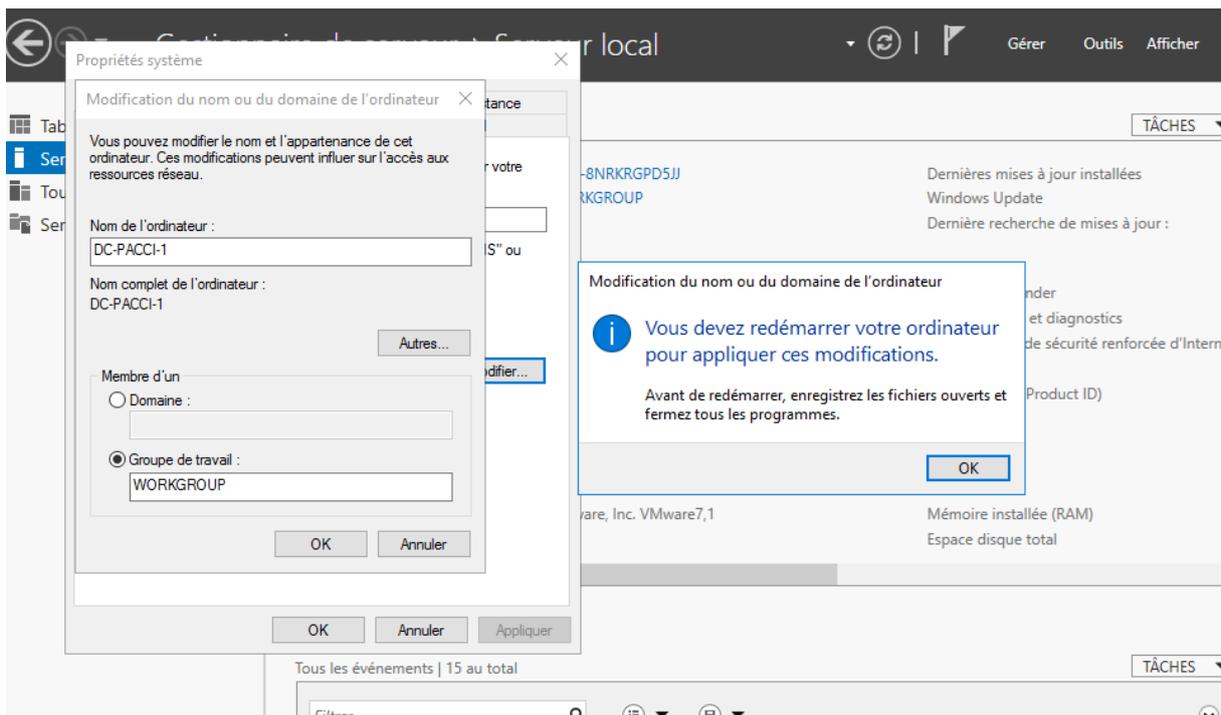


CHAPITRE II : CREATION D'UN CONTROLEUR DE DOMAINE

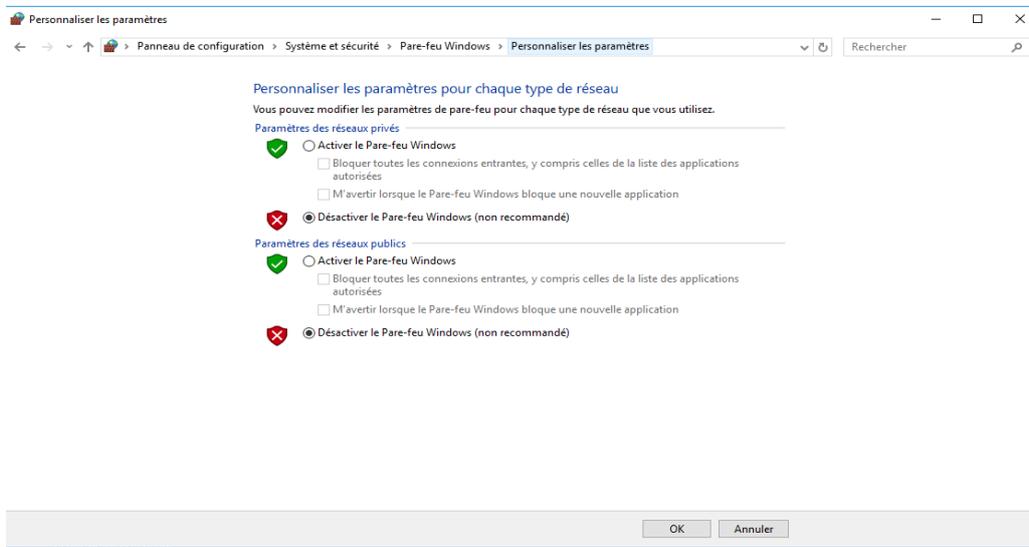
Etape 1 : Page d'accueil du gestionnaire de serveur



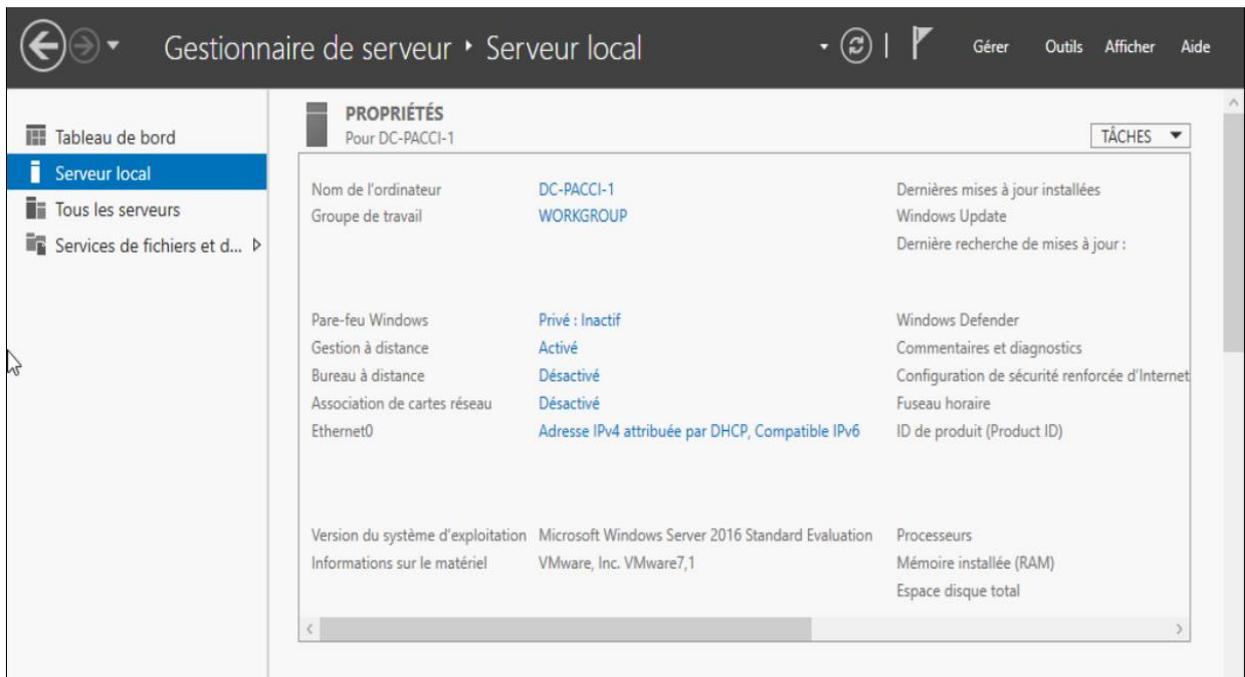
Etape 2 : Renommer le nom de l'ordinateur : DC-PACCI 1



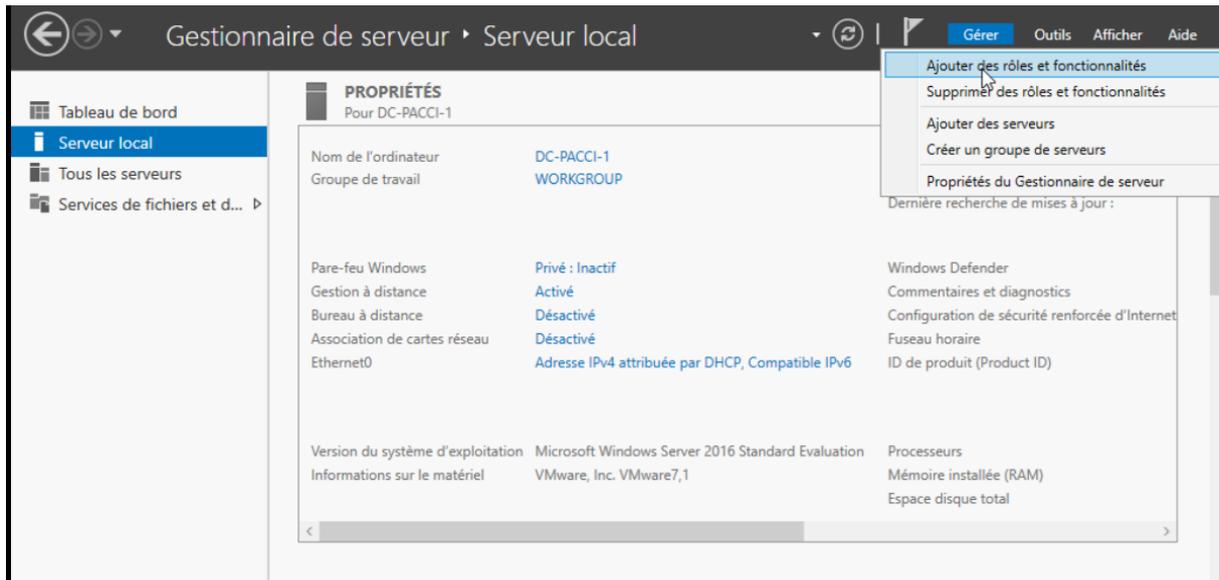
Etape 3 : Désactivation du Pare feu



Etape 4 : Propriété du serveur local

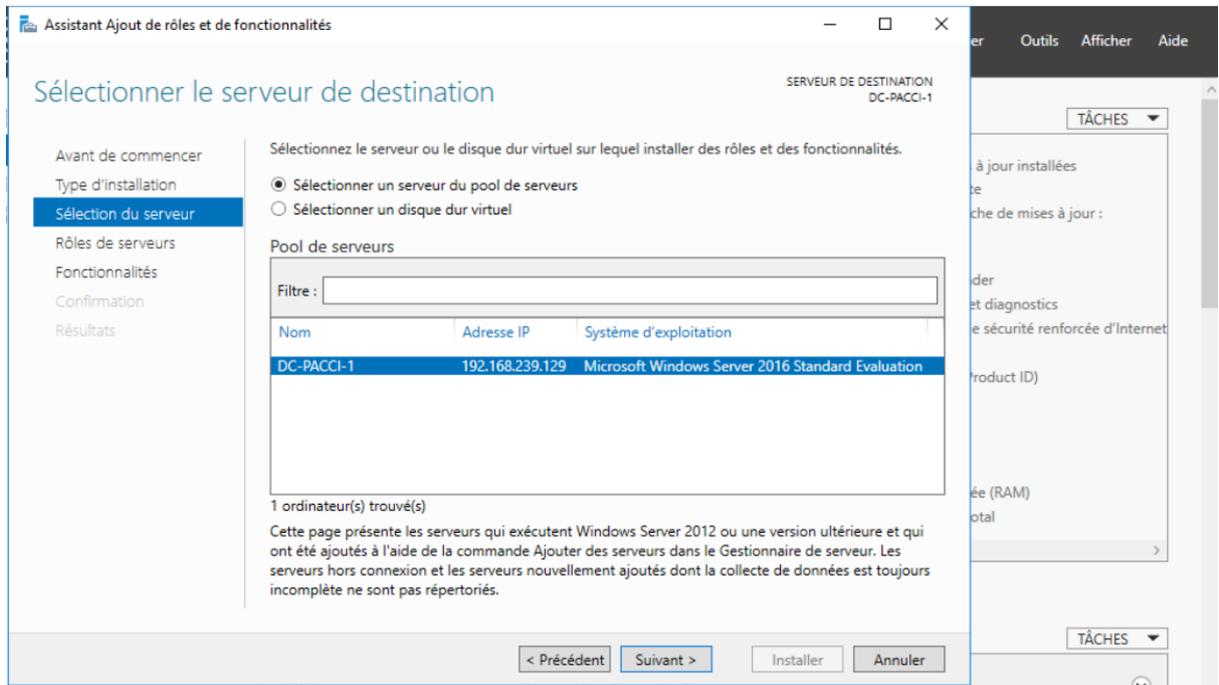


Etape 5: Menu d'installation du contrôleur de Domaine

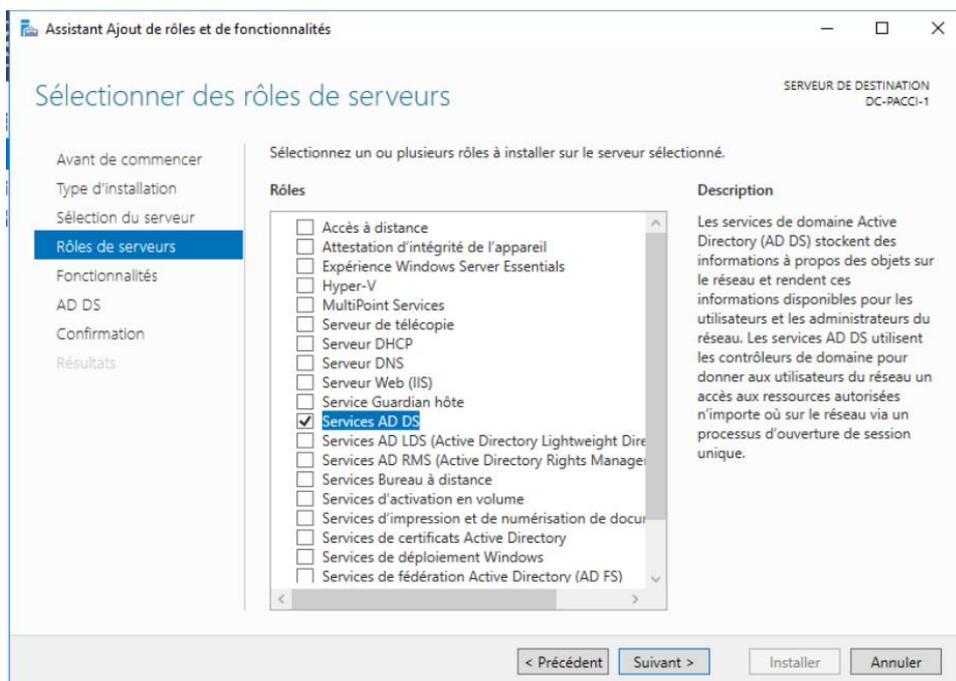


Etape 6 : Présentation de l'assistance d'installation du DC

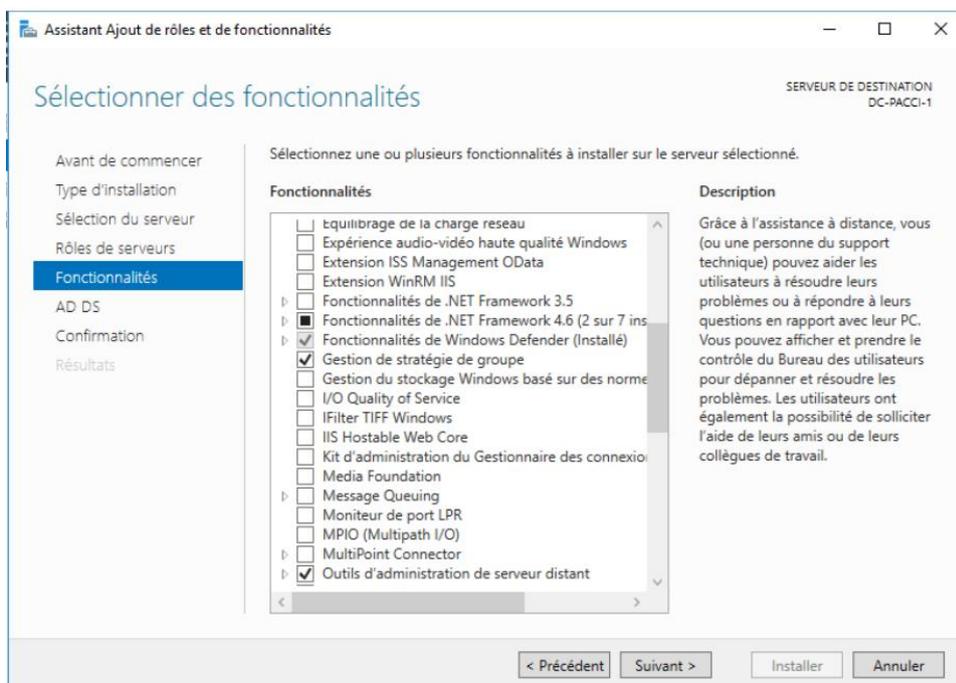
Etape 7 : Choix du serveur à configurer



Etape 8 : Sélection du Rôles de serveurs



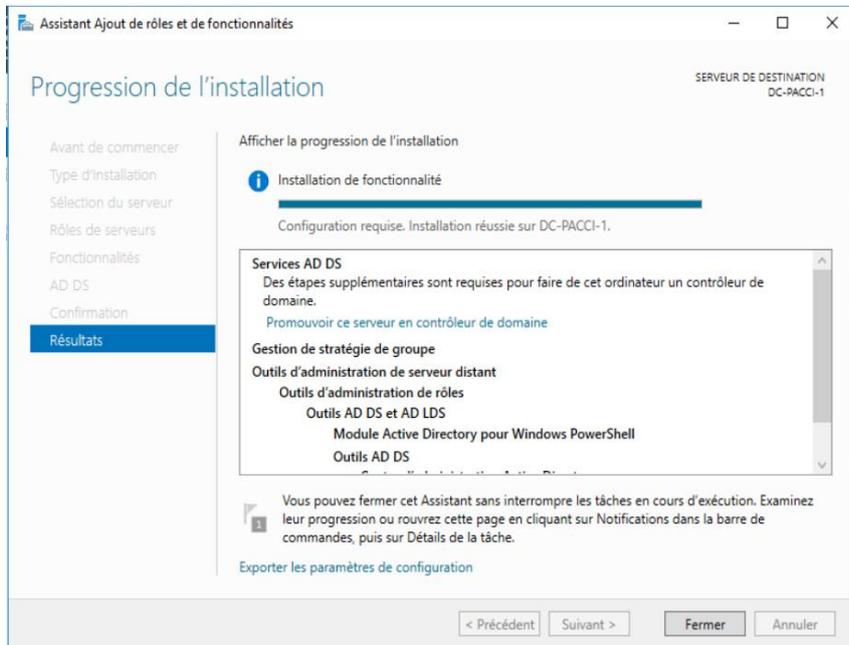
Etape 9 : Sélection des fonctionnalités



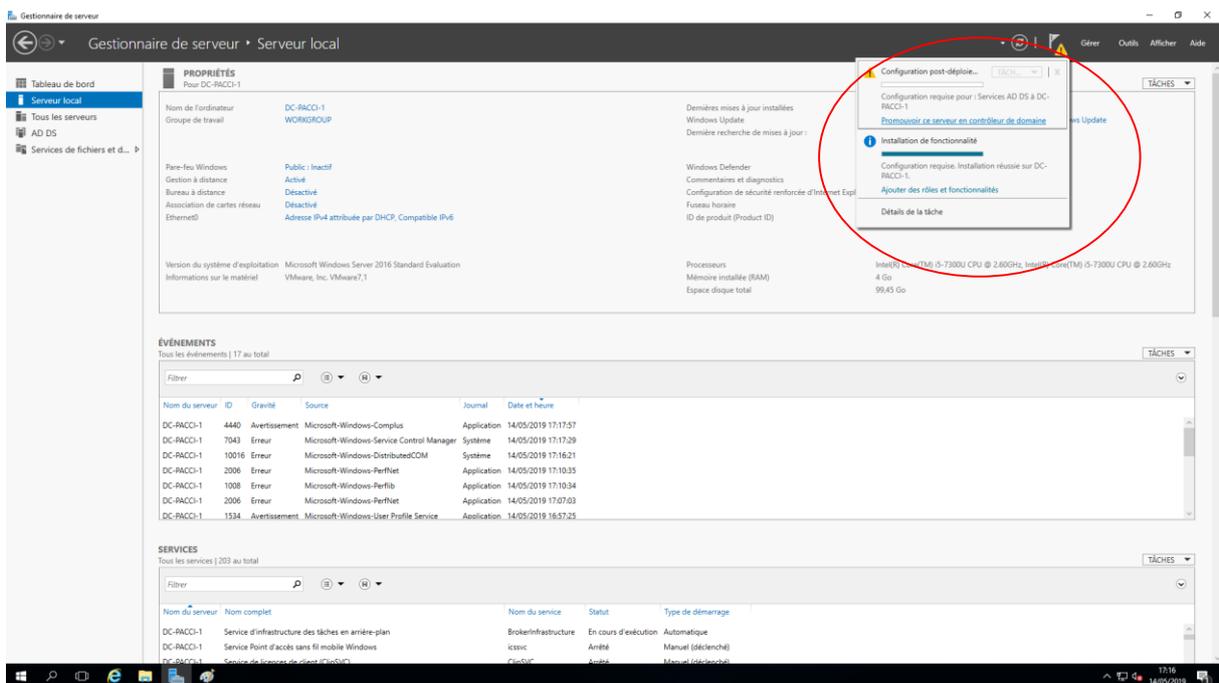
Etape 10: Présentation du rôle sélectionné

Etape 11 : confirmation du rôle

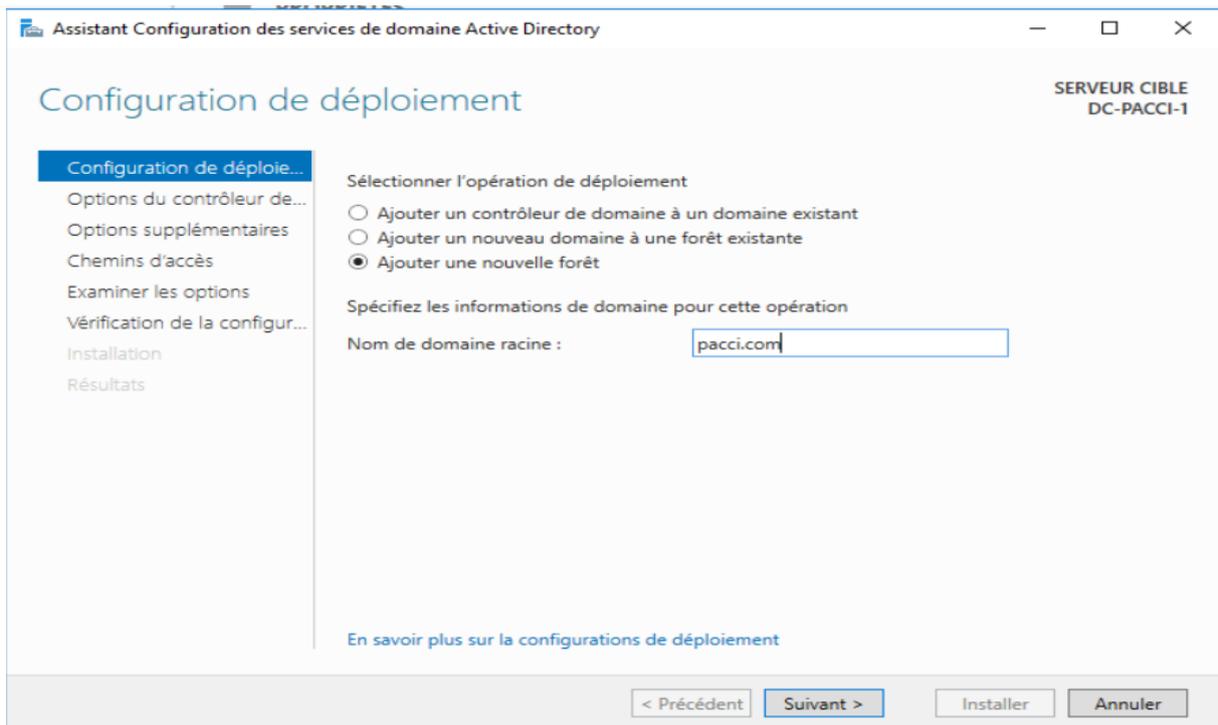
Etape 12 : installation du rôle



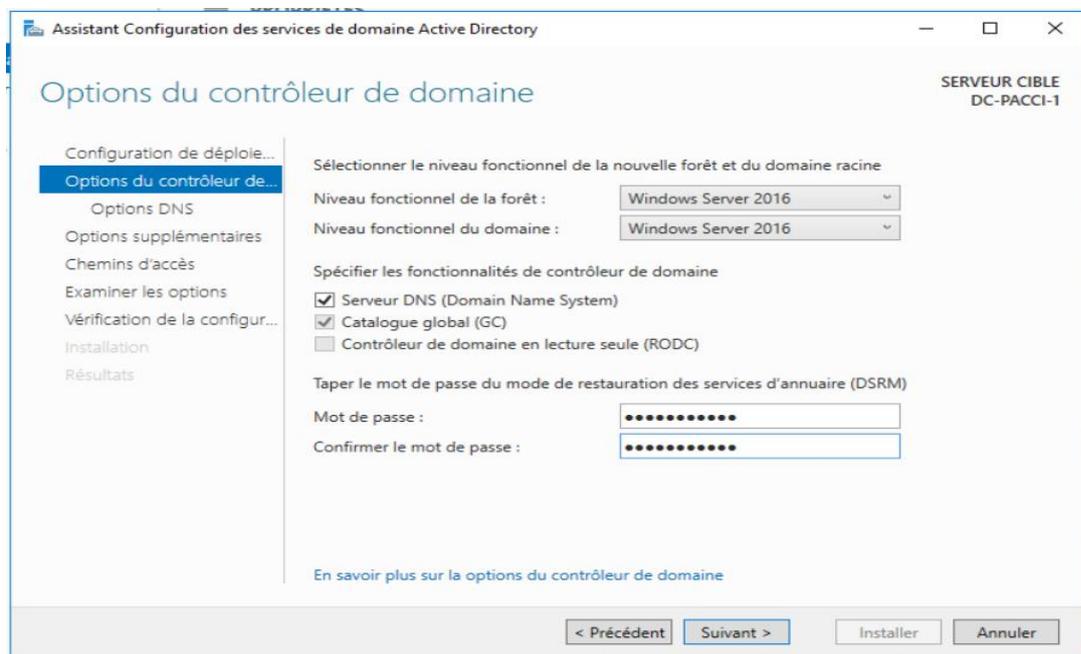
Etape 13 : Message d'avertissement de promotion du serveur en contrôleur de domaine



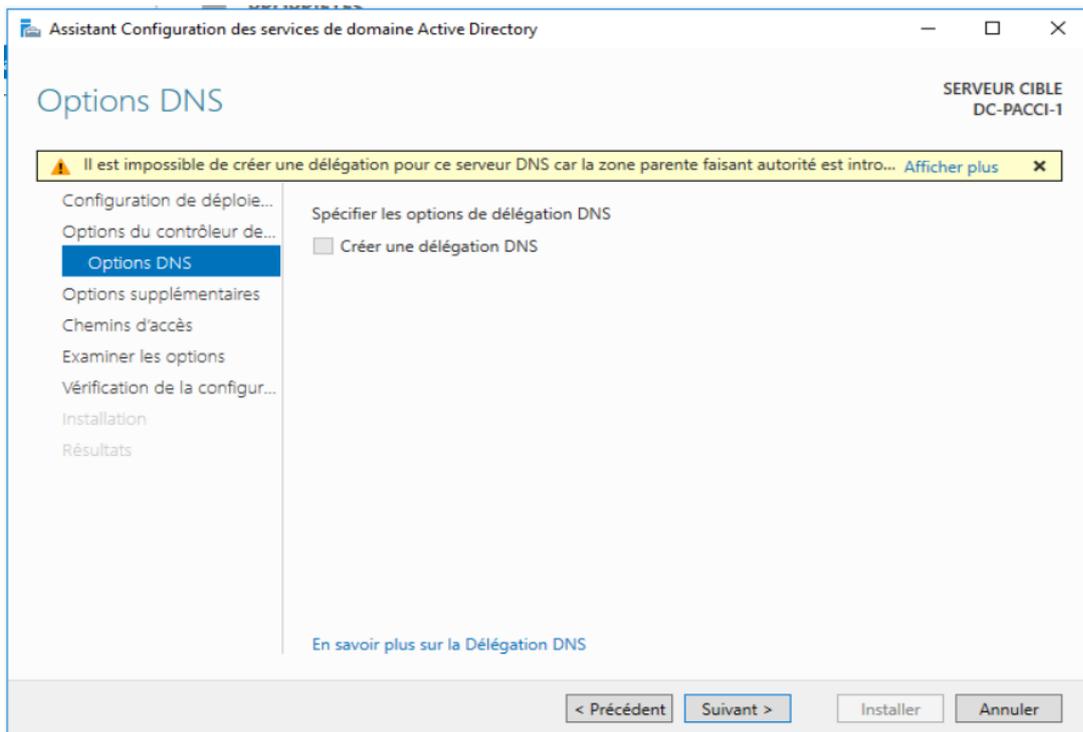
Etape 14 : Création du domaine



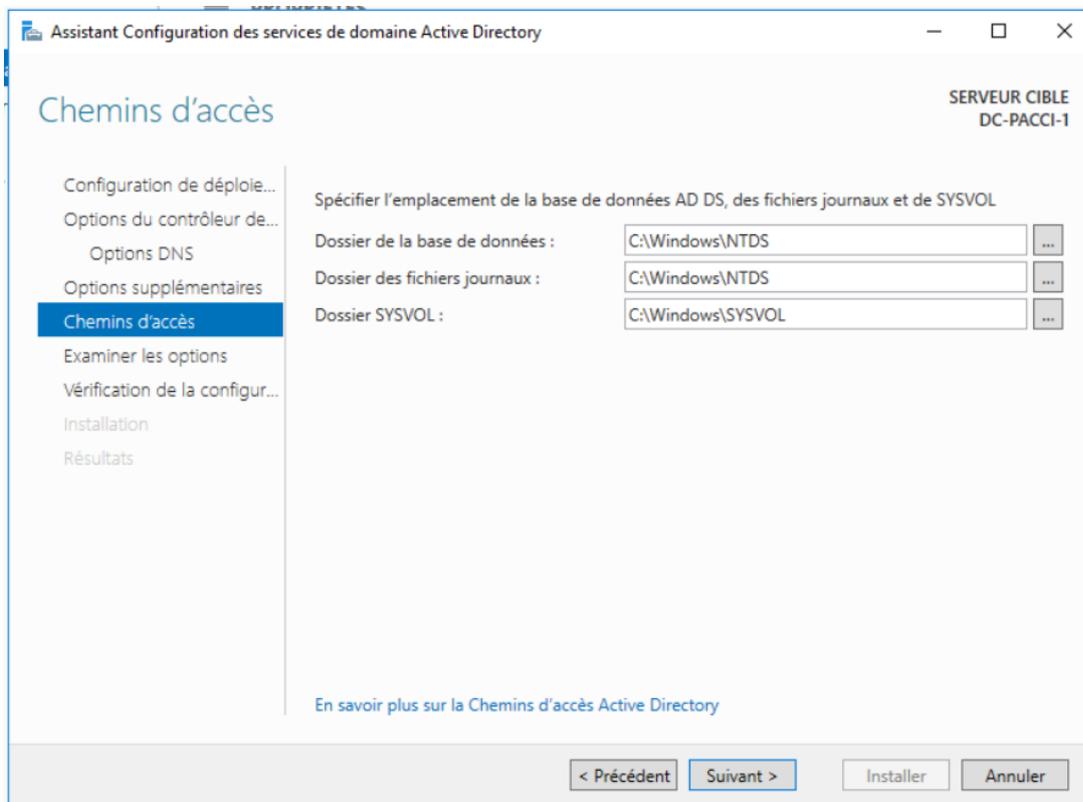
Etape 15 : Option du contrôleur de domaine



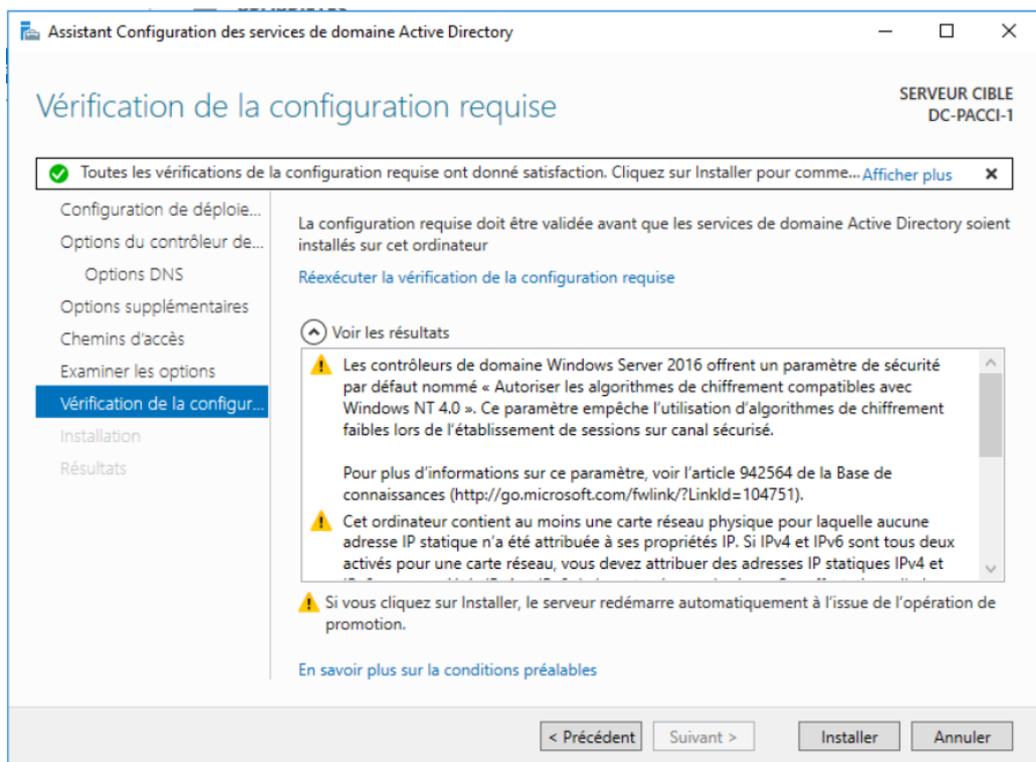
Etape 16 : Option du DNS



Etape 17 : Choix des chemins d'accès



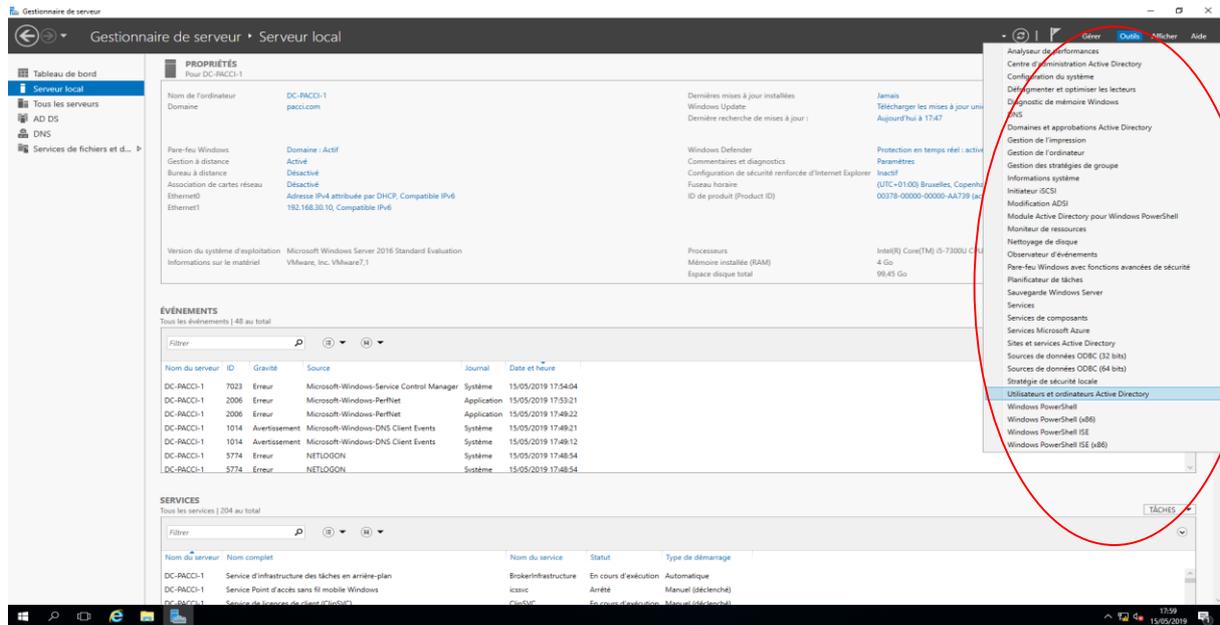
Etape 18 : Fin de la création



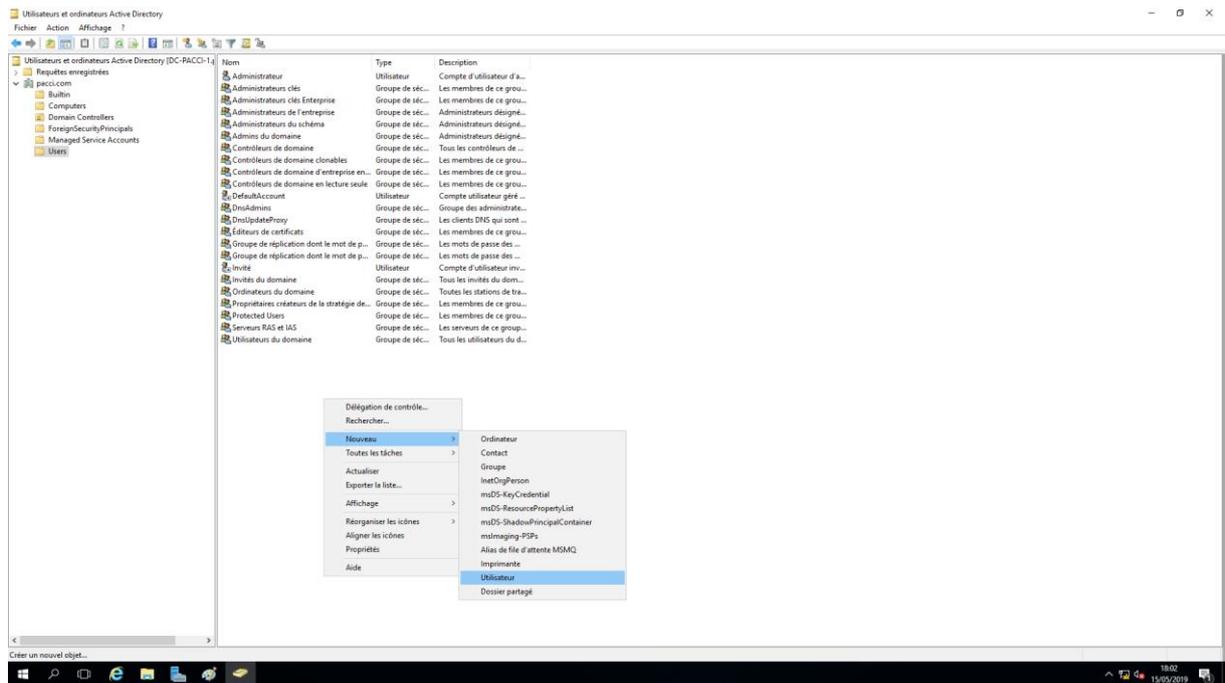
CHAPITRE III : CREATION DES OBJETS

I. CREATION D'UN COMPTE UTILISTAEUR

Etape 1 : Fenêtre des outils du serveur



Etape 2 : création d'un nouvel utilisateur



Etape 3 : Information personnel à compléter

Utilisateur : C.Fahe

Nouvel objet - Utilisateur

Créer dans : pacci.com/Users

Prénom : Cedric Initiales : CF

Nom : FAHE

Nom complet : Cedric CF. FAHE

Nom d'ouverture de session de l'utilisateur :
C.Fahe | @pacci.com

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :
PACCIN | C.Fahe

< Précédent Suivant > Annuler

Utilisateur : Boura

Nouvel objet - Utilisateur

Créer dans : pacci.com/Users

Prénom : Aristide Initiales : BA

Nom : Boura

Nom complet : Aristide BA. Boura

Nom d'ouverture de session de l'utilisateur :
Boura | @pacci.com

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

< Précédent Suivant > Annuler

Nouvel objet - Utilisateur

Créer dans : pacci.com/Users

Mot de passe : [masqué]

Confirmer le mot de passe : [masqué]

L'utilisateur doit changer le mot de passe à la prochaine ouverture de session

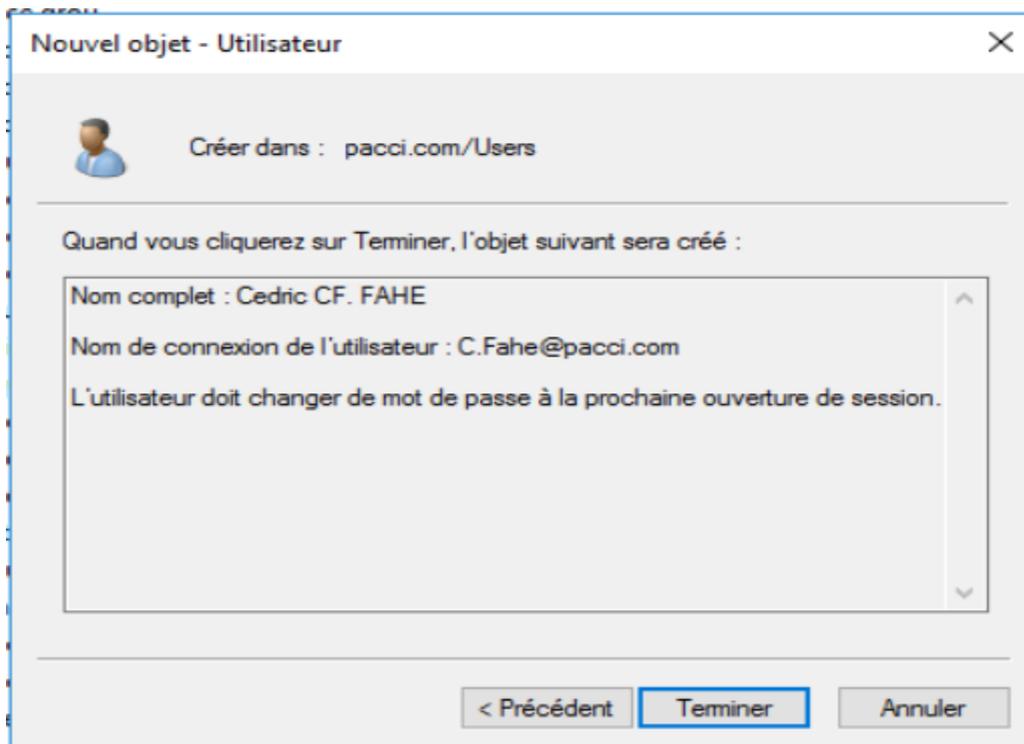
L'utilisateur ne peut pas changer de mot de passe

Le mot de passe n'expire jamais

Le compte est désactivé

< Précédent Suivant > Annuler

Etape 4 : fin de la création

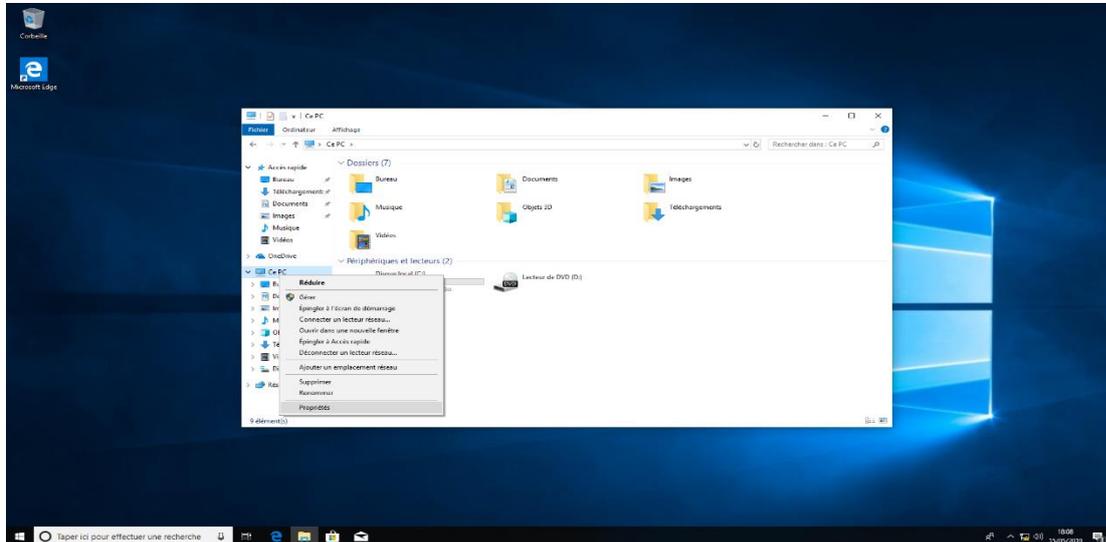


Vue des comptes créés

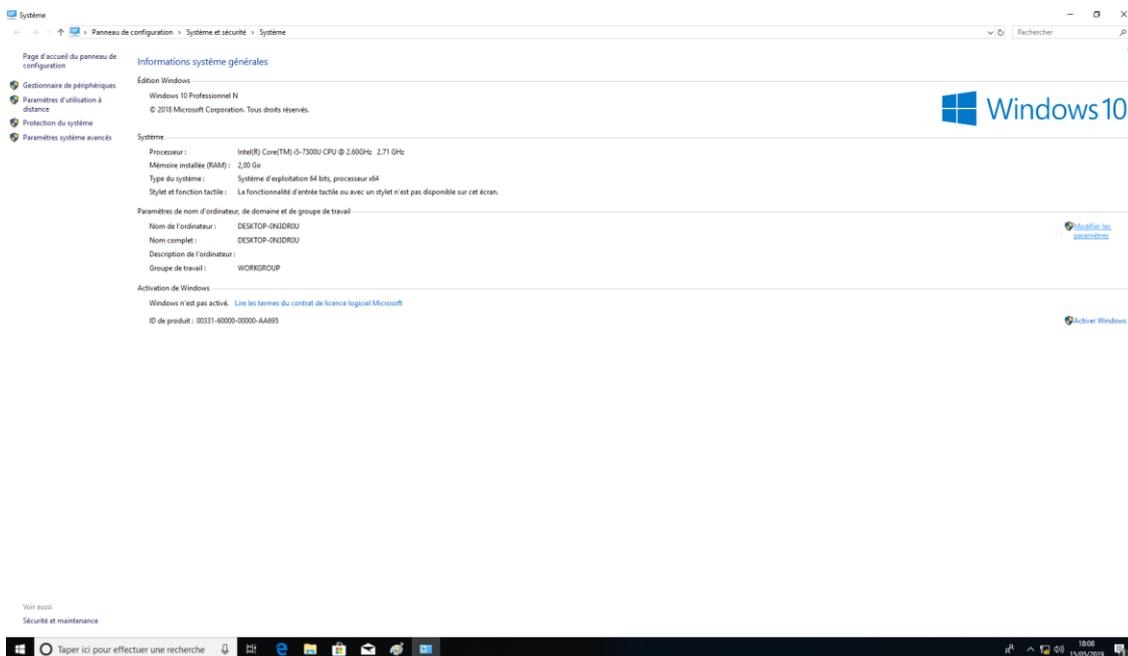
	Nom	Type	Description
Utilisateurs et ordinateurs Active			
> Requetes enregistrées			
▼ pacci.com			
> BuiltIn			
> Computers			
> Domain Controllers			
> ForeignSecurityPrincipal:			
> Managed Service Account			
Users			
	Administrat...	Utilisateur	Compte d'utilisateur d'a...
	Administrat...	Groupe de séc...	Les membres de ce grou...
	Administrat...	Groupe de séc...	Les membres de ce grou...
	Administrat...	Groupe de séc...	Administrateurs désigné...
	Administrat...	Groupe de séc...	Administrateurs désigné...
	Admins du ...	Groupe de séc...	Administrateurs désigné...
	Aristide BA. ...	Utilisateur	
	Cedric CF. F...	Utilisateur	
	Contrôleurs ...	Groupe de séc...	Tous les contrôleurs de ...
	Contrôleurs ...	Groupe de séc...	Les membres de ce grou...
	Contrôleurs ...	Groupe de séc...	Les membres de ce grou...
	Contrôleurs ...	Groupe de séc...	Les membres de ce grou...
	DefaultAcco...	Utilisateur	Compte utilisateur géré ...

II. CONNEXION D'UN NOUVEL UTILISATEUR

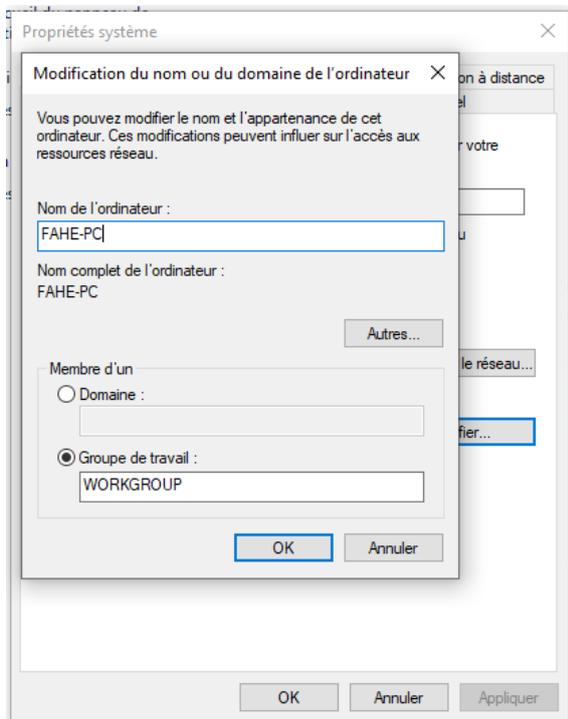
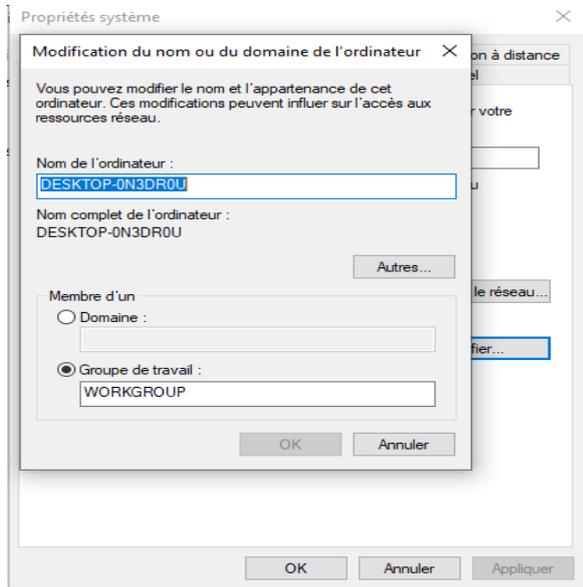
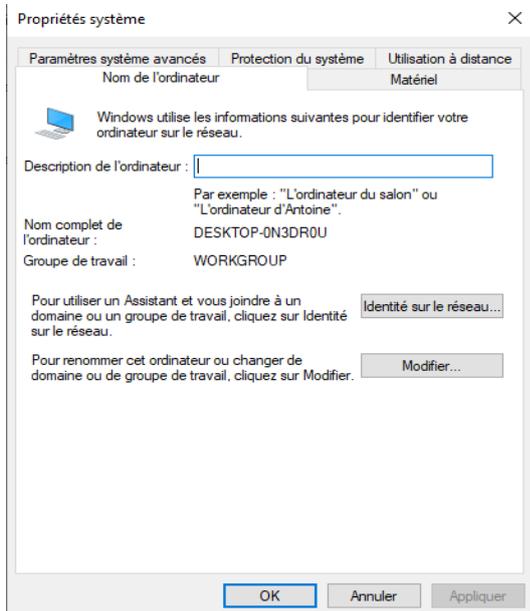
Menu : ouverture Propriété ordinateur



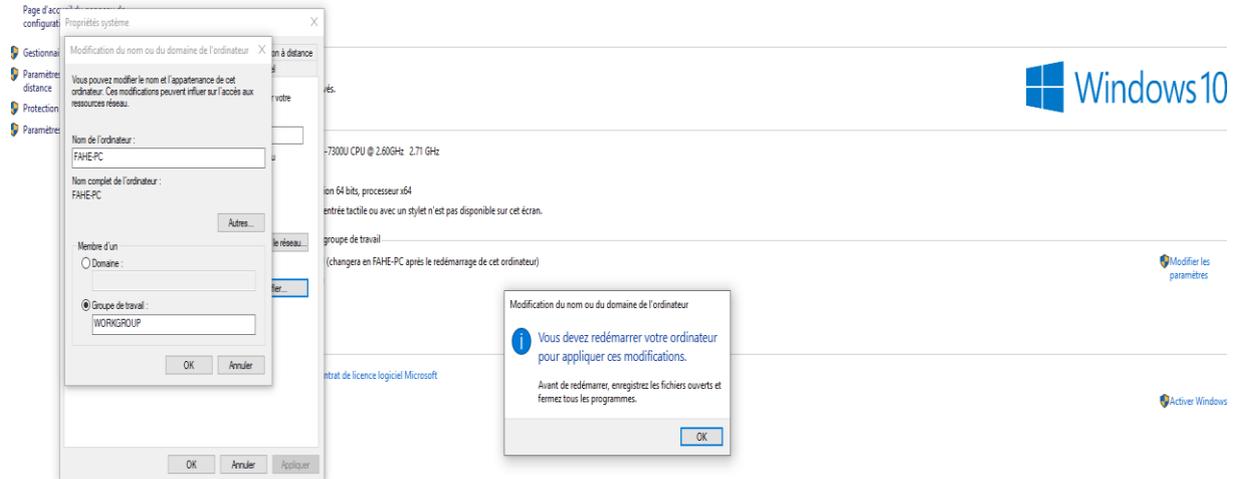
Propriété ordinateur



Modification des propriétés de l'ordinateur



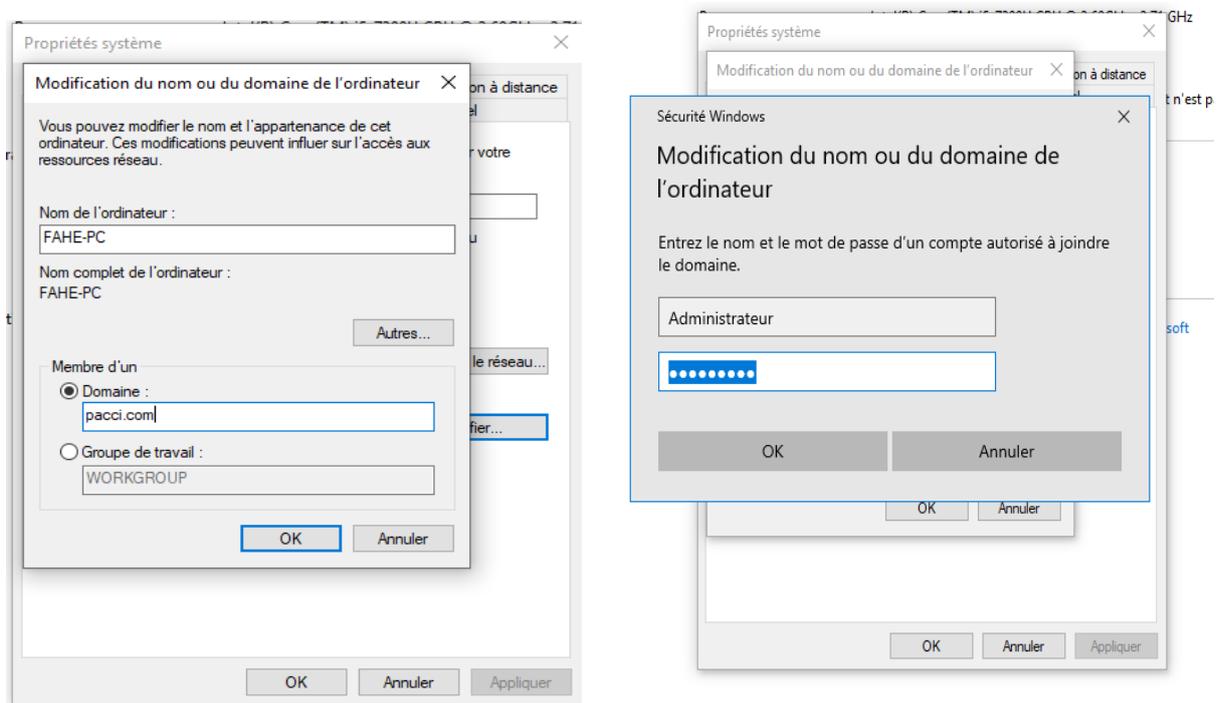
Message de redémarrage

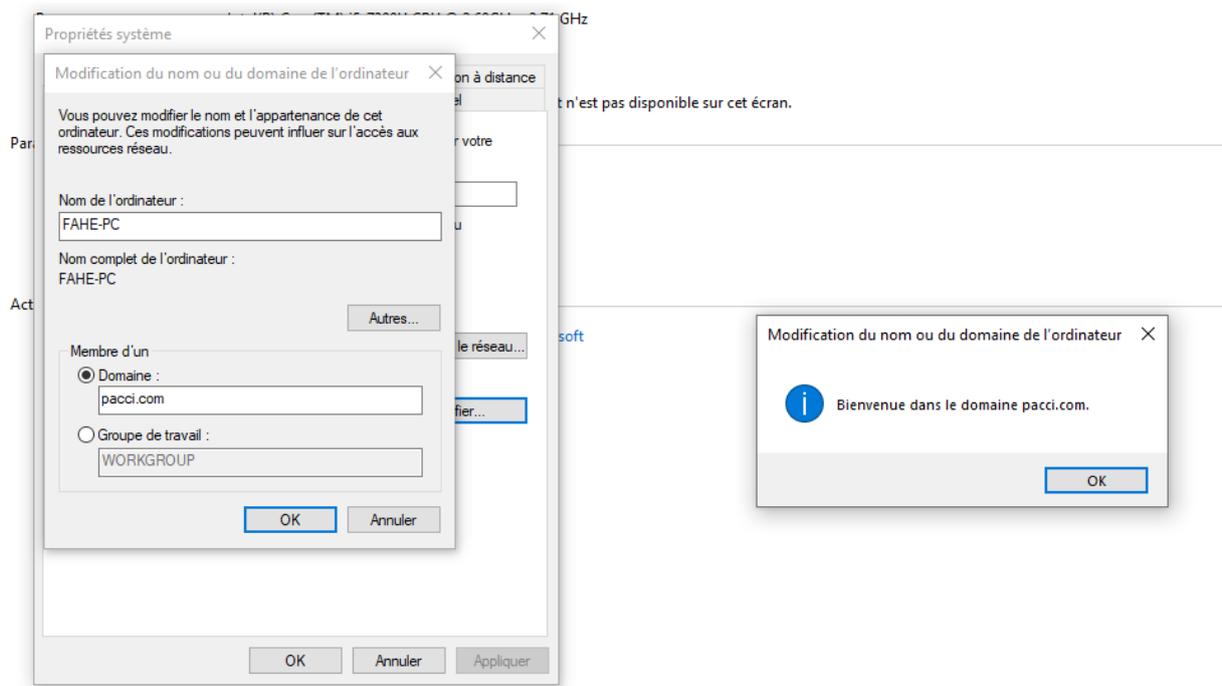


Après redémarrage de l'ordinateur

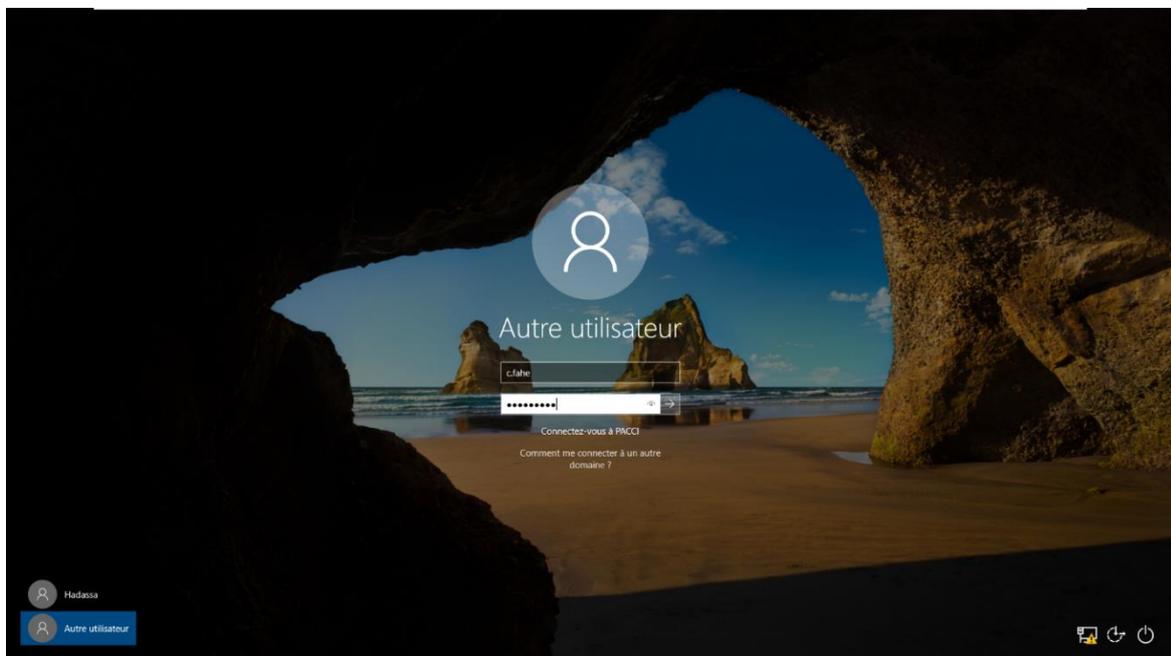
Modification des propriétés du PC

Insertion de la machine dans le domaine *pacci.com*

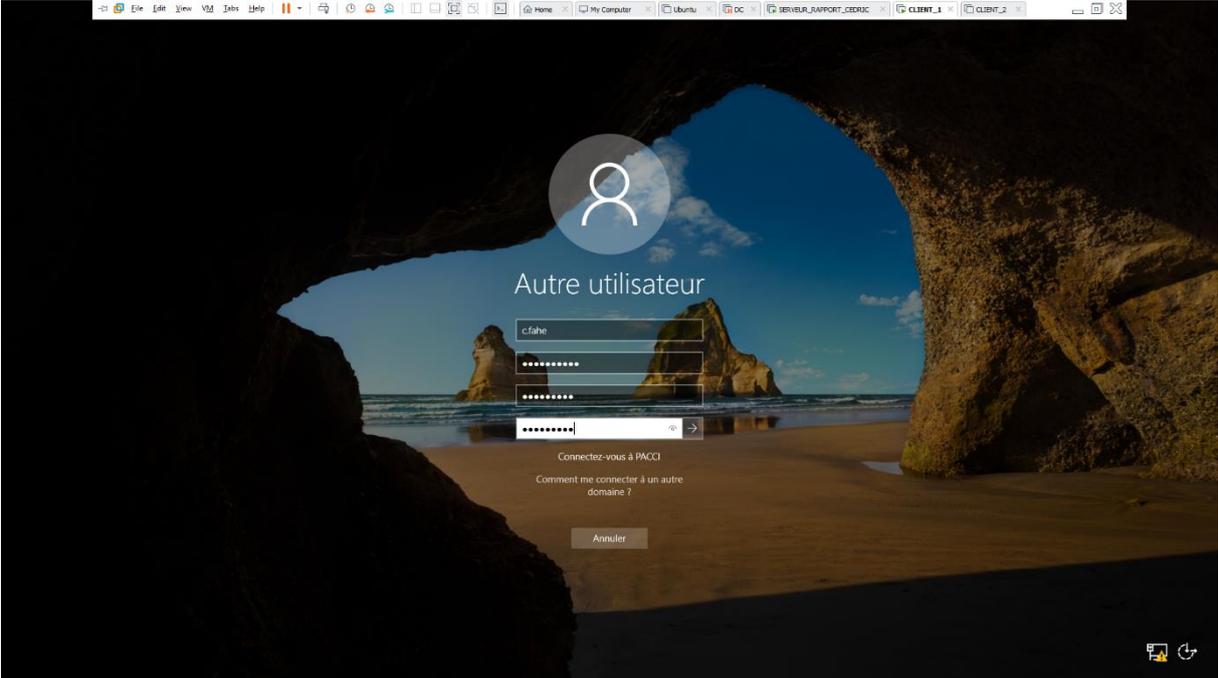




Après redémarrage, Connexion du nouvel utilisateur dans le domaine pacci.com



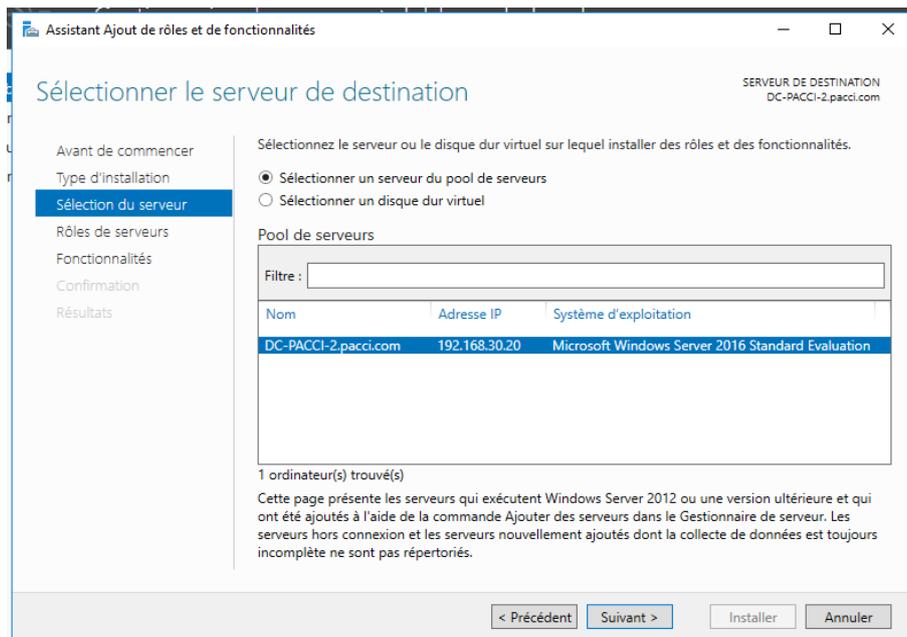
Groupe de stratégie appliqué sur le nouvel utilisateur



III. CREATION D'UN SECOND CONTROLEUR DE DOMAINE

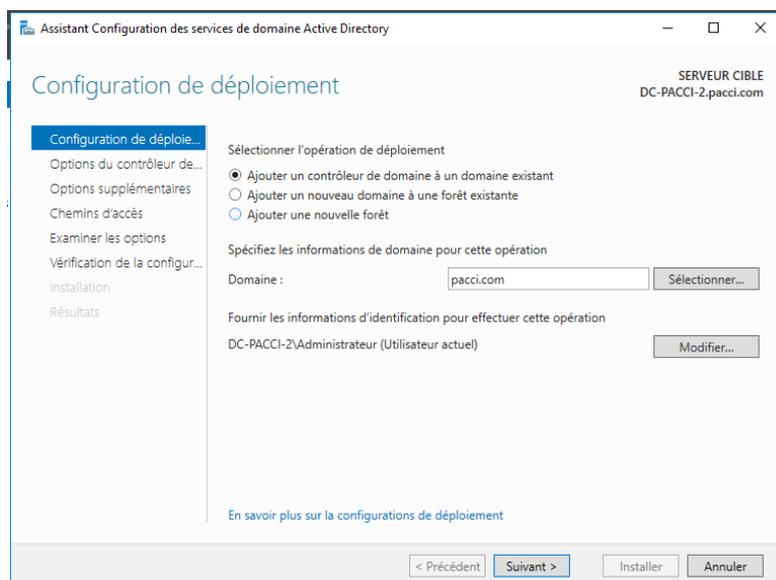
Page d'accueil du gestionnaire de serveur → Renommer le nom de l'ordinateur : DC-PACCI 2 → Désactivation du Pare feu → Propriété du serveur local → Menu d'installation du contrôleur de Domaine → Présentation de l'assistance d'installation du DC→

Choix du serveur à configurer

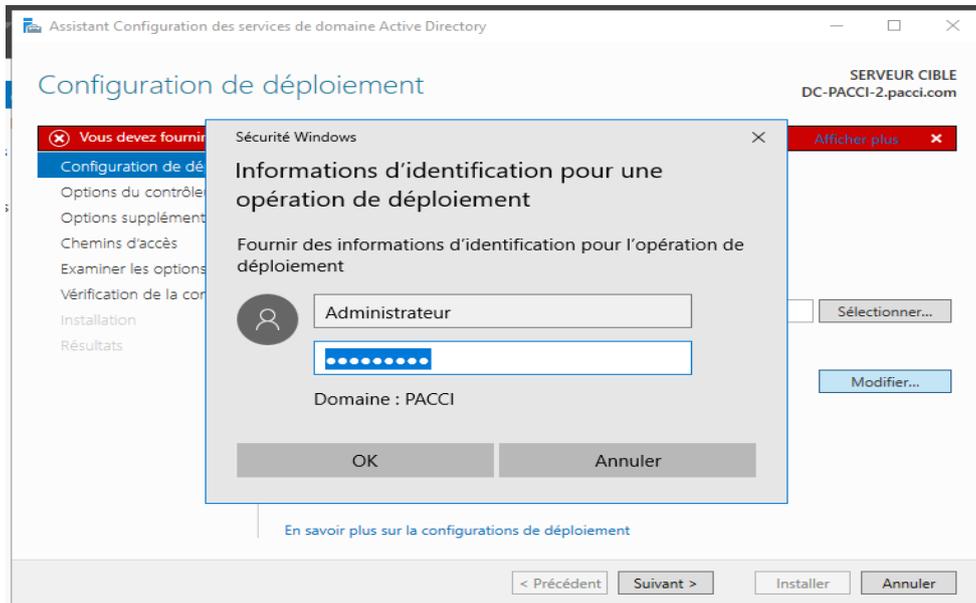


Sélection du Rôles de serveurs→ Sélection des fonctionnalités→Présentation du rôle sélectionné→confirmation du rôle→installation du rôle →Message d'avertissement de promotion du serveur en contrôleur de domaine→

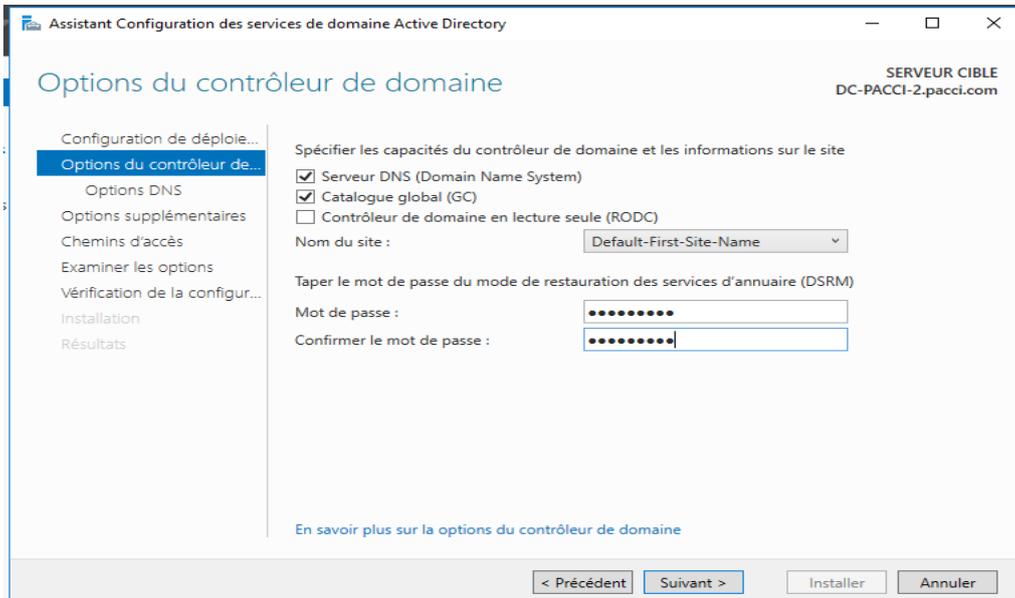
Insertion dans le domaine pacci.com



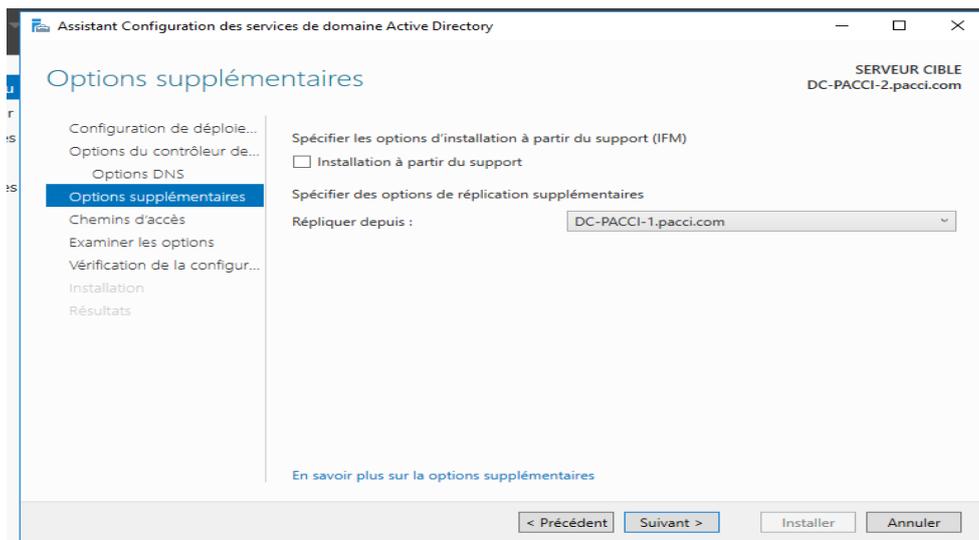
Autorisation de Déploiement



Option du contrôleur de domaine



Configuration de la réplication



Choix des chemins d'accès → redémarrage.

ARCHITECTURE RESEAU

DC-1 :192.168.30.10



DC-2 :192.168.30.20



POSTE-1 :192.168.30.31



POSTE-2 :192.168.30.32

