SERVICES D'ANNUAIRES ET ACTIVE DIRECTORY

Auteur: Bernard GIACOMONI
Autoentreprise GIACOMONI Bernard

Version	Date
1.0	12/02/2019

Table des matières

I. INTRODUCTION:....3
II. LES SERVICES D'ANNUAIRES:....4
II.1. DÉFINITIONS:....4
II.2. UTILITÉ DES ANNUAIRES INFORMATISÉS:....4
II.3. PRÉSENTATION SOMMAIRE DU PROTOCOLE L.D.A.P:....5
II.3.1. GÉNÉRALITÉS:....5
II.3.2. ORGANISATION GÉNÉRALE:....5
II.3.3. CONVENTIONS DE NOMMAGE:....6
III. PRÉSENTATION D'ACTIVE DIRECTORY:....7
III.1. GÉNÉRALITÉS:....7
III.2. PRINCIPES:....7
III.3. ORGANISATION GLOBALE:....8
III.4. STRUCTURE LOGIQUE GÉNÉRALE:....9
III.5. NOMMAGE DES OBJETS:....10
III.5.1. IDENTIFIANT UNIQUE D'UN OBJET:....10
III.5.2. NOM CANONIQUE UNIQUE D'UN OBJET:....10
III.5.3. IDENTIFIANT GLOBAL UNIQUE D'UN OBJET:....10
III.5.4. NOM D'UTILISATEUR PRINCIPAL:....10
III.6. DESCRIPTION DES DIFFÉRENTS OBJETS:....10
III.6.1. LES OBJETS TERMINAUX:....10
III.6.1.1. NATURE DES OBJETS TERMINAUX:....10
III.6.1.2. NOTION DE SCHÉMA:....11
III.6.2. LES OBJETS NON TERMINAUX:....11
III.6.2.1. LES UNITÉS D'ORGANISATION (O.U):....11
III.6.2.2. LES GROUPES D'UTILISATEURS:....11
III.6.2.3. LES "STRATÉGIE DE GROUPES":....11
III.6.2.4. LES DOMAINES:....12
III.7. RELATIONS D'APPROBATION ENTRE DOMAINES:....13
III.7.1. PRINCIPE:....13
III.7.2. EXEMPLE: APPROBATION KEREBOS:....13
III.8. RÉPLICATION, NOTION DE PARTITION:....14
IV. INSTALLATION DU SERVICE ACTIVE DIRECTORY:....15
IV.1. GÉNÉRALITÉS:....15
IV.2. CONFIGURER LA CONNEXION RÉSEAU EN IP FIXE:....15
IV.3. INSTALLER LES FONCTIONNALITÉS ACTIVE DIRECTORY DANS LA MACHINE:....17
IV.4. CONFIGURER LE SERVEUR DE DOMAINE A.D:....18
IV.4.1. ACTIVATION DE l'ASSISTANT D'INSTALLATION:....18
IV.4.2. DÉTERMINATION DE LA POSITION DU DOMAINE DANS L'ARBORESCENCE GÉNÉRALE:....20
IV.4.3. NOMMAGE DU NOUVEAU DOMAINE ACTIVE DIRECTORY:....21
IV.4.4. DÉTERMINATION DU "NOM NETBIOS" DU DOMAINE:....22
IV.4.5. DÉTERMINATION DU NIVEAU FONCTIONNEL DE LA FORÊT:....22
IV.4.6. VÉRIFICATION DU RÔLE DE SERVEUR DNS:....22
IV.4.7. DÉTERMINATION DE CERTAINS NOMS DE DOSSIERS ET CHEMINS D'ACCÈS:....23
IV.4.8. DÉTERMINATION DU MOT DE PASSE DE RESTAURATION:....23
IV.4.9. FIN DE L'INSTALLATION:....23
IV.5. INTÉGRATION D'UN POSTE CLIENT DANS UN DOMAINE ACTIVE DIRECTORY:....24
IV.5.1. REMARQUE PRÉLIMINAIRE:....24
IV.5.2. PROCÉDURE CÔTE SERVEUR:....24
IV.5.3. PROCÉDURE CÔTE CLIENT:....24

I. INTRODUCTION:

Ce document a pour objet d'expliquer les missions et fonctionnalités caractéristiques des SERVICES D'ANNUAIRES informatisés en les illustrant à travers une présentation de l'outil ACTIVE DIRECTORY de WINDOWS.

Après un premier chapitre consacré aux aspects fonctionnels liés aux services d'annuaires, au protocole LDAP et aux principes de description des données qui lui sont rattachés, l'ouvrage se poursuit par une présentation détaillée de l'outil ACTIVE DIRECTORY: principes généraux, organisation globale, conventions de nommage, etc.

Les chapitres suivants sont consacrés à l'installation d'Active Directory sur un poste équipé d'un système d'exploitation WINDOWS SERVER et à la création d'une amorce d'annuaire.

REMARQUE: Les menus d'installation d'ACTIVE DIRECTORY présentés ici correspondent à la version WINDOW SERVER 2008 R2. Cette version qui peut être installée gratuitement pendant une période d'essai de 6 mois permet de constituer facilement un atelier d'entraînement local, le plus simple étant d'installer cette version dans une machine virtuelle à l'intérieur d'un poste WINDOWS.

II. LES SERVICES D'ANNUAIRES:

II.1. DÉFINITIONS:

Un ANNUAIRE désigne un mode d'organisation de données permettant à des utilisateurs de retrouver facilement et rapidement des informations se rapportant à des OBJETS d'un type donné (ces objet peuvent être, par exemple, des abonnées au téléphone fixe, des sites internet, des annonceurs, etc..).

Un SERVICE D'ANNUAIRE est un logiciel qui permet de gérer et d'utiliser un annuaire, c'est à dire:

- L'ADMINISTRER: créer, supprimer, modifier des objets, les rendre accessibles aux utilisateurs, contrôler l'accès aux informations, etc.;
- L'UTILISER: permettre au public autorisé d'accéder aux informations.

Un SERVICE D'ANNUAIRE est donc un SYSTÈME DE GESTION D'ANNUAIRE (comme il existe des systèmes de gestion de bases de données).

EXEMPLE: Un annuaire téléphonique contient des informations sur des «objets» appelés «abonnés au téléphone». Ces objets (abonnées) sont repérés par leur nom, leurs prénoms, leur adresse postale et leur numéro de téléphone. L'organisation des données est dans ce cas HIÉRARCHIQUE (classement par pays, départements et communes). Un utilisateur connaissant le nom et le(s) prénom(s) d'un abonné et sa commune de résidence peut accéder grâce à l'annuaire à un certain nombre d'informations concernant cet abonné, et en particulier à son numéro de téléphone.

II.2. UTILITÉ DES ANNUAIRES INFORMATISÉS:

Lorsqu'un système d'informations atteint une certaine dimension, les utilisateurs et les administrateurs du système informatique (surtout s'il est réparti) ne sont plus en capacité de mémoriser les renseignements nécessaires à l'utilisation des ressources dont ils ont besoin.

De plus, il est dans ce cas pratiquement impossible de disposer de documents à jour répertoriant la totalité des ressources offertes par ce système et leur état de disponibilité à un instant donné. En effet:

- La liste de ces ressources varie constamment au grès de l'évolution des besoins;
- Ces ressources peuvent être situées à de grandes distances des utilisateur (à un autre étage, dans un autre bâtiment, dans une autre implantation, etc.).

De ce fait, disposer d''un outil informatique donnant accès "en temps réel" à la liste des ressources disponibles devient pratiquement indispensable si l'on veut éviter que les utilisateurs passent une grande partie de leur temps à rechercher ces ressources.

Un outil informatique de ce type, permettant à un utilisateur donné d'accéder à la liste des ressources informatiques de l'organisation, accompagnée pour chaque d'entre elles des informations nécessaires à son utilisation depuis le poste de l'utilisateur est appelé SERVICE D'ANNUAIRE.

II.3. PRÉSENTATION SOMMAIRE DU PROTOCOLE L.D.A.P:

II.3.1. GÉNÉRALITÉS:

Un certain nombre de protocoles de gestion d'annuaires distribués ont été définis. L'un des plus connus est L.D.A.P (Lightweight Directory Access Protocol), qui est utilisé par le service d'annuaire ACTIVE DIRECTORY de Microsoft.

LDAP est un protocole dont la finalité est la gestion d'un SERVICE D'ANNUAIRE DISTRIBUÉ (création, modification, interrogation de l'annuaire). LDAP utilise TCP/IP pour communiquer sur le réseau de l'organisation à laquelle l'annuaire est dédié.

Actuellement, il est devenu une norme incluant:

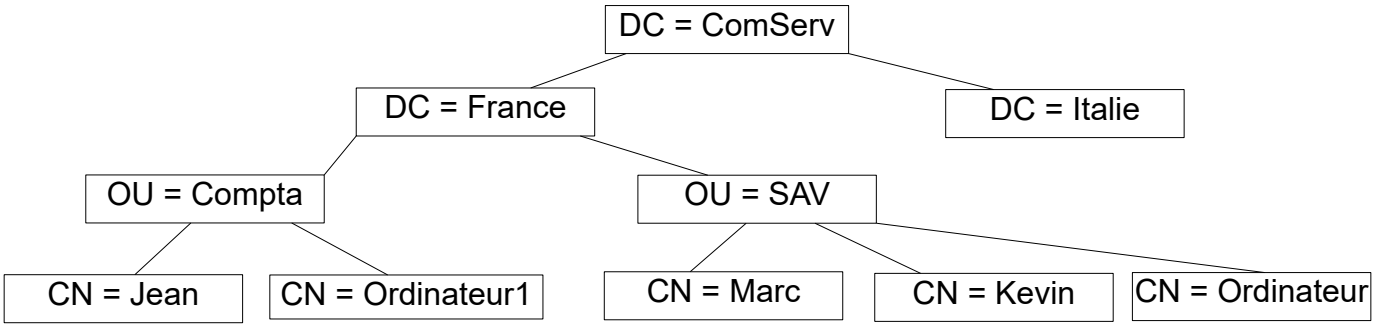
- un modèle de données;
- un modèle de nommage;
- un modèle fonctionnel;
- un modèle de sécurité;
- un modèle de réplication des annuaires.

II.3.2. ORGANISATION GÉNÉRALE:

L'annuaire est décrit sous la forme d'une ARBORESCENCE dont les nœuds terminaux sont les OBJETS gérés par cet annuaire (décrits sous la forme d'attributs associés à des valeurs) et dont les nœuds non terminaux sont des CONTENEURS:

- Les nœuds les plus "profonds" de l'arborescence représentent soit des OBJETS terminaux à gérer (ex: personnes, équipements, logiciels, etc), désignés par un NOM COMMUN (C.N), soit des CONTENEURS regroupant ces objets en UNITÉS D'ORGANISATION (O.U).
- Les nœuds des niveaux élevés représentent des COMPOSANTS DE DOMAINES (Domain Composants: DC), concept proche de celui des domaines et sous-domaines d'un réseau.

EXEMPLE: Arborescence d'une entreprise internationale ComServ :



A chaque nœud pourront être associés des ATTRIBUTS correspondant à des VALEURS: au nœud terminal Jean de l'O.U. Compta pourront être associés les attributs Nom, Prénom, Fonction, etc.

II.3.3. CONVENTIONS DE NOMMAGE:

DISTINGUISHED NAME:
Les conventions de nommage permettent d'identifier chaque objet terminal par une chaîne de caractères appelée "distinguished name" (D.N), équivalente à son "nom propre".

EXEMPLE: Dans l'arborescence précédente, l'ordinateur n°1 du service après vente aura pour D.N:

"CN=Ordinateur1, OU=SAV, DC=France, DC=Comserv"

CANONICAL NAME:

Il est également possible de nommer un objet en utilisant les conventions utilisés par les serveurs D.N.S: les composants de domaines sont assimilés à des domaines et sous-domaines de l'adressage URL et les composants inférieurs sont assimilés à des répertoires, sous-répertoires et fichiers. Cette dénomination s'appelle NOM CANONIQUE (Canonical name ou C.N).

EXEMPLE: Dans l'arborescence précédente, l'ordinateur n° 1 du service après vente aura pour C.N:

"France.Comserv\SAV\Ordinateur1"

III. PRÉSENTATION D'ACTIVE DIRECTORY:

III.1. GÉNÉRALITÉS:

ACTIVE DIRECTORY (A.D) est le SERVICE d'ANNUAIRE de Microsoft. Il permet de gérer les données d'un ANNUAIRE dont les données sont réparties sur plusieurs postes informatiques reliés par un réseau. Il utilise pour cela le protocole L.D.A.P (Lightweight Directory Access Protocol).

C'est un outil d'administration qui permet d'une part de gérer (créer, maintenir à jour, sécuriser) un ANNUAIRE rassemblant des renseignement sur les différentes ressources partageables d'un SYSTÈME INFORMATIQUE, et d'autre part d'accéder à ces renseignements depuis différents postes de travail connectés au système.

NOTA: *On entend ici par système informatique un certain nombre de moyens informatiques (ordinateurs, imprimantes, scanners, etc.) connectés au réseau général d'une organisation (entreprise, administration, association, etc.).*

Du point de vue informatique, l'outil A.D. est intégré en tant que RÔLE aux systèmes d'exploitation MICROSOFT WINDOWS SERVER.

III.2. PRINCIPES:

L'outil A.D permet de:

- Organiser les objets de façon hiérarchique;
- Contrôler les accès aux objets et la sécurité des données;
- Fournir des informations sur ces objets.

Un UTILISATEUR d"A.D emploie cet outil pour accéder à des ressources partagées (Ex: une imprimante, un fichier, etc..). Ces ressources sont situés sur différentes machines d'un réseau d'entreprise (LAN, Réseau étendu, etc.). A.D permet à tout utilisateur titulaire d'un COMPTE d'accéder aux ressources partageables du système, quelle que soient leurs localisation, sous réserve que les DROITS accordés à son compte le lui permettent.

Un ADMINISTRATEUR d'A.D emploie cet outil pour:

- CRÉER et GÉRER l'ANNUAIRE des ressources partageables disponibles sur le réseau administré (comptes utilisateurs, serveurs, postes de travail, dossiers partagés, imprimantes, etc);
- CONTRÔLER L'UTILISATION de ces ressources par les utilisateurs (distribution, duplication, partitionnement, sécurisation des accès, attribution de droits);
- DISTRIBUER et DÉPLOYER des logiciels;
- INSTALLER DES MISES À JOUR critiques;
- RÉPLIQUER l'annuaire en fonction des besoins et assurer la SAUVEGARDE des données qu'il renferme.

III.3. ORGANISATION GLOBALE:

Un réseau Active Directory est composé:

- De postes SERVEURS qui gèrent l'ANNUAIRE global des ressources disponibles. Ces serveurs sont équipés de systèmes d'exploitation WINDOWS SERVERS;
- De postes CLIENTS qui permettent aux utilisateurs d'accéder à ces ressources pour les utiliser. Ces postes sont équipés de systèmes d'exploitation WINDOWS CLIENTS.

Les deux rôles ne peuvent être supportés que par des systèmes WINDOWS en version «professionnelle». Un serveur informatique hébergeant un annuaire ACTIVE DIRECTORY est appelé CONTRÔLEUR DE DOMAINE.

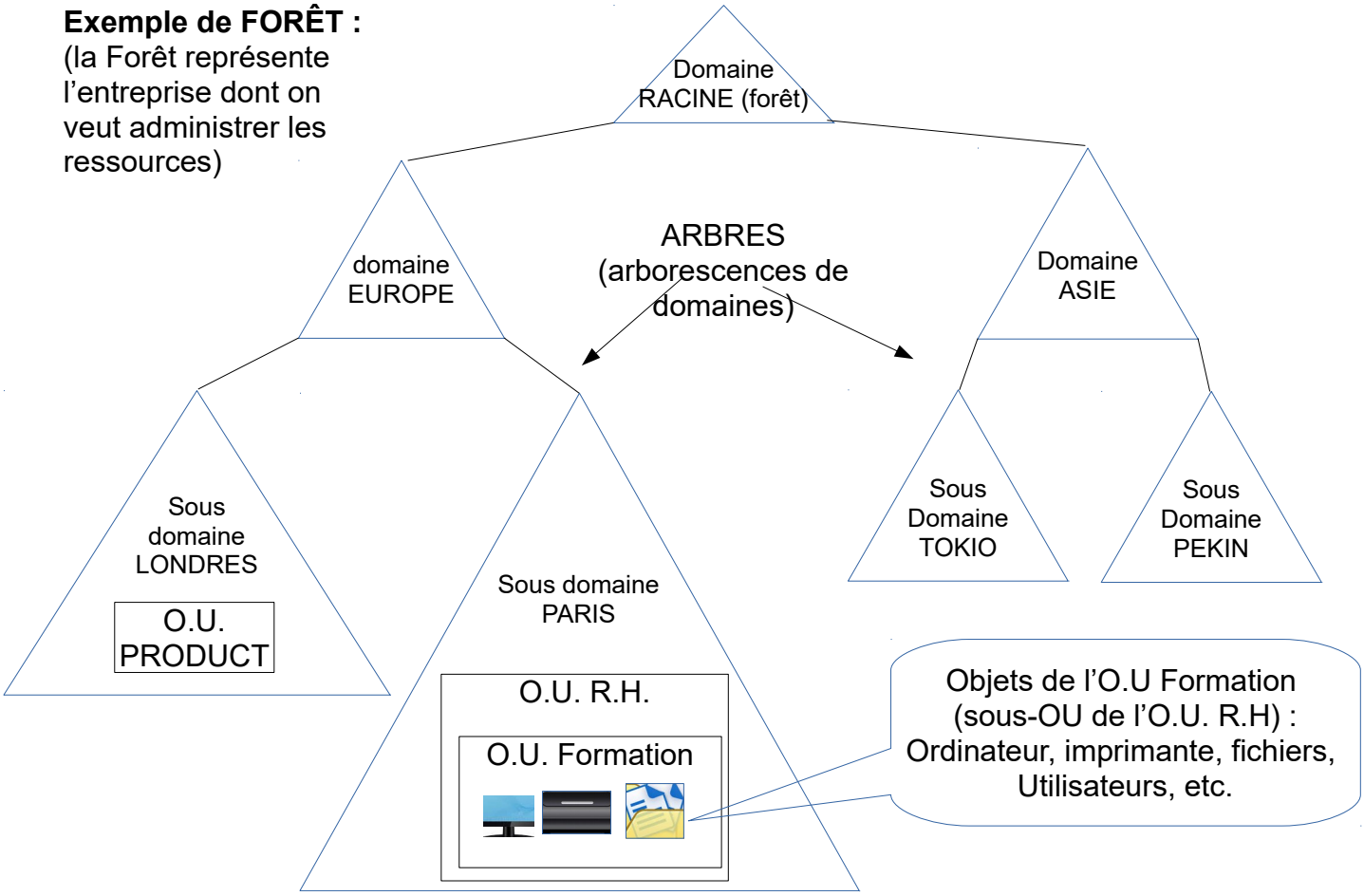
Un système A.D peut inclure plusieurs contrôleurs de domaines. Chacun de ces contrôleurs possède une copie de l'annuaire global. Un système de mise à jour (réplication de l'arborescence) permet de maintenir la cohérence en répercutant sur tous les serveurs les modifications effectuées sur l'un d'entre eux.

III.4. STRUCTURE LOGIQUE GÉNÉRALE:

A.D. S'appuie sur le modèle initié par LDAP pour organiser les données qu'il gère: les différents objets du système informatique sont organisés sous la forme d'une HIÉRARCHIE d'entités:

- Les entités terminales de cette hiérarchie (les "feuilles" de l'arbre) sont les OBJETS gérés par le système (équipements matériels, logiciels, fichiers, etc.);
- Ces objets sont englobés dans des CONTENEURS appelés UNITÉS D'ORGANISATION (O.U);
- Les UNITÉS D'ORGANISATION peuvent elles-mêmes être englobées par des unités d'organisation de rang supérieur ou par des DOMAINES;
- Un DOMAINE peut être un sous-domaines d'un domaines englobant: les domaines PARIS et LONDRES peuvent être des sous-domaines d'un domaine EUROPE;
- Une hiérarchie de domaines est appelée ARBRE.
- Plusieurs ARBRES constituent une FORÊT. La FORÊT correspond généralement à l'organisation globale.

Le schéma ci-dessous donne une représentation graphique de cette organisation:



REMARQUE: l'administrateur est libre de donner à chaque nœud de la hiérarchie la destination qu'il veut: ainsi, rien n'empêche de représenter une implantation avec une O.U.

ou de définir un sous-domaine RH. Remarquons tout de même qu'à chaque domaine correspond un Contrôleur de Domaine qui le gère et inversement. Un domaine ou sous-domaine est donc un nœud du réseau "physique".

III.5. NOMMAGE DES OBJETS:

III.5.1. IDENTIFIANT UNIQUE D'UN OBJET:

Chacun des objet de l'arborescence peut être repéré par un IDENTIFIANT UNIQUE appelé DN (pour Distinguished Name). Active Directory respecte la convention LDAP:

EXEMPLE: Dans le schéma précédent, l'imprimante de l'O.U "Formation" aura pour "distinguished name" la chaîne:

"CN=Epsom660_S34, OU=Formation, OU=RH, DC=PARIS, DC=EUROPE"

NOTA: Le nom commun (CN) peut être utilisé comme identifiant unique "relatif" dans l'O.U. qui englobe l'objet.

III.5.2. NOM CANONIQUE UNIQUE D'UN OBJET:

Le NOM CANONIQUE (Canonical Name) est une autre façon d'identifier d'une manière unique un objet de l'arborescence. Là encore, A.D. respecte les conventions LDAP:

EXEMPLE: Dans le schéma précédent, l'imprimante de l'O.U "Formation" aura pour "Canonical Name" la chaîne:

"PARIS.EUROPE/RH/Formation/Epsom660_S34"

III.5.3. IDENTIFIANT GLOBAL UNIQUE D'UN OBJET:

Chaque objet possède également un Identifiant Global Unique (GUID, pour Globally Unique Identifier). Celui-ci est une chaîne de caractères de 128 bits unique et non modifiable, utilisée par AD pour les opérations de recherche et de réplication.

III.5.4. NOM D'UTILISATEUR PRINCIPAL:

Les objets utilisateurs possèdent également un Nom d'Utilisateur principal (UPN, pour User Principal Name) qui permet de les identifier à l'intérieur de leur domaine. Celui-ci se présente sous la forme d'une adresse de messagerie internet:

<nom d'objet>@<nom de domaine>

III.6. DESCRIPTION DES DIFFÉRENTS OBJETS:

III.6.1. LES OBJETS TERMINAUX:

III.6.1.1. NATURE DES OBJETS TERMINAUX:

A.D structure les entités constituant le système d'information sous la forme d'une organisation HIÉRARCHISÉE dont les "feuilles" sont les objets terminaux. Ces objets, qui sont des entités UNIQUES, sont classés en trois grandes catégories:

- Les RESSOURCES, qui représentent essentiellement des équipements matériels (par exemple les postes de travail, les imprimantes, les scanners, etc.);

- Les SERVICES, qui représentent des outils logiciels (par exemple, un traitement de textes, le courrier électronique, etc.);
- Les UTILISATEURS, qui renvoient à la notion de COMPTE UTILISATEUR qui permet de contrôler l'accès des utilisateurs aux différents OBJETS administrés.

III.6.1.2. NOTION DE SCHÉMA:

Les objets d'ACTIVE DIRECTORY sont décrits au moyen de SCHÉMAS. Un schéma contient des définitions de TYPES d'objets, ainsi que celle des attributs qui les caractérisent;

EXEMPLE: *un type IMPRIMANTE, aura comme attributs l'adresse IP, les fonctionnalités (couleur/noir-et-blanc, scanner), etc.*

Un TYPE joue donc le rôle d'une CLASSE de la programmation objet: on peut dire qu'un objet A.D. est "instancié" à partir d'un TYPE défini par un SCHÉMA A.D.

Définir un TYPE revient donc à créer la liste et la définition des attributs qui lui sont rattachés. Un nombre illimité de TYPES d'objets peut être défini.

Lorsqu'un schéma est appliqué à tout ou partie de la hiérarchie d'A.D, tous les objets doivent être conformes aux types définis dans ce schéma.

III.6.2. LES OBJETS NON TERMINAUX:

REMARQUE: Par rapport aux objets terminaux, ces objets sont des CONTENEURS.

III.6.2.1. LES UNITÉS D'ORGANISATION (O.U):

Les UNITÉS D'ORGANISATION (O.U) sont des CONTENEURS D'OBJETS. Elles permettent de créer des hiérarchies d'objets au sein d'un DOMAINE. Ceci permet la DÉLÉGATION DE DROITS et l'application de STRATÉGIES DE GROUPES (G.P.O).
Une unité d'organisation peut contenir une autre unité d'organisation: ceci permet de créer des arborescences d'objet au cœur d'un domaine.

III.6.2.2. LES GROUPES D'UTILISATEURS:

Les groupes d'utilisateurs sont des conteneurs qui rassemblent des objets utilisateurs. Cette notion permet de déléguer les droits du groupe aux utilisateurs qu'il renferme.

III.6.2.3. LES "STRATÉGIE DE GROUPES":

Les G.P.O (Group Policy Object) ne doivent pas être confondus avec la notion de groupe d'utilisateur: ils définissent des stratégies de groupe applicables aux Sites, Domaines et O.U. Une stratégie de groupe permet de restreindre la possibilité de certains utilisateurs d'effectuer certaines actions, comme par exemple l'accès à certaines ressources ou à certains exécutables.

Il existe trois types de G.P.O:

Groupe Local (L.G)	S'appliquent aux utilisateurs du domaine et aux utilisateurs appartenant à des GG ou UG d'autres domaines.
Groupe Global (G.G)	S'appliquent uniquement aux utilisateurs du domaine
Groupe Universel (U.G)	S'appliquent aux groupes et utilisateurs d'autres domaines.

III.6.2.4. LES DOMAINES:

Les domaines sont les composants qui constituent les nœuds de l'arborescence Active Directory au niveau "réseau". Rappelons qu'une arborescence de domaines constitue un ARBRE et que l'ensemble des arbres constitue la FORÊT (racine de l'ANNUAIRE de l'organisation).

L'arborescence des domaines A.D. peut être "superposée" à l'arborescence DNS du réseau.

III.7. RELATIONS D'APPROBATION ENTRE DOMAINES:

III.7.1. PRINCIPE:

Afin de permettre à un utilisateur d'un domaine d'accéder aux ressources d'un autre domaine, A.D. utilise un mécanisme basé sur des relations d'APPROBATION et d'AUTHENTIFICATION. Ces relations permettent d'accorder aux utilisateurs des permissions d'accès dans des domaines différents de celui auquel ils appariennent. Ces relations peuvent concerner:

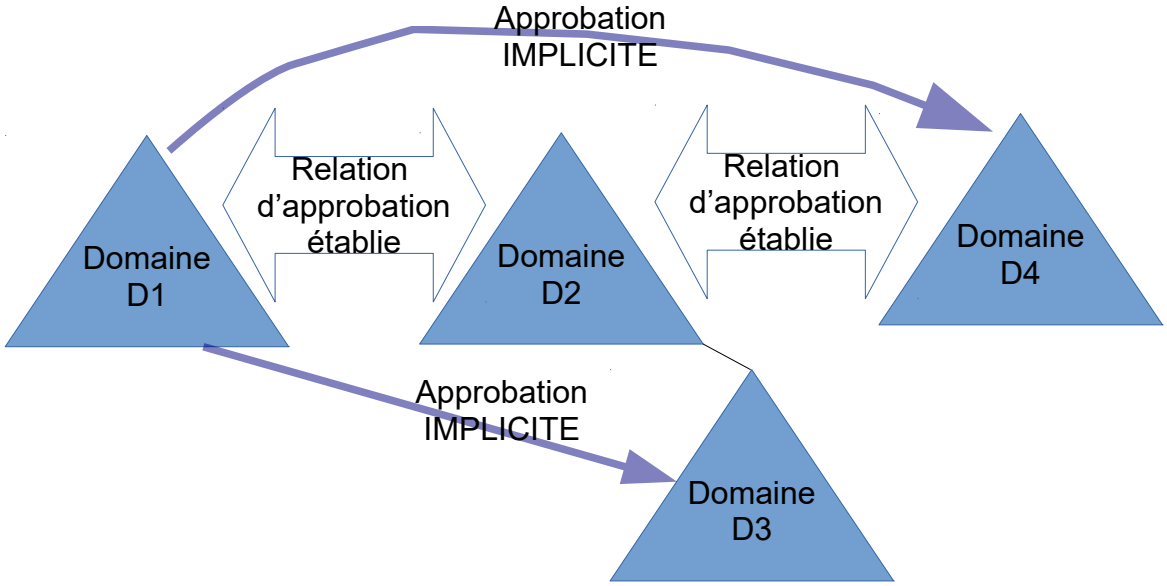
- Des domaines situés à l'intérieur d'une même forêt;
- Des domaines situés dans deux forêts différentes;
- Etc..

Chaque domaine est informé des relations qui sont établies avec les autres domaines.

III.7.2. EXEMPLE: APPROBATION KEREBOS:

L'approbation Kerberos est à la fois TRANSITIVE et HIÉRARCHIQUE :

- Si un domaine D1 fait confiance à un domaine D2 et que le domaine D3 est un sous-domaine de D2, alors le domaine D1 fait lui aussi confiance au domaine D3;
- Si de plus D2 fait confiance à D4, D1 fait lui aussi confiance à D4.



III.8. RÉPLICATION, NOTION DE PARTITION:

Nous avons vu qu'un réseau ACTIVE DIRECTORY peut comprendre plusieurs CONTRÔLEURS DE DOMAINES (CD). Chacun de ces contrôleurs contient une "copie" de l'annuaire (c'est à dire de l'arborescence).

De ce fait, lorsque le contenu de l'annuaire d'un Contrôleur de Domaine est modifié par un administrateur, ces modifications doivent être propagées automatiquement sur les annuaires de tous les autres C.D, grâce à la fonction de réplication.

La réplication se fait partition par partition: une PARTITION est un sous-arbre d'un arbre de domaines.

IV. INSTALLATION DU SERVICE ACTIVE DIRECTORY:

IV.1. GÉNÉRALITÉS:

- Le service ACTIVE DIRECTORY est installable en tant que RÔLE dans les postes informatiques munis du système d'exploitation WINDOWS SERVER.
- Un poste informatique sur lequel les services d'Active Directory sont installés est appelé CONTRÔLEUR DE DOMAINE. Comme son nom l'indique, un DOMAINE A.D. de base est associé à ce contrôleur. La finalité première de l'installation est donc de créer et de configurer ce domaine de base.
- Après cette première phase, il s'agira de créer l'arborescence des OBJETS contenus dans ce domaine, c'est à dire le contenu de l'ANNUAIRE. Nous ne traiteront pas ici cette deuxième phase.
- Comme pour tout serveur, un Contrôleur de Domaine doit posséder une adresse IP fixe. L'étape préliminaire à toute installation d'A.D. est la configuration d'une IP fixe sur le poste de travail, si ce n'est pas encore le cas.

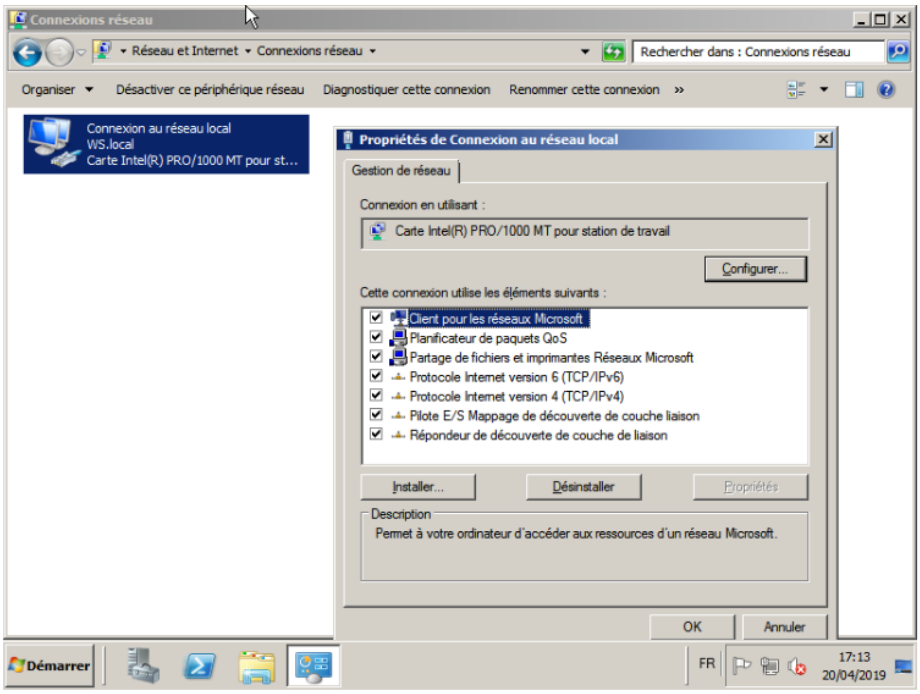
IV.2. CONFIGURER LA CONNEXION RÉSEAU EN IP FIXE:

Il faut pour cela ouvrir le menu de configuration de la carte réseau du Serveur permettant la connexion aux ressources à administrer. A partir du menu "démarrer", ceci correspond à la navigation suivante:

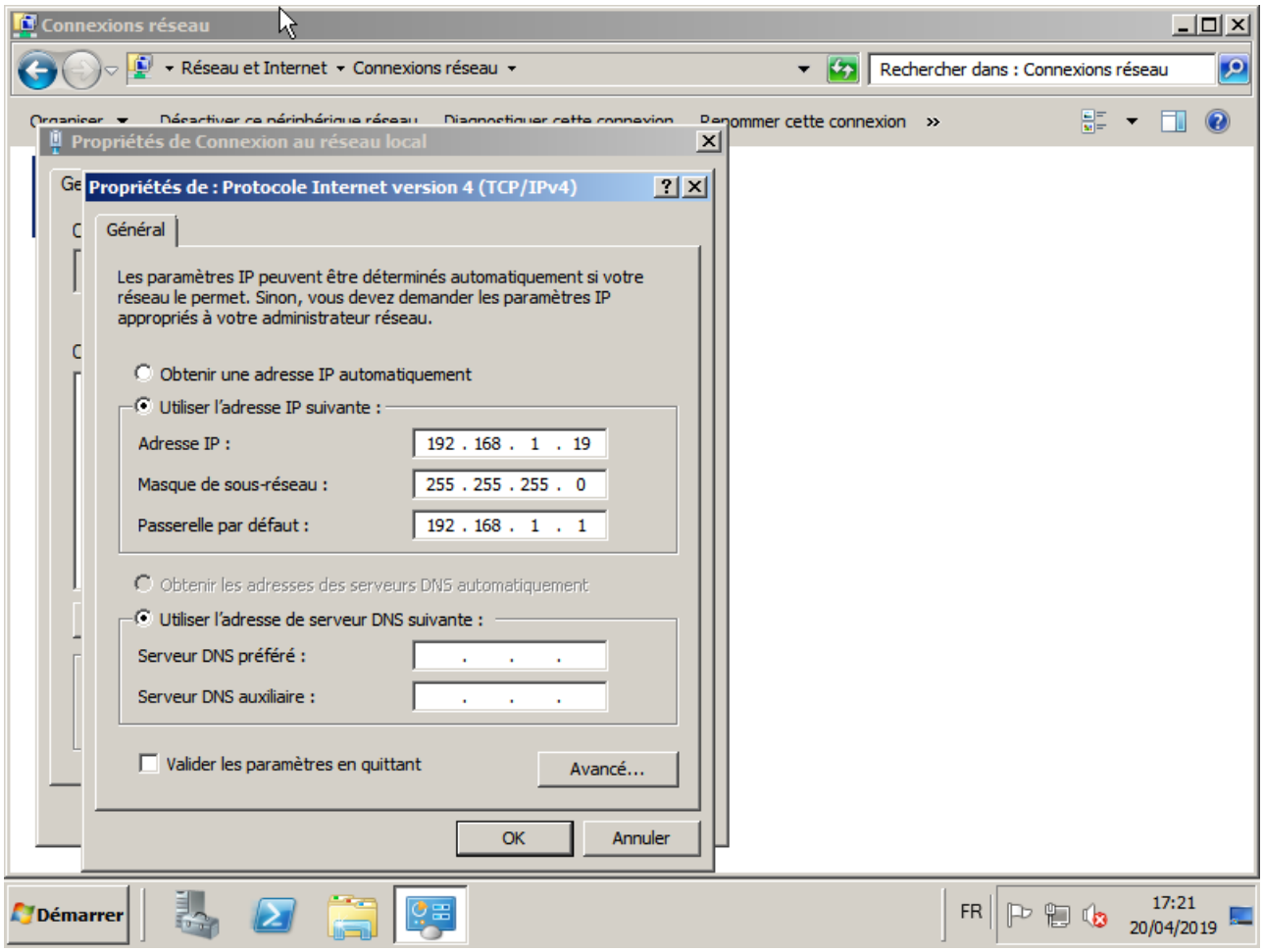
Démarrer → Réseau → Centre réseau et partage → Modifier les paramètres de la carte.

L'icône représentant la carte réseau concernée apparaît alors sur l'écran. En cliquant (clic droit) sur cette icône, on fait apparaître un menu contextuel. Choisir "propriétés". Le menu suivant s'affiche:

Sélectionner alors l'option "protocole IPV4", puis cliquer sur "propriétés.



Le menu de configuration du protocole IP V4 s'affiche alors:



REMARQUES:

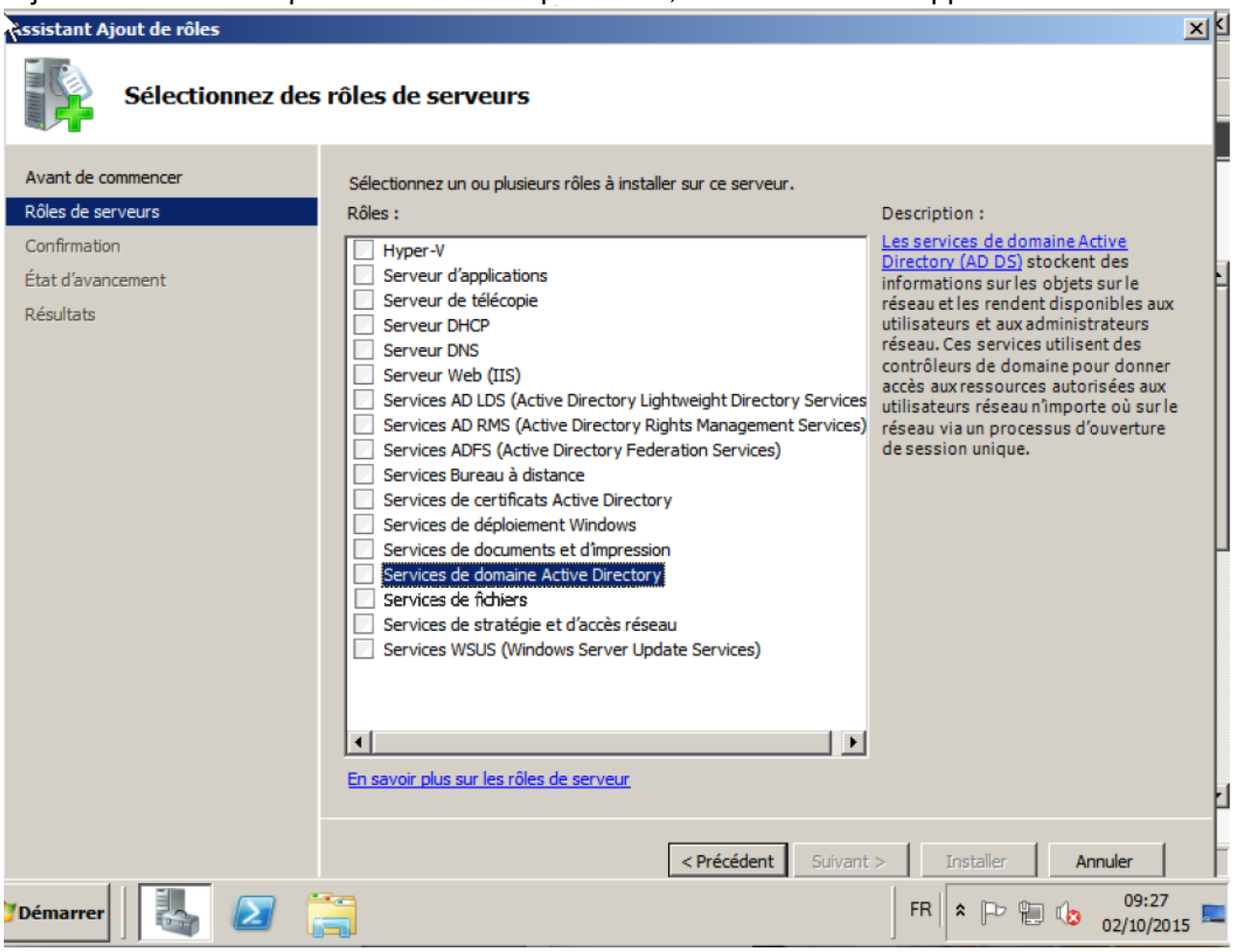
- Nous voyons ici que ce menu permet soit d'utiliser une adresse IP fixe (option "utiliser l'adresse IP suivante), soir d'obtenir une adresse IP automatiquement en utilisant un serveur DHCP (Dynamic Host Configuration Protocol) situé sur le réseau (en général, sur un routeur). C'est évidemment la première option qu'il faut choisir pour avoir une adresse fixe;
- Dans l'image présentée, les champs "Adresse IP", "Masque de sous-réseau" et "Passerelle par défaut" sont remplis: la machine est donc déjà configurée en IP fixe. Sinon, il faudra remplir ces champs;
- Cliquer sur OK pour terminer le paramétrage.

IV.3. INSTALLER LES FONCTIONNALITÉS ACTIVE DIRECTORY DANS LA MACHINE:

A partir du menu DÉMARRAGE de Windows Server, faire la navigation suivante:

Démarrer → Outils d'administration → Gestionnaire de serveur

puis, quand le menu principal du gestionnaire de serveur est ouvert, choisir l'option "ajouter des rôles". Après un écran d'explications, la liste des rôles apparaît:



Il suffit alors de cocher les rôles que l'on veut installer, puis de cliquer sur "suivant" pour lancer les installations. Il est conseillé d'installer le rôle de serveur DNS en même temps que celui de Serveur de Domaine A.D. Il faudra donc cocher ces deux rôles.

L'Assistant d'ajout de rôles s'ouvre alors. Suivre la procédure indiquée par l'enchaînement des menus pour:

- Choisir les fonctionnalités requises pour le fonctionnement d'A.D (logiciel Net Framework);
- Confirmer les options sélectionnées;
- Lancer les installations.

A la fin de l'installation, un encart indiquera le résultat obtenu.

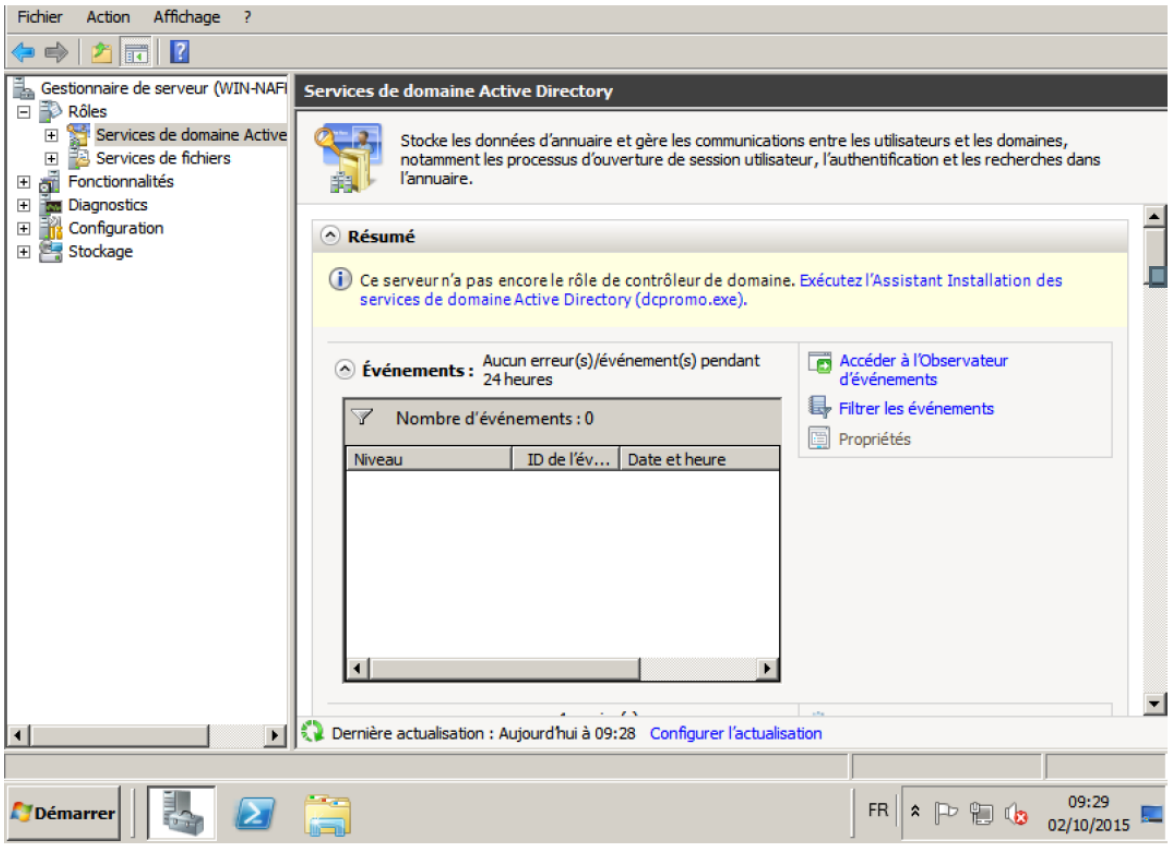
IV.4. CONFIGURER LE SERVEUR DE DOMAINE A.D:

IV.4.1. ACTIVATION DE l'ASSISTANT D'INSTALLATION:

Cette troisième étape consistera à configurer la machine pour en faire un SERVEUR DE DOMAINE A.D. Ceci consiste principalement en la création du DOMAINE A.D. de base du serveur, puis dans la construction d'un début d'arborescence à l'intérieur de ce domaine. Pour cela, nous allons encore utiliser le gestionnaire de serveur:

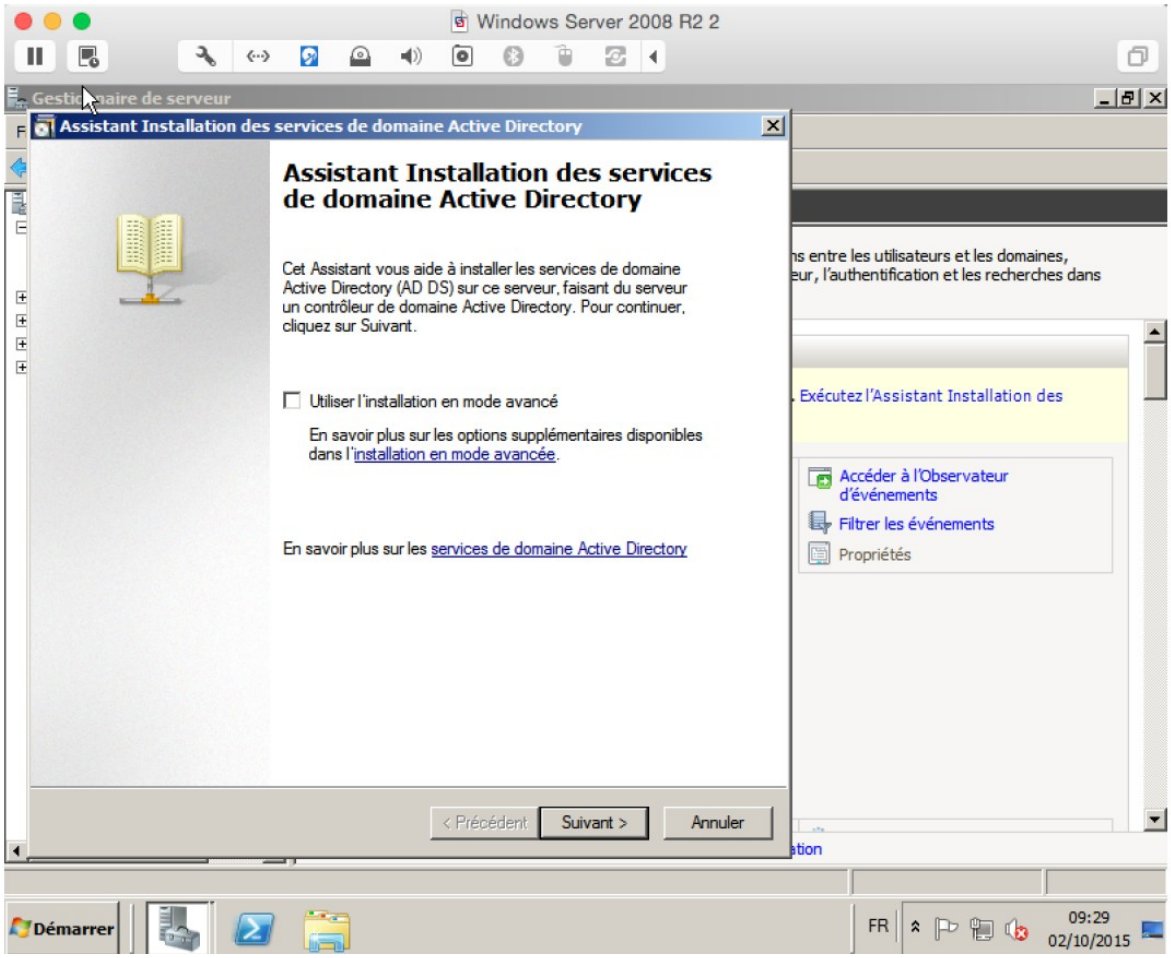
Démarrer → Outils d'administration → Gestionnaire de serveur→ Rôles → Services de domaine Active Directory.

Le menu principal du gestionnaire de serveur réapparaît:



Nous pouvons voir que les services de domaines active directory sont bien installés, mais que le rôle de contrôleur de domaine n'est pas encore installé. Pour cela, il faut créer un domaine A.D. de base dans la machine.

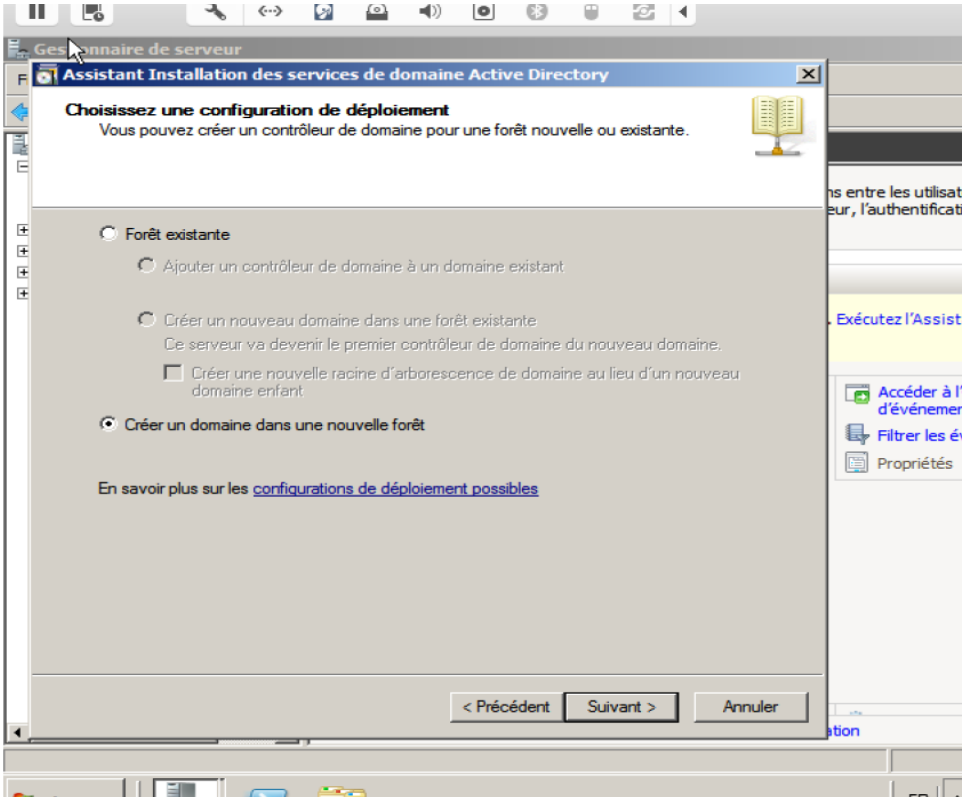
Activer alors le lien "Exécuter l'assistant d'installation des services de domaine Active Directory". La page d'accès à cet assistant apparaît alors:



Cocher l'option "Utiliser l'installation en mode avancé" avant de continuer. Après l'affichage d'une page de renseignements apparaît un menu de configuration du déploiement. Celui-ci va nous permettre de créer le domaine de base du serveur:

IV.4.2. DÉTERMINATION DE LA POSITION DU DOMAINE DANS L'ARBORESCENCE GÉNÉRALE:

Le menu suivant va nous permettre de déterminer la position du nouveau domaine dans l'arborescence des domaines existants:



Nous pouvons voir que deux options nous sont proposées:

- Soit créer le domaine à l'intérieur d'une FORÊT existante;
- Soit le créer dans une nouvelle forêt.

Dans le premier cas (forêt existante), vous pourrez:

- Soit rattacher le contrôleur de domaine en cours de création à un domaine existant de la forêt;
- Soit créer un nouveau domaine dans la forêt existante. Ce domaine pourra être soit un sous-domaine, soit le domaine racine d'un nouvel arbre de la forêt.

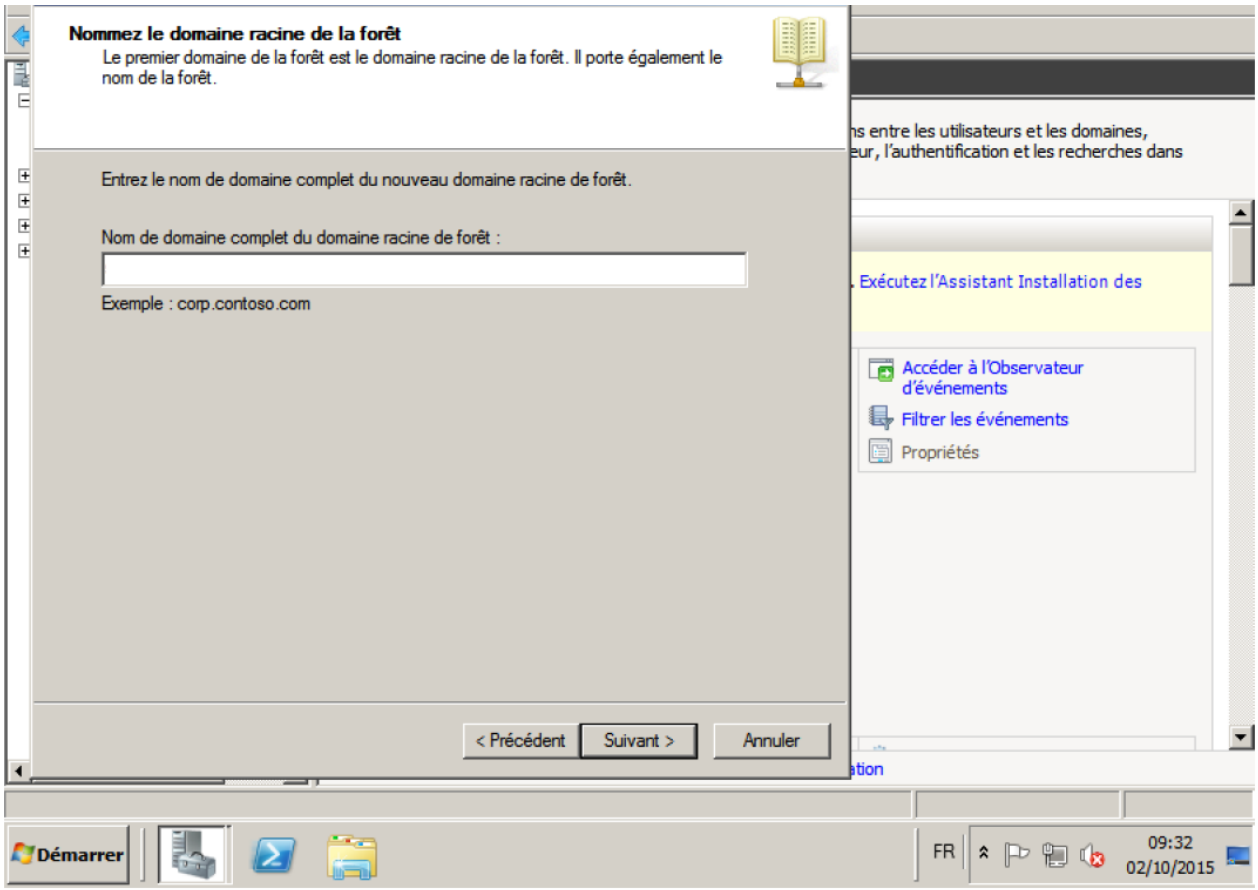
Dans le deuxième cas (nouvelle forêt): le domaine créé sera forcément le domaine racine d'une arborescence de la forêt.

Nous nous occuperons ici du deuxième cas, qui correspond au paramétrage initial d'un serveur de domaine. Nous sélectionnerons donc l'option "créer dans une nouvelle forêt" avant de poursuivre.

IV.4.3. NOMMAGE DU NOUVEAU DOMAINE ACTIVE DIRECTORY:

REMARQUE: Un nom de domaine Active Directory ne doit pas être choisi au hasard: en effet, pour éviter une trop grande complexité, l'arborescence des domaines A.D. (qui a un caractère PRIVÉ) doit pouvoir se superposer, au moins pour les niveaux supérieurs, à l'arborescence des domaines et sous-domaines PUBLICS (domaines au sens d'internet) utilisés par l'entreprise. De ce fait, la méthode de nommage la plus utilisée consiste à nommer les domaines A.D. comme s'ils étaient des sous-domaines de ces domaines publics. Par exemple, si le domaine public de l'entreprise est mycompany.com, le nom du domaine A.D (qui sera dans ce cas le domaine racine de la nouvelle forêt) pourra être: **dirgen.mycompany.com**.

Le menu suivant permet de déterminer le nom complet du domaine racine de la forêt (qui, rappelons le, sera également le nom de cette forêt). Rappelons qu'une forêt correspond en général à une organisation globale (entreprise, administration, université, etc.).



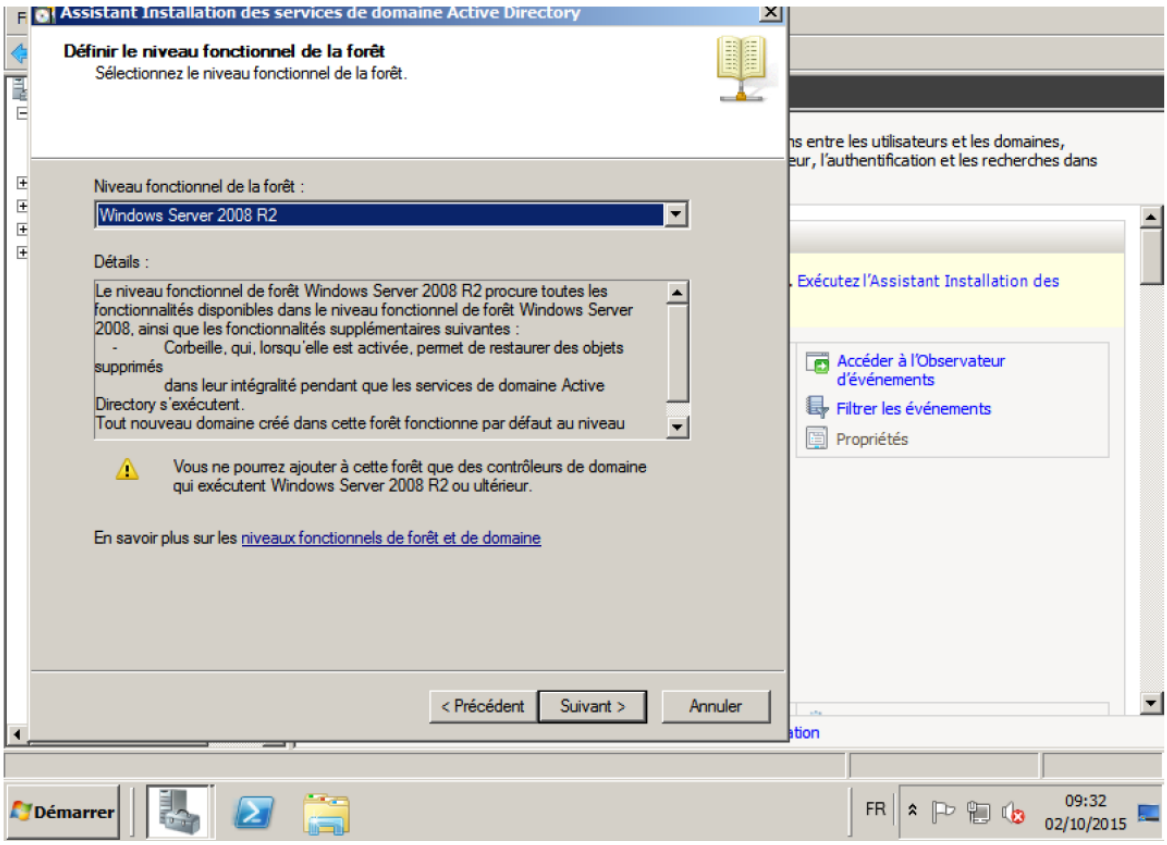
Il suffit de saisir le nom choisi (par exemple: "dirgen.mycompany.com") puis de passer au menu suivant.

IV.4.4. DÉTERMINATION DU "NOM NETBIOS" DU DOMAINE:

Le menu suivant permettra de confirmer ou d'infirmer le nom "netbios" donné automatiquement au domaine par le logiciel. Ce menu n'apparaît que s'il existe une possibilité de conflit (le nom netbios est une survivance des systèmes antérieurs à W 2000, gardée pour des raisons de compatibilité).

IV.4.5. DÉTERMINATION DU NIVEAU FONCTIONNEL DE LA FORÊT:

Le menu suivant permettra de déterminer le "niveau fonctionnel" de la forêt, ce qui revient à choisir la version la plus ancienne de Windows Server qui pourra équiper les contrôleurs de domaine utilisant cette forêt: par exemple, si l'on sélectionne "Window Serveur 2008 R2", ces contrôleurs de domaines devront être équipés de cette version ou de versions plus récentes.

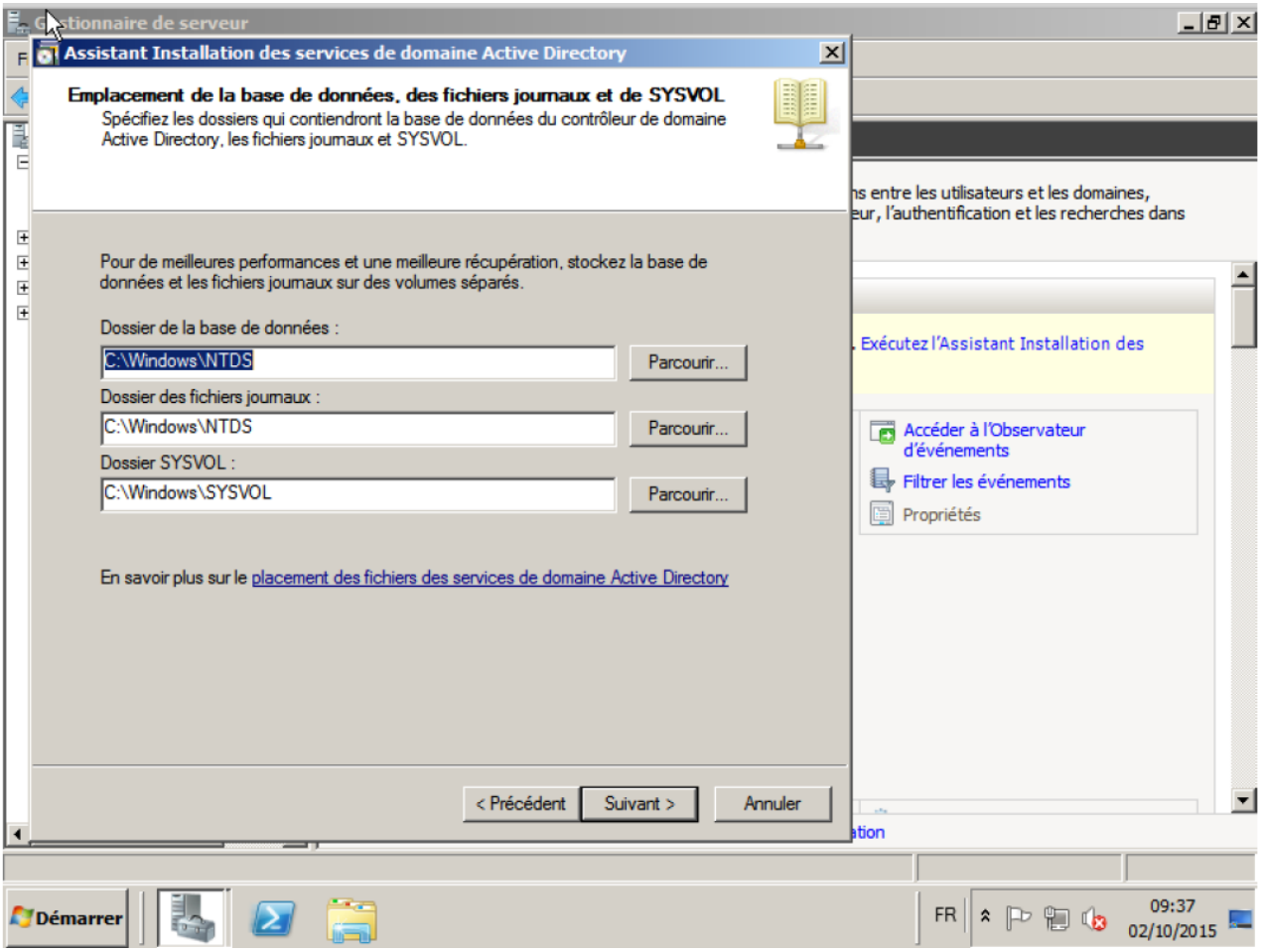


IV.4.6. VÉRIFICATION DU RÔLE DE SERVEUR DNS:

Le menu suivant va permettre de vérifier que le rôle de serveur DNS a bien été coché. Des avertissements seront peut-être affichés si le domaine à créer est le domaine racine d'une nouvelle forêt. Vérifier que le rôle SERVEUR DNS est bien coché, puis continuer.

IV.4.7. DÉTERMINATION DE CERTAINS NOMS DE DOSSIERS ET CHEMINS D'ACCÈS:

Le menu suivant va permettre de déterminer les noms et chemins d'accès de certains dossiers de travail:



En général, on peut conserver les valeurs par défaut. Passer au menu suivant.

IV.4.8. DÉTERMINATION DU MOT DE PASSE DE RESTAURATION:

Ce mot de passe, différent du mot de passe de l'administrateur, n'est utilisé qu'au cas où on a besoin de restaurer les services d'annuaire (redémarrage en mode restauration).

IV.4.9. FIN DE L'INSTALLATION:

Les deux menus suivants permettent l'affichage d'un résumé de l'installation effectuée et de signaler la fin de la procédure d'installation.

IV.5. INTÉGRATION D'UN POSTE CLIENT DANS UN DOMAINE ACTIVE DIRECTORY:

IV.5.1. REMARQUE PRÉLIMINAIRE:

Un utilisateur d'A.D. peut accéder à l'annuaire à partir d'un POSTE CLIENT à condition que celui-ci soit muni d'une VERSION PROFESSIONNELLE de WINDOWS (les versions familiales ne le permettent pas.

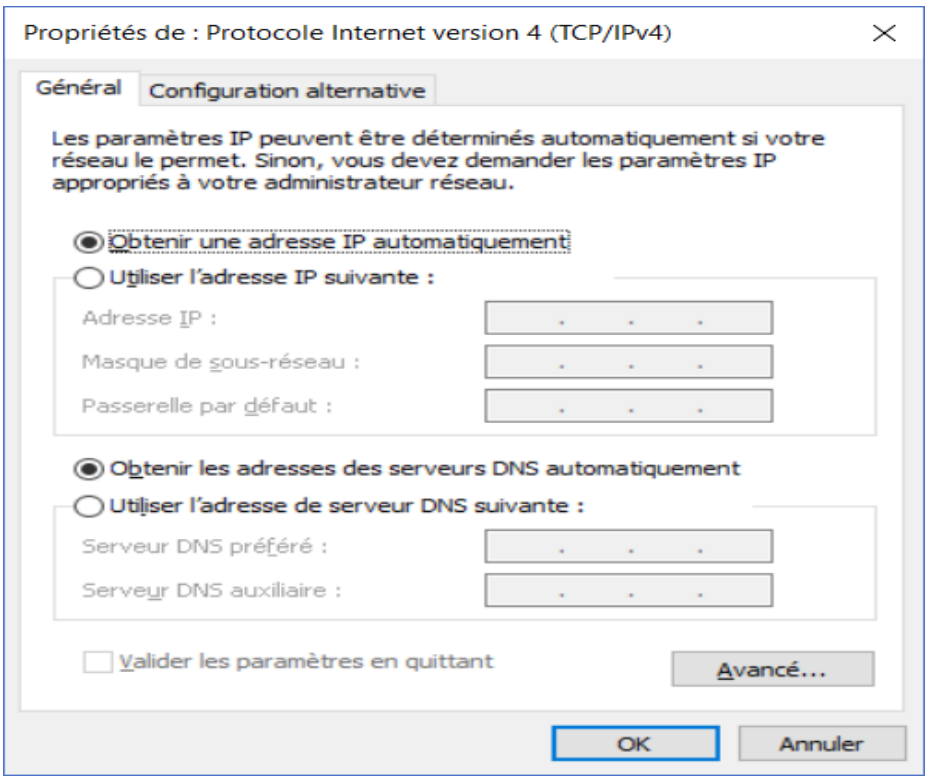
IV.5.2. PROCÉDURE CÔTE SERVEUR:

Le poste client doit être déclaré comme un objet "ordinateur" à l'intérieur d'un DOMAINE. Cette manipulation s'effectue dans le SERVEUR DE DOMAINE qui gère ce domaine. A cette occasion, un NOM DNS est attribué à l'objet.

IV.5.3. PROCÉDURE CÔTE CLIENT:

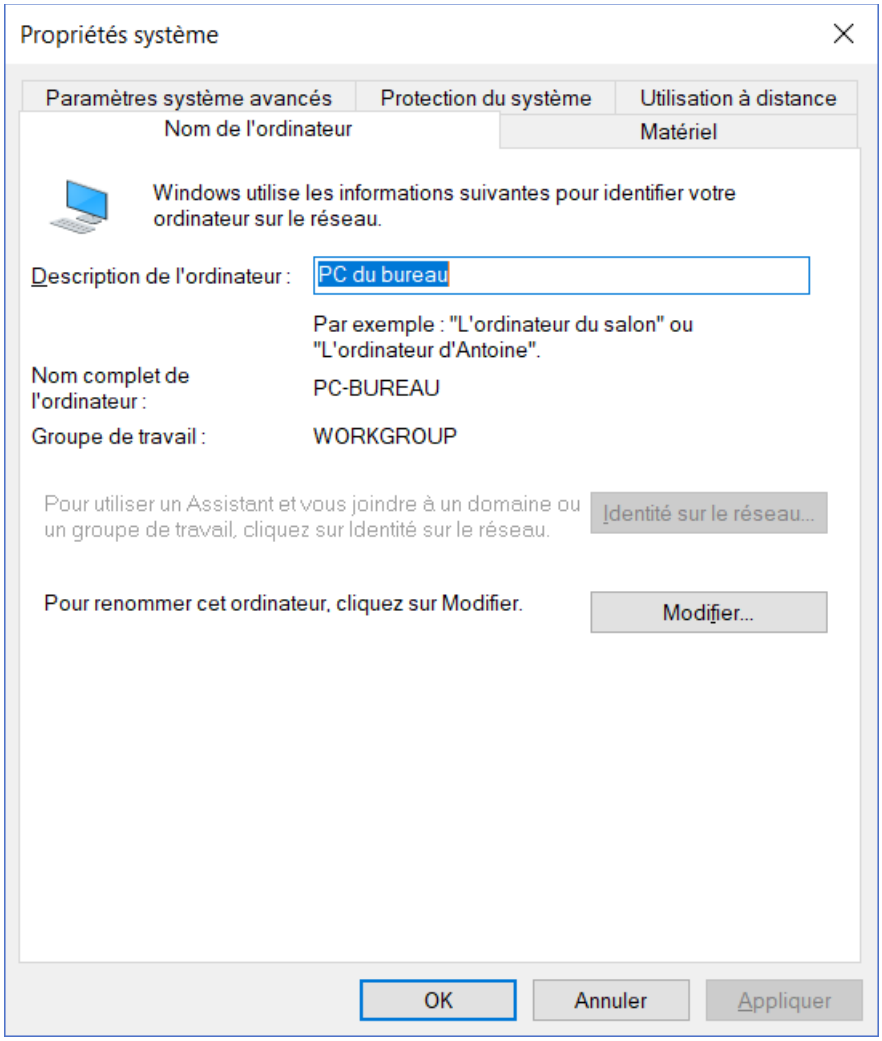
Les propriétés de la carte réseau communicant avec le serveur de domaines doivent être modifiées afin de déclarer le contrôleur de domaine gérant l'objet l'ordinateur correspondant au poste client en tant que serveur DNS:

- Naviguer: → Paramètres → Réseau et internet → Centre réseau et partage → Modifier les paramètres de la carte, puis cliquer sur l'icône de la carte concernée et choisir "propriétés".
- Sélectionner alors le protocole internet version 4 et cliquer sur "propriétés". Le menu suivant s'affiche:

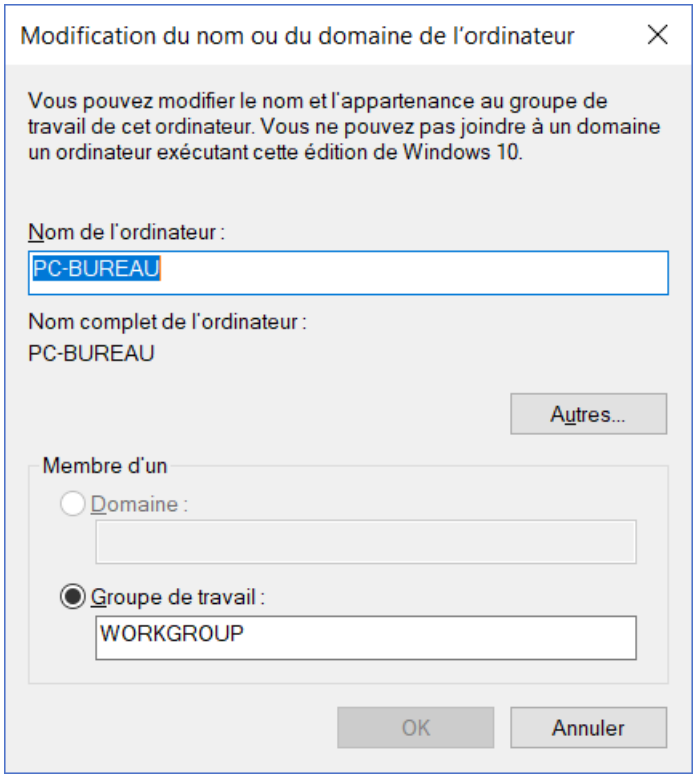


Sélectionner alors "Utiliser l'adresse de serveur DNS suivante:" et saisir l'adresse du serveur de domaine dans le premier champ de saisie.

Naviguer alors vers → Système → Informations système → Paramètres système avancés. Le menu suivant s'affiche:



En sélectionnant l'onglet "Nom de l'ordinateur" puis "Modifier" on obtient alors le menu suivant:



Il suffit alors de saisir le NOM DNS utilisé dans le serveur dans le champ "Nom de l'ordinateur", de sélectionner "Membre d'un domaine", de saisir le nom du domaine et de valider pour achever l'intégration.

REMARQUES :

Cette manipulation n'est possible que si le système WINDOWS est une version "professionnelle".

L'intégration peut prendre quelques minutes car elle déclenche des recherches sur le réseau.