TUTORIEL

WINDOWS 2022 Créer un contrôleur de domaine Créer un Active Directory (AD)



SOMMAIRE

1. PREPARATION DU SERVEUR

- a. Affectation d'une adresse IP fixe au serveur
- **b. Nommer le serveur**
- c. Désactiver la configuration renforcée d'IE
- d. Définir le mot de passe administrateur et son expiration
- 2. CREATION DU CONTROLEUR DE DOMAINE ET ACTIVE

DIRECTORY (AD DS)

- a. Les objets
- b. Le schéma
- c. Le domaine
- d. Mise en place quidée

Ce tutoriel nécessite de disposer d'une machine Windows Server 2022 (en version standard). Ici, nous avons préalablement préparé une machine virtuelle avec les caractéristiques suivantes :

- Espace disque = 40 Go
- Mémoire vive = 4 Go au minimum (il est vivement conseillé d'augmenter la taille de la mémoire)
- Version « standard » <u>avec expérience de bureau</u> (c'est-à-dire avec une interface graphique)
- Un accès à Internet

Attention, lors de l'installation de votre machine Windows Server 2022, sélectionnez la bonne version :

022 Standard x64 07/08/2021
022 Standard (expérience de bureau) x64 07/08/2021
022 Datacenter x64 07/08/2021
022 Datacenter (expérience de bureau) x64 07/08/2021
DescriptionControl (Control)Control (Control)122 Datacenterx6407/08/202122 Datacenter (expérience de bureau)x6407/08/202

Attention, sélectionnez la version « expérience de bureau » afin de bénéficier d'une interface graphique pour votre serveur !

1 - PREPARATION DU SERVEUR

Au lancement, Windows Server 2022 affiche le « Gestionnaire de serveur » sous cette forme :



<u>Il est nécessaire d'affecter une adresse IP fixe à votre serveur</u> avant de procéder à l'installation des rôles. En effet, étant donné qu'il s'agit d'un serveur sur lequel nous attacherons des rôles, il est important que son adresse IP ne soit pas modifiée.

- Ouvrez l'explorateur en cliquant l'icône dans la barre des tâches
- Faites un clic droit sur « Réseau » et « Propriétés » :



- Cliquez, dans la partie gauche, sur « Modifier les paramètres de la carte »
- Faites un clic droit sur l'icône du réseau et cliquez « Propriétés » :



• Sélectionnez « Protocole Internet version 4 (TCP/IPv4) » et cliquez le bouton « Propriétés » :



• Saisissez les paramètres qui correspondent à votre réseau (à adapter selon votre environnement réseau) :



Afin de simplifier les traitements ultérieurs, nous recommandons de nommer le serveur de manière à l'identifier simplement :

- Ouvrez l'explorateur en cliquant l'icône dans la barre des tâches
- Faites un clic droit sur « Ce PC » et cliquez sur « Propriétés » :



- Dans la fenêtre affichée, cliquez le bouton « Renommer ce PC » :
 Renommer ce PC
- Dans la fenêtre affichée, saisissez le nom que vous souhaitez donner à votre serveur et cliquez « Suivant » :

Renommer votre PC			
Vous pouvez utiliser une combinaison	de lettres, de traits d'union	et de chiffres.	
Nom actuel du PC : WIN-49Q9D5RNJ2	23		
win2022	×		
		Suivant	Annuler

Cliquez impérativement « Redémarrer maintenant » afin que le nouveau nom soit pris en compte :



Le message suivant permet de justifier le redémarrage du serveur (inscription de l'évènement dans le journal) ; vous pouvez laisser sur « Autre (non planifié) » et cliquer le bouton « Continuer » :

Choisissez le motif qui justifie, selon v cet ordinateur.	ous, d'arrêter	
Autre (non planifié)	~	
	Continuer	

3^{ème} étape : désactivation de la configuration renforcée d'Internet Explorer

Même si Internet Explorer a été arrêté, nous désactivons, ici, la configuration renforcée du navigateur pour éviter les messages d'alertes lors d'ouverture de liens par exemple :

renforcée

messages

'utilité de nos jours (le supporté par Microsoft).

ctivons cette option ici.

d'Internet

d'alertes

- Dans le gestionnaire de serveur, cliquez, dans la partie gauche, sur « Serveur local »
- Recherchez, dans la partie droite
 Configuration de sécurité renforcée d'Internet Explorer Actif
- Cliquez sur « Actif »
- Sélectionnez « Désactivé » et cliquez « Ok » :

La Configuration de sécurité renforcée d'Internet Explorer (IE ESC) diminue l'exposition de votre serveur à des attaques potentielles provenant de contenus Web. La Configuration de sécurité renforcée d'Internet Explorer est activée par défaut pour les groupes Administrateurs et Utilisateurs.	
Administrateurs :	La « configuration Explorer » n'a plus d navigateur n'est plus s
Vtlisateurs :	récurrents, nous désa
Activé (recommandé)	
S Obésactivé	

4^{ème} étape : définition du mot de passe de l'administrateur et désactivation de l'expiration du mot de passe

• Dans le gestionnaire de serveur, cliquez sur « Outils » et « Gestion de l'ordinateur » :



- Dans le volet de gauche, cliquez sur « Utilisateurs et groupes locaux » et sur « Utilisateurs »
- Dans le volet de droite, faites un clic droit sur « Administrateur » :

 Gestion de l'ordinateur (local) ✓ [№] Outils système 	Nom	Nom complet
> Planificateur de tâches > Planificateur d'événements	DefaultAccount	Définir le mot de passe
 > B Dossiers partagés 	😓 Gilles 死 Invité	Toutes les tâches
 Wtilisateurs et groupes locaux Utilisateurs 	WDAGUtilityAccour	Supprimer
Groupes		Renommer

Saisissez le mot de passe qui sera défini pour l'administrateur et cliquez « OK » :



Un message indique que le nouveau mot de passe de l'administrateur a été défini :



Il est possible d'empêcher l'expiration du mot de passe de la manière suivante :

- Faites un clic droit sur « Administrateur »
- Cliquez sur « Propriétés » :

Nom	Nom complet	De
Administrateur DefaultAccount Gilles Unvité WDAGUtilityAccount	Définir le mot de passe Toutes les tâches Supprimer Renommer Propriétés	4

• Cliquez la case « Le mot de passe n'expire jamais » et cliquez « OK » pour valider vos choix :

Propriétés de : Ad	lministrat	eur			? ×
Contrôle à dist	ance	Profil	des services B	ureau à distance	Appel entrant
Général	Membr	re de	Profil	Environnement	Sessions
Administrateur Nom complet : Description : Compte d'utilisateur d'administration					
L'utilisateur de	oit change	r le mot de	passe à la pro	chaine ouverture de ses	sion
L'utilisateur ne	e peut pas	changer d	le mot de pass	e	
Le mot de pa	sse n'expir	e jamais			
Le compte es	t désactiv	é			
Le compte es	t verrouillé				

La préparation de notre serveur est maintenant terminée et le gestionnaire de serveur affiche les caractéristiques suivantes :

	PROPRIÉTÉS Pour win2022		Nom du serveur et mode «Workgroup»
Nom Grou	de l'ordinateur pe de travail WORKGROUP		 activé par défaut étant donné qu'aucun rôle n'est présent sur le serveur actuellement.
Pare- Gesti Bure Asso Ether	feu Microsoft Defender Public : Actif on à distance Activé au à distance Désactivé ciation de cartes réseau Désactivé net0 192.168.183.22, compatible IPA	/6	Adressage IP fixe tel qu'il a été défini par l'administrateur du système.
Versi	on du système d'exploitation Microsoft Windows Server 202 PROPRIÉTÉS Pour win2022 Dernières mises à jour installées Windows Update	2 Standard TÀCHES Jamais Télécharger les mises à jour uniquement à l'aide d	
	Dernière recherche de mises à jour : Antivirus Microsoft Defender Commentaires et diagnostics Configuration de sécurité renforcée d'Internet Explorer	Jamais Protection en temps réel : activée Paramètres Inactif	Configuration renforcée d'Internet Explorer désactivée et caractéristiques générales de la machine.
	Fuseau horaire ID de produit (Product ID)	(UTC+01:00) Bruxelles, Copenhague, Madrid, Paris Non activé	
ard	Processeurs Mémoire installée (RAM)	11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz, 7.81 Go	
	Espace disque total	59,68 Go	

2 – CREATION D'UN CONTROLEUR DE DOMAINE ET ACTIVE DIRECTORY (AD)

L'Active Directory est un annuaire LDAP pour les systèmes d'exploitation Windows, le tout étant créé par Microsoft. Cet annuaire contient différents objets, de différents types (utilisateurs, ordinateurs, etc...).

<u>L'objectif étant de centraliser</u> deux fonctionnalités essentielles : l'**identification** et l'**authentification** au sein d'un système d'information :





La structure de l'Active Directory

A. Les classes et les attributs

Au sein de l'annuaire Active Directory, il y a différents types <u>d'objets</u> tels que : les *utilisateurs*, les *ordinateurs*, les *serveurs*, les *unités d'organisation* ou encore les *groupes*. En fait, ces objets correspondent à des <u>classes</u>, c'està-dire des objets disposant des mêmes attributs.

De ce fait, un objet ordinateur sera une instance d'un objet de la classe « **Ordinateur** » avec des valeurs spécifiques à l'objet concerné.



Par ailleurs, les **unités d'organisation (appelées « OU »)** sont des containers d'objets afin de faciliter l'organisation de l'annuaire et <u>permettre une organisation avec plusieurs niveaux</u>. Sans les unités d'organisations, l'annuaire ne pourrait pas être trié correctement et l'administration serait moins efficace. Comparez les unités d'organisations à des dossiers qui permettent de ranger les objets à l'intérieur.

B. Le schéma

Par défaut, tout annuaire Active Directory dispose de classes prédéfinies ayant chacune une liste d'attributs bien spécifique, et propre à tout annuaire, cela est défini grâce à **un schéma**.



Le schéma contient la définition de toutes les classes et de tous les attributs disponibles et autorisés au sein de votre annuaire. Il est à noter que le schéma est évolutif, le modèle de base n'est pas figé et peut évoluer selon vos besoins.

Par exemple, l'application de messagerie Microsoft Exchange effectue des modifications au schéma lors de son installation.

Groupe de travail et notion de domaine

Du groupe de travail au domaine

Pour rappel, toutes les machines sous Windows sont par défaut intégrées dans un groupe de travail nommé « **WORKGROUP** ». Cela permet de mettre en relation des machines d'un même groupe de travail, notamment pour le partage de fichiers, mais <u>il n'y a pas de notions d'annuaire, ni de centralisation</u> avec ce mode de fonctionnement.

A. Modèle « Groupe de travail »

- **Une base d'utilisateurs par machine** : appelée « base SAM », <u>cette base est unique sur chaque machine</u> et <u>non</u> <u>partagée</u>. Ainsi, chaque machine contient sa propre base d'utilisateurs.

- Ce modèle devient très vite inadapté notamment pour la gestion des comptes utilisateurs en nombre. En effet, chaque utilisateur devra disposer d'un compte sur chaque machine si l'on souhaite mettre en place une authentification. Par exemple, une salle avec 10 machines nécessitera de créer le compte de l'utilisateur sur chacune des 10 machines si l'on veut qu'il conserve à chaque fois le même identifiant et le même mot de passe ! Donc pour 10 utilisateurs, il faudra créer 10 utilisateurs par machine x 10 soit 100 manipulations !

B. Modèle « Domaine »

- Base d'utilisateurs, de groupes et d'ordinateurs <u>centralisée</u>. Un seul compte utilisateur est nécessaire pour accéder à l'ensemble des machines du domaine.

- L'annuaire contient toutes les informations relatives aux objets, tout est centralisé sur le contrôleur de domaine, il n'y a pas d'éparpillement sur les machines au niveau des comptes utilisateurs.

- Ouverture de session unique par utilisateur, notamment pour l'accès aux ressources situées sur un autre ordinateur ou serveur.

- Chaque contrôleur de domaine contient une copie de l'annuaire, qui est maintenue à jour et qui permet d'assurer la disponibilité du service et des données qu'il contient. Les contrôleurs de domaine se répliquent entre eux pour assurer cela.

Administration et gestion de la sécurité complètement centralisée avec mise en place de « stratégies »

Les contrôleurs de domaine

A. <u>Qu'est-ce qu'un contrôleur de domaine ?</u>

Lorsque l'on crée un domaine, le serveur depuis lequel on effectue cette création est promu au rôle de « contrôleur de domaine » du domaine créé. Il devient contrôleur du domaine créé, ce qui implique qu'il sera au cœur des requêtes à destination de ce domaine.

De ce fait, il devra vérifier les identifications des objets, traiter les demandes d'authentification, veiller à l'application des stratégies de groupe ou encore stocker une copie de l'annuaire Active Directory.

Un contrôleur de domaine est indispensable au bon fonctionnement du domaine, si l'on éteint le contrôleur de domaine ou qu'il est corrompu, le domaine devient inutilisable.

De plus, lorsque vous créez le premier contrôleur de domaine dans votre organisation, vous créez également le premier domaine, la première forêt, ainsi que le premier site.

B. Le fichier de base de données NTDS.dit

Sur chaque contrôleur de domaine, on trouve une copie de la base de données de l'annuaire Active Directory. Cette copie est symbolisée par un fichier « **NTDS.dit** » qui contient l'ensemble des données de l'annuaire.

C. La réplication des contrôleurs de domaine

Afin d'assurer une haute disponibilité et d'éviter tout problème, il est vivement recommandé d'avoir **au minimum deux contrôleurs de domaine** pour assurer la disponibilité et la continuité de service des services d'annuaire.

De plus, cela permet d'assurer la pérennité de la base d'annuaire qui est très précieuse. À partir du moment où une entreprise crée un domaine, même si ce domaine est unique, il est important de mettre en place au minimum deux contrôleurs de domaine.

DOMAINE



Notion d'arbre et de forêt

Au sein du domaine schématisé par des triangles généralement, on retrouvera **tout un ensemble d'Unités d'Organisation remplies d'objets de différentes classes** : utilisateurs, ordinateurs, groupes, contrôleurs de domaine, etc...

De nombreuses entreprises ont plusieurs succursales, ce qui implique plusieurs sites sur différents emplacements géographiques. Selon l'importance de ces sites, on pourra envisager de créer un sous-domaine au domaine principal, voir même plusieurs sous-domaines selon le nombre de succursales.

Lorsqu'un domaine principal contient plusieurs sousdomaines on parle alors **d'arbre**, où chaque sousdomaine au domaine racine représente une branche de l'arbre. **Un arbre est un regroupement hiérarchique de plusieurs domaines.**



Une **forêt** est un regroupement d'une ou plusieurs arborescences de domaine, autrement dit d'un ou plusieurs arbres. Ces arborescences de domaine sont indépendantes et distinctes bien qu'elles soient dans la même forêt. Mais alors qu'apporte la création d'une forêt ?

- Tous les arbres d'une forêt partagent un schéma d'annuaire commun

- Tous les domaines d'une forêt partagent un « catalogue global commun ».

- Les domaines d'une forêt fonctionnent de façon indépendante, mais la forêt facilite les communications entre les domaines, c'est-à-dire dans toute l'architecture.7

- Création de relations entre les différents domaines de la forêt

- Simplification de l'administration et flexibilité. Un utilisateur d'un domaine pourra accéder à des ressources situées dans un autre domaine ou se connecter sur une machine du domaine si les autorisations le permettent.

Notion de niveau fonctionnel

Le niveau fonctionnel est une notion également à connaître lors de la mise en œuvre d'une infrastructure Active Directory. À la création d'un domaine, un niveau fonctionnel est défini et il correspond généralement à la version du système d'exploitation serveur depuis lequel on crée le domaine.

Par exemple, si l'on effectue la création du domaine depuis un serveur sous Windows Server 2012, le niveau fonctionnel sera « *Windows Server 2012* ». Dans un environnement existant, on est souvent amené à faire évoluer notre infrastructure, notamment les systèmes d'exploitation, ce qui implique le déclenchement d'un processus de migration. Une étape incontournable lors de la migration d'un Active Directory vers une version plus récente et le changement du niveau fonctionnel. Ainsi, il est important de savoir à quoi il correspond et les conséquences de l'augmentation du niveau.

<u>Plus le niveau fonctionnel est haut, plus vous pourrez bénéficier des dernières nouveautés liées à l'Active Directory</u> et à sa structure. Par exemple, si le niveau fonctionnel est « Windows Server 2003 », vous ne pourrez pas ajouter un nouveau contrôleur de domaine sous Windows Server 2012 et les versions plus récentes.

À l'inverse, si le niveau fonctionnel est « *Windows Server 2012* », il sera impossible d'intégrer de nouveaux contrôleurs de domaine qui utilisent un système d'exploitation plus ancien que Windows Server 2012.

De plus, vous ne pouvez pas avoir un niveau fonctionnel plus haut que la version de votre contrôleur de domaine le plus récent.

<u>Il est impossible de passer à un niveau inférieur</u>. Par exemple, on peut passer du niveau « *Windows Server 2003* » à « *Windows Server 2008* », mais pas l'inverse. Il existe toutefois une exception, il est possible rétrograder le niveau fonctionnel de Windows Server 2008 R2 à Windows Server 2008.

Notion de protocole LDAP

Le protocole LDAP

A. <u>Qu'est-ce que le protocole LDAP ?</u>

Le protocole LDAP (*Lightweight Directory Access Protocol*) est **un protocole qui permet de gérer des annuaires**, notamment grâce à des requêtes d'interrogations et de modification de la base d'informations. En fait, l'Active Directory est un annuaire LDAP.

Les communications LDAP s'effectuent sur le port 389, en TCP, du contrôleur de domaine cible.

Il existe une déclinaison du protocole LDAP appelée LDAPS (*LDAP over SSL*) est qui apporte une couche de sécurité supplémentaire avec du chiffrement.

B. <u>Que contient l'annuaire LDAP ?</u>

L'annuaire LDAP correspond directement à l'Active Directory. Il contient un ensemble d'unités d'organisation qui forment l'arborescence générale. Ensuite, on trouve tous les différents types d'objets classiques : utilisateurs, ordinateurs, groupes, contrôleurs de domaine, serveurs et imprimantes.

Pour chaque classe d'objets, il stocke les attributs correspondants et les différentes valeurs de ces attributs pour chaque instance d'un objet. Par exemple, il va stocker toutes les informations relatives à un utilisateur (nom, prénom, description, mot de passe, adresse e-mail, etc...).

C. Comment est structuré l'annuaire LDAP ?

Un annuaire est un ensemble d'entrées, ces entrées étant elles-mêmes constituées de plusieurs attributs. De son côté, un attribut est bien spécifique et dispose d'un nom qui lui est propre, d'un type et d'une ou plusieurs valeurs.

Chaque entrée dispose d'un identifiant unique qui permet de l'identifier rapidement, de la même manière que l'on utilise les identifiants (clé primaire) dans les bases de données pour identifier rapidement une ligne.

L'identifiant unique d'un objet est appelé GUID qui est « l'identificateur unique global ». Par ailleurs, un nom unique (DN – *Distinguished Name*) est attribué à chaque objet, et il se compose du nom de domaine auquel appartient l'objet ainsi que du chemin complet pour accéder à cet objet dans l'annuaire (le chemin à suivre dans l'arborescence d'unités d'organisation pour arriver jusqu'à cet objet).

Par exemple, le chemin d'accès suivant, correspondant à un objet « *utilisateur* » nommé « *prof* », du domaine « laboprof.fr » et étant stocké dans une unité d'organisation (OU) nommée « *btssio* » : laboprof.fr,btssio,prof

En « langage » LDAP, on traduira ainsi : cn=prof,ou=btssio,dc=laboprof,dc=fr

Ainsi, la chaîne ci-dessus correspondra au Distinguished Name (DN) unique de l'objet.

Dans un chemin LDAP vers un objet, on trouve toujours la présence du domaine sous la forme : « *dc=laboprof,dc=fr* » (ne pas mettre d'espace)

D. A quel moment a-t-on besoin d'utiliser le protocole LDAP ?

Le protocole LDAP permet de créer des liaisons entre une application et l'annuaire des utilisateurs. Prenons pour exemple un helpdesk de type GLPI. Lorsque les utilisateurs du domaine souhaitent se connecter à l'interface GLPI pour saisir un ticket de maintenance, il est souhaitable que l'identifiant de connexion et le mot de passe soient les mêmes que ceux utiliser pour la connexion au domaine. On évite ainsi les erreurs et une accumulation d'identifiants avec des mots de passe nombreux.

Le protocole LDAP permet donc d'effectuer une liaison entre GLPI et l'Active Directory de manière à **importer les utilisateurs de l'annuaire AD** dans l'application GLPI. Ainsi, les utilisateurs ne seront pas à créer dans l'application puisqu'ils existent déjà dans l'annuaire et l'authentification de ces derniers restera identique (nous travaillerons ce point lors d'un TP ultérieur).





Mise en œuvre sur la machine Windows Server 2022 :

• Dans le gestionnaire de serveur, cliquez sur « Ajouter des rôles et des fonctionnalités » :

💽 کې ۲۰۰۰ Tablea	u de bord	- 🕲 🚩	Gérer	Outils	Afficher	Aide
 Tableau de bord Serveur local Tous les serveurs Services de fichiers et d 	BIENVENUE DANS GESTIONNAIRE DÉMARRAGE RAPIDE	e de serveur nfigurer ce serveur Njouter des rôles et des f a	local	nalités		

• Un message d'introduction s'affiche : cliquez « Suivant » :

📥 Assistant Ajout de rôles et de fon	ctionnalités	_		×
Avant de commen	cer	SERVEUR DE I	DESTINATIO win20	DN 122
Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités Confirmation Résultats	Cet Assistant permet d'installer des rôles, des services de rôle ou des fonct déterminer les rôles, services de rôle ou fonctionnalités à installer en foncti de votre organisation, tels que le partage de documents ou l'hébergement Pour supprimer des rôles, des services de rôle ou des fonctionnalités : Démarrer l'Assistant de Suppression de rôles et de fonctionnalités Avant de continuer, vérifiez que les travaux suivants ont été effectués : • Le compte d'administrateur possède un mot de passe fort • Les paramètres réseau, comme les adresses IP statiques, sont configurés • Les dernières mises à jour de sécurité de Windows Update sont installées Si vous devez vérifier que l'une des conditions préalables ci-dessus a été sa exécutez les étapes, puis relancez l'Assistant.	ionnalités. Vous c on des besoins ir d'un site Web. tisfaite, fermez l'	levez nformatiq Assistant	jues
	Cliquez sur Suivant pour continuer.			
	< Précédent Suivant >	Installer	Annule	r

L'assistant se lance et propose des fenêtres successives qui vous permettront de configurer votre contrôleur de domaine (voir pages suivantes).

• Sélectionnez « Installation basée sur un rôle ou une fonctionnalité » et cliquez « Suivant » :

🚔 Assistant Ajout de rôles et de fo	nctionnalités	_	
Sélectionner le ty	Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités Confirmation Résultats		
Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités Confirmation Résultats	Sélectionnez le type d'installation. Vous pouvez installer des ré ordinateur physique ou virtuel en fonctionnement, ou sur un d Installation basée sur un rôle ou une fonctionnalité Configurez un serveur unique en ajoutant des rôles, des ser Installation des services Bureau à distance Installez les services de rôle nécessaires à l'infrastructure VE déployer des bureaux basés sur des ordinateurs virtuels ou	iles et des fonctionnalités su lisque dur virtuel hors conn vices de rôle et des fonction)I (Virtual Desktop Infrastruc sur des sessions.	ur un exion. nnalités. cture) pour
	< Précédent Suiva	nt > Installer	Annuler

Sélectionnez le serveur sur lequel le rôle doit être installé (ici il n'y a que celui que l'on vient d'installer) et cliquez
 « Suivant » :

🚔 Assistant Ajout de rôles et de	onctionnalités		- 0	×
Sélectionner le s	erveur de destination		SERVEUR DE DESTINATION win202	N 2
Avant de commencer Type d'installation	Sélectionnez le serveur ou le disque du Sélectionner un serveur du pool de Sélectionner un disque dur virtuel	r virtuel sur lequel installer des rô serveurs	les et des fonctionnalités.	
Rôles de serveurs Fonctionnalités	Pool de serveurs			
Résultats	Nom Adresse win2022 192.168.1	P Système d'exploitation 83.22 Microsoft Windows Serv	ver 2022 Standard	
	1 ordinateur(s) trouvé(s)			
	Cette page présente les serveurs qui e ont été ajoutés à l'aide de la command serveurs hors connexion et les serveurs incomplète ne sont pas répertoriés.	récutent Windows Server 2012 ou e Ajouter des serveurs dans le Ge nouvellement ajoutés dont la col	une version ultérieure et qui stionnaire de serveur. Les llecte de données est toujours	5
		< Précédent Suivant >	Installer Annuler	
Cliquez la case s	ituée à gauche du rôle « Serv	ces AD DS » et cliquez	z « Suivant » :	
🛓 Assistant Ajout de rôles et de	onctionnalités		- 0)

Sélectionner des	rôles de serveurs	SERVEUR DE DESTINATION win2022
Avant de commencer	Sélectionnez un ou plusieurs rôles à installer sur le serveur séle	ectionné.
Type d'installation	Rôles	Description
Sélection du serveur	Accès à distance	Les services de domaine Active
Rôles de serveurs	Attestation d'intégrité de l'appareil	Directory (AD DS) stockent des
Fonctionnalités	Hyper-V	informations à propos des objets sur le réseau et rendent ces
Confirmation	Serveur DHCP	informations disponibles pour les
Résultats	Services AD DDS Services AD DDS Services AD IDS Services AD I	utilisateurs et les administrateurs du réseau. Les services AD DS utilisent les contrôleurs de domaine pour donner aux utilisateurs du réseau un accès aux ressources autorisées n'importe où sur le réseau via un
	Services AD KMS (Active Directory Rights Manage) Services Bureau à distance Services d'activation en volume	processus d'ouverture de session unique.

Un message s'affiche en vous invitant à ajouter des fonctionnalités obligatoires et liées au rôle AD DS sélectionné ; cliquez le bouton « **Ajouter des fonctionnalités** » :

Ajouter les fonctionnalités requises pour Services AD DS ?		
Vous ne pouvez pas installer Services AD DS sauf si les services de rôle ou les fonctionnalités suivants sont également installés.		
 [Outils] Gestion de stratégie de groupe 4 Outils d'administration de serveur distant 4 Outils d'administration de rôles 4 Outils AD DS et AD LDS Module Active Directory pour Windows PowerShell 4 Outils AD DS [Outils] Centre d'administration Active Directory [Outils] Composants logiciels enfichables et outils e 		
< >		
Inclure les outils de gestion (si applicable)		
Ajouter des fonctionnalités Annuler		

 Après avoir cliqué sur « Ajouter des fonctionnalités », l'écran des rôles s'affiche de nouveau. La case « Services AD DS » est maintenant activée ; cliquez le bouton « Suivant » :

Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.			
Rôles	Description		
 Accès à distance Attestation d'intégrité de l'appareil Hyper-V Serveur de télécopie Serveur DHCP Serveur Web (IIS) Service Guardian hôte ✓ Services AD DS Services AD LDS (Active Directory Lightweight Dire Services Bureau à distance Services d'activation en volume Services de certificats Active Directory (AD FS) ♦ Services de stratégie et d'accès réseau Services WSUS (Windows Server Update Services) 	Les services de domaine Active Directory (AD DS) stockent des informations à propos des objets sur le réseau et rendent ces informations disponibles pour les utilisateurs et les administrateurs du réseau. Les services AD DS utilisent les contrôleurs de domaine pour donner aux utilisateurs du réseau un accès aux ressources autorisées n'importe où sur le réseau via un processus d'ouverture de session unique.		
< Précédent Suivant :	> Installer Annuler		

 Les fonctionnalités obligatoires qui s'installeront avec le rôle AD DS sont affichées ci-dessous ; cliquez le bouton « Suivant » pour poursuivre l'installation :

Fonctionnalités	Description
 INET Framework 4.8 Features (2 sur 7 installé(s)) Antivirus Microsoft Defender (Installé) Assistance à distance Base de données interne Windows BranchCache Chiffrement de lecteur BitLocker Client d'impression Internet Client pour NFS Client Telnet Client TFTP Clustering de basculement Collection des événements de configuration et de Compression différentielle à distance Conteneurs Data Center Bridging Déverrouillage réseau BitLocker DirectPlay Enhanced Storage Équilibrage de la charge réseau 	.NET Framework 4.8 provides a comprehensive and consistent programming model for quickly and easily building and running applications that are built for various platforms including desktop PCs, Servers, smart phones and the public and private cloud.
< Précédent Suivant >	> Installer Annuler
Cliquez, ici, le bouton « Suivant » pour lancer la c	réation de l'Active Directory :

Sélectionnez une ou plusieurs fonctionnalités à installer sur le serveur sélectionné.

GABRIEL GANEM - CREER UN CONTROLEUR DE DOMAINE ET UN AD

Services de domaine Active Directory

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

Fonctionnalités

AD DS

Confirmation

Résultats



Les services de domaine Active Directory (AD DS) stockent des informations sur les utilisateurs, les ordinateurs et les périphériques sur le réseau. Les services AD DS permettent aux administrateurs de gérer ces informations de façon sécurisée et facilitent le partage des ressources et la collaboration entre les utilisateurs.

À noter :

- · Pour veiller à ce que les utilisateurs puissent quand même se connecter au réseau en cas de panne de serveur, installez un minimum de deux contrôleurs de domaine par domaine.
- · Les services AD DS nécessitent qu'un serveur DNS soit installé sur le réseau. Si aucun serveur DNS n'est installé, vous serez invité à installer le rôle de serveur DNS sur cet ordinateur.

Azure Active Directory, un service en ligne distinct, peut fournir une gestion simplifiée des identités et des accès, des rapports de sécurité et une authentification unique aux applications web dans le cloud et sur site. En savoir plus sur Azure Active Directory Configurer Office 365 avec Azure Active Directory Connect

> < Précédent Suivant >

Installer

Annuler

Confirmer l'installation en cliquant « Installer » ; le processus se lance :

Confirmer les séle	ections d'installation serveur de destination win2022
Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités AD DS Confirmation Résultats	Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectionné, cliquez sur Installer. Redémarrer automatiquement le serveur de destination, si nécessaire Il se peut que des fonctionnalités facultatives (comme des outils d'administration) soient affichées sur cette page, car elles ont été sélectionnées automatiquement. Si vous ne voulez pas installer ces fonctionnalités facultatives, cliquez sur Précédent pour désactiver leurs cases à cocher. Gestion de stratégie de groupe Outils d'administration de serveur distant Outils d'administration de rôles Outils AD DS te AD LDS Module Active Directory pour Windows PowerShell Outils AD DS Centre d'administration Active Directory Composants logiciels enfichables et outils en ligne de commande AD DS Services AD DS Exporter les paramètres de configuration Spécifier un autre chemin d'accès source
	< Précédent Suivant > Installer Annuler

L'installation du contrôleur de domaine et de l'Active Directory se lance ; patientez :

Avant de commencer Avant de commencer Type d'installation Afficher la progression de l'installation Sélection du serveur Installation de fonctionnalité Rôles de serveurs Installation démarrée sur win2022

A la fin du processus, un message s'affiche en indiquant la réussite de l'installation ; cliquez sur « Fermer » :

Installation de fonctionnalité
Configuration requise. Installation réussie sur win2022.
Services AD DS Des étapes supplémentaires sont requises pour faire de cet ordinateur un contrôleur de domaine. Promouvoir ce serveur en contrôleur de domaine
Gestion de stratégie de groupe
Outils d'administration de serveur distant Outils d'administration de rôles Outils AD DS et AD LDS Module Active Directory pour Windows PowerShell Outils AD DS
Vous pouvez fermer cet Assistant sans interrompre les tâches en cours d'exécution. Examinez leur progression ou rouvrez cette page en cliquant sur Notifications dans la barre de commandes, puis sur Détails de la tâche. Exporter les paramètres de configuration
< Précédent Suivant > Fermer Annuler

Le menu du gestionnaire de serveur affiche maintenant une alerte (triangle jaune) ; cliquez dessus :



• Cliquez sur le lien « Promouvoir ce serveur en contrôleur de domaine » :



 Cliquez sur « Ajouter une nouvelle forêt » et saisissez le nom que vous souhaitez donner à votre contrôleur de domaine :

Configuration de	déploiement	SERVEUR CIBLE win2022
Configuration de déploie Options du contrôleur de Options supplémentaires Chemins d'accès Examiner les options Vérification de la configur Installation Résultats	Sélectionner l'opération de déploiement Ajouter un contrôleur de domaine à un domaine existant Ajouter un nouveau domaine à une forêt existante Ajouter une nouvelle forêt Spécifiez les informations de domaine pour cette opération Nom de domaine racine : tutos-info.ft	
	En savoir plus sur les configurations de déploiement	
	< Précédent Suivant > Installer	Annuler

• Saisissez un mot de passe pour le mode de restauration des services d'annuaire et cliquez « Suivant » :

Options du contrá	òleur de domaine	SERVEUR CIBLE win2022
Configuration de déploie Options du contrôleur de Options DNS Options supplémentaires Chemins d'accès Examiner les options Vérification de la configur Installation Résultats	Sélectionner le niveau fonctionnel de la nouvelle forêt et du domaine racine Niveau fonctionnel de la forêt : Windows Server 2016 ✓ Niveau fonctionnel du domaine : Windows Server 2016 ✓ Spécifier les fonctionnalités de contrôleur de domaine Serveur DNS (Domain Name System) ✓ Catalogue global (GC) Contrôleur de domaine en lecture seule (RODC) Taper le mot de passe du mode de restauration des services d'annuaire (DSRM) Mot de passe : Confirmer le mot de passe :	
	En savoir plus sur les options pour le contrôleur de domaine	
	< Précédent Suivant > Installer	Annuler

• Cliquez le bouton « Suivant » (pour l'instant nous ne créons pas de délégation DNS) :

Options DNS	SERVEUR CIE win20	3LE 122
Il est impossible de créer u	ne délégation pour ce serveur DNS car la zone parente faisant autorité est intro Afficher plus	۲,
Configuration de déploie Options du contrôleur de Options DNS	Spécifier les options de délégation DNS Créer une délégation DNS	
Options supplementaires		
Examiner les options		
Vérification de la configur		
Installation		
Résultats		
	En savoir plus sur la délégation DNS	
	< Précédent Suivant > Installer Annuler	

• Patientez le temps que le nom NetBIOS attribué au domaine soit validé et cliquez « Suivant » :

Options supplém	entaires	SERVEUR CIBLE win2022
Configuration de déploie Options du contrôleur de Options DNS Options supplémentaires Chemins d'accès Examiner les options Vérification de la configur Installation Résultats	Vérifiez le nom NetBIOS attribué au domaine et modifiez-le s Le nom de domaine NetBIOS : TUTOS-INFO	si nécessaire.
	En savoir plus sur d'autres options	Installer

• On laisse, ci-dessous, l'emplacement par défaut et on clique sur « Suivant » :

Chemins d'accès		SERVEUR CIBLE win2022
Configuration de déploie Options du contrôleur de Options DNS Options supplémentaires Chemins d'accès Examiner les options Vérification de la configur Installation Résultats	Spécifier l'emplacement de la base d Dossier de la base de données : Dossier des fichiers journaux : Dossier SYSVOL :	e données AD DS, des fichiers journaux et de SYSVOL C:\Windows\NTDS C:\Windows\SYSVOL
	En savoir plus sur les chemins d'accè	s Active Directory
	<	Précédent Suivant > Installer Annuler

• Vérifiez l'ensemble de la configuration et, si tout est correct, cliquez « Suivant » :

Examiner les optio	DDS SERVEUR CIBLE win2022
Configuration de déploie Options du contrôleur de Options DNS Options supplémentaires Chemins d'accès Examiner les options Vérification de la configur Installation Résultats	Vérifiez vos sélections : Configurez ce serveur en tant que premier contrôleur de domaine Active Directory d'une nouvelle forêt. Le nouveau nom de domaine est « tutos-info.fr ». C'est aussi le nom de la nouvelle forêt. Nom NetBIOS du domaine : TUTOS-INFO Niveau fonctionnel de la forêt : Windows Server 2016 Niveau fonctionnel du domaine : Windows Server 2016 Options supplémentaires : Catalogue global : Oui Serveur DNS : Oui Ces paramètres peuvent être exportés vers un script Windows PowerShell pour automatiser des installations supplémentaires Afficher le script En savoir plus sur les options d'installation
	< Précédent Suivant > Installer Annuler

• Patientez pendant la vérification de la configuration :

Vérification de la configuration requise

Configuration de déploie... Options du contrôleur de... Options DNS

La configuration requise doit être validée avant que les services de domaine Active Directory soient installés sur cet ordinateur

Vérification des conditions préalables pour le fonctionnement du contrôleur de domaine...

Si la configuration générale est valide, le bouton « Installer » s'active ; cliquez-le pour lancer le processus :



L'installation est lancée ; le processus peut prendre du temps selon la puissance de votre machine : patientez !

Installation	SERVEUR CIBLE win2022
Configuration de déploie Options du contrôleur de	État d'avancement Création en cours de la partition d'annuaire : CN=Schema,CN=Configuration,DC=tutos-info,DC=fr; 1585 objets restants

Lorsque le processus est terminé, redémarrez votre serveur.

Une fois le serveur redémarré, ouvrez une session en tant qu'administrateur : le gestionnaire de serveur se lance et affiche les rôles installés :



IMPORTANT

Attention, lorsque vous installez le rôle AD DS, <u>nous vous conseillons fortement de modifier l'adresse DNS de</u> <u>votre serveur</u>.

- Ouvrez l'explorateur en cliquant l'icône dans la barre des tâches
- Faites un clic droit sur « Réseau » et « Propriétés » :



- Cliquez, dans la partie gauche, sur « Modifier les paramètres de la carte »
- Faites un clic droit sur l'icône du réseau et cliquez « Propriétés » :



• Sélectionnez « Protocole Internet version 4 (TCP/IPv4) » et cliquez le bouton « Propriétés » :



Accédez aux propriétés du protocole TCP/IPv4 pour définir l'adresse IP fixe.

• Modifiez l'adresse du DNS affectée par Microsoft par l'adresse IP du serveur lui-même et cliquez « OK » :

Propriétés de : Protocole Internet version 4 (TCP/IPv4)	Propriétés de : Protocole Internet version 4 (TCP/IPv4) ×
Général	Général
Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.	Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.
Obtenir une adresse IP automatiquement	Obtenir une adresse IP automatiquement
● Utiliser l'adresse IP suivante :	Utiliser l'adresse IP suivante :
Adresse IP : 192 . 168 . 183 . 22	Adresse IP : 192 . 168 . 183 . 22
Masque de sous-réseau : 255 . 255 . 255 . 0	Masque de sous-réseau : 255 . 255 . 0
Passerelle par défaut : 192 . 168 . 183 . 240	Passerelle par défaut : 192 . 168 . 183 . 240
Obtenir les adresses des serveurs DNS automatiquement	Obtenir les adresses des serveurs DNS automatiquement
O Utiliser l'adresse de serveur DNS suivante :	• Utiliser l'adresse de serveur DNS suivante :
Serveur DNS préféré : 127 . 0 . 0 . 1	Serveur DNS préféré : 192 . 168 . 183 . 22
Serveur DNS auxiliaire :	Serveur DNS auxiliaire :
Valider les paramètres en quittant Avancé	Modifiez l'adresse du serveur DNS Avancé
La service DNC a tht market OK Annuler	est le serveur lui-même (remettre OK Annuler
suite à l'installation du rôle AD DS	son IP.
par l'adresse « 1270.0.1 ».	

Votre contrôleur de domaine et Active Directory est maintenant fonctionnel. Nous étudierons, dans un autre tutoriel, comment administrer l'Active Directory (gestion des utilisateurs, des lecteurs réseau et des stratégies).