Active directory

1. Qu'est-ce que l'Active Directory (AD) ?

L'Active Directory (AD) est un service d'annuaire développé par Microsoft pour les systèmes Windows Server. Il permet de centraliser la gestion des utilisateurs, des ordinateurs et des ressources (comme des imprimantes ou des partages réseau) dans un réseau d'entreprise.

Comment fonctionne l'Active Directory ?

• L'AD fonctionne selon une structure hiérarchique basée sur des domaines, des arbres et des forêts.

• Les données sont stockées dans une base de données distribuée, appelée NTDS (NT Directory Services).

• Il utilise le protocole LDAP (Lightweight Directory Access Protocol) pour interagir avec d'autres systèmes et clients.

• L'authentification est assurée par le protocole Kerberos, et les objets sont organisés en unités organisationnelles (OU).

• Un contrôleur de domaine (DC) est chargé de gérer toutes les authentifications et l'accès aux ressources.

4. Quels sont les points clés de son fonctionnement ?

• Contrôleur de domaine : Point central de gestion du réseau.

Page | 1 Thomas Kireche 2024

- **Unités organisationnelles :** Permettent d'organiser les objets AD pour appliquer des stratégies spécifiques.
- **GPO (Group Policy Objects) :** Règles appliquées à des utilisateurs ou ordinateurs pour définir leurs comportements.
- **Replication :** Les DC répliquent les données AD entre eux pour garantir une disponibilité et une cohérence des informations.

5. Comment installer l'Active Directory sur Windows Server 2022 ?

Pré-requis :

- Un serveur Windows Server 2022 avec un nom unique et une adresse IP statique.
- Les privilèges administratifs sur la machine.

Installation des services AD

- Ouvrez le Gestionnaire de serveur.
- Cliquez sur Ajouter des rôles et des fonctionnalités.

Gestionnaire de serveur				- 0 X
Gestionnaire de	e serveur • Tableau d	le bord	• ②	Gérer Outils Afficher Aide
Tableau de bord BIENV Serveur local Tous les serveurs	VENUE DANS GESTIONNAIRE DE	serveur		Ajouter des rôles et fonctionnalités Supprimér des rôles et fonctionnalités Ajouter des serveurs Créer un groupe de serveurs Propriétés du Gestionnaire de serveur
Services de fichiers et d P	VEAUTÉS 2 Ajou 3 Ajou 4 Crée 5 Con	uter des rôles et des fonctionnali uter d'autres serveurs à gérer er un groupe de serveurs inecter ce serveur aux services c	tés loud	Masquer
Rôles : Rôles :	et groupes de serveurs 1 Groupes de serveurs : 1 Nomb Services de fichiers et 1 de stockage 1 Facilité de gestion Événements Performances Résultats BPA	re total de serveurs : 1 Serveur local 1 Facilité de gestion Événements Services Performances Résultats BPA 09/10/2024 14:01	 Tous les serveurs 1 Facilité de gestion Événements Services Performances Résultats BPA 09/10/2024 14:01 	
Assistant Ajout de rôles et de Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités Confirmation	Cet Assistant perm déterminer les rôle de votre organisat Pour supprimer de Démarrer l'Assista Avant de continue • Le compte d'adn	net d'installer des rôles, des se es, services de rôle ou fonctior ion, tels que le partage de do es rôles, des services de rôle ou nt de Suppression de rôles et er, vérifiez que les travaux suiva ninistrateur possède un mot d	rvices de rôle ou des fonction malités à installer en fonction cuments ou l'hébergement d'u u des fonctionnalités : de fonctionnalités ants ont été effectués : e passe fort	- C X
kesultats 	 Les paramètres ri Les dernières mi Si vous devez vérit exécutez les étape Cliquez sur Suivan Ignorer cette 	réseau, comme les adresses IP ses à jour de sécurité de Wind filòque l'une des conditions p is, puis relancez l'Assistant. It pour continuer.	statiques, sont configurés ows Update sont installées réalables ci-dessus a été satisf	aite, fermez l'Assistant,
		< Précéo	lent Suivant >	Installer Annuler

	1 Configurar co convour local			
📥 Assistant Ajout de rôles et de fo	onctionnalités	-		\times
Assistant Ajout de rôles et de for Sélectionner le ty Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités Confirmation Résultats	 pe d'installation Sélectionnez le type d'installation. Vous pouvez installer des rôles et el ordinateur physique ou virtuel en fonctionnement, ou sur un disque el ordinateur physique ou virtuel en ajoutant des rôles, des services de Configurez un serveur unique en ajoutant des rôles, des services de linstallation des services Bureau à distance Installation des services de rôle nécessaires à l'infrastructure VDI (Virtu déployer des bureaux basés sur des ordinateurs virtuels ou sur des 	SERVEUR DE WIN-3 des fonctionnalités sui dur virtuel hors conne de rôle et des fonction ual Desktop Infrastruct s sessions.	DESTINATIC BODAQOFUF r un exion. nalités. ture) pour	X DN B9
	< Précédent Suivant >	Installer	Annule	r

• Dans la liste des rôles, cochez Services AD DS et cliquez sur Suivant.



Installez les dépendances nécessaires et terminez l'installation.







🚖 Assistant Ajout de rôles et de	fonctionnalités	-		×
Assistant Ajout de roies et de Confirmer les sél 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 ser Installer. Image: Comparison of the serveur de destination, si nécessaire Il se peut que des fonctionnalités facultatives (comme des outils d'administ cette page, car elles ont été sélectionnées automatiquement. Si vous ne voi fonctionnalités facultatives, cliquez sur Précédent pour désactiver leurs case Gestion de stratégie de groupe Outils d'administration de serveur distant Outils d'administration de rôles Outils AD DS et AD LDS	SERVEUR DE DESTINATION WIN-30DAQOFUFB9 rveur sélectionné, cliquez sur tration) soient affichées sur pulez pas installer ces es à cocher.		
	Module Active Directory pour Windows PowerShell Outils AD DS Centre d'administration Active Directory Composants logiciels enfichables et outils en ligne de o Services AD DS Exporter les paramètres de configuration Spécifier un autre chemin d'accès source < Précédent	commande AD I	Annuk	er





Configurer le contrôleur de domaine :

• Une fois le rôle AD DS installé, cliquez sur la notification **Promouvoir ce serveur en contrôleur de domaine**.



• Choisissez **Ajouter une nouvelle forêt** si c'est le premier DC, et entrez le nom de domaine (ex. : exemple.local).

🚡 Assistant Configuration des servi	ices de domaine Active Directory			_		×
Configuration de d	W	SER	VEUR C	IBLE IFB9		
Configuration de déploie Options du contrôleur de Options DNS 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 Ajouter un nouveau domaine à une f Ajouter une nouvelle forêt Spécifiez les informations de domaine pu Nom de domaine racine : S	un domaine existant forêt existante our cette opération lan.local				
	En savoir plus sur les configurations de c < Pré	déploiement cédent Suivant >	Installer		Annule	r

- Configurez le niveau fonctionnel de la forêt et du domaine (Windows Server 2016 par défaut).
- Définissez un mot de passe pour le mode de restauration des services d'annuaire.
- Laissez les paramètres DNS par défaut (le rôle DNS est installé automatiquement).

🚡 Assistant Configuration des servi	ces de domaine Active Directory	- 0	×
Doptions du contrô	leur de domaine	SERVEUR CIB WIN-30DAQOFUFI	LE B9
Configuration de déploie O Options du contrôleur de options DNS	Sélectionner le niveau fonctionnel de la nouvelle forêt et Niveau fonctionnel de la forêt : Windows Serve	er 2016 v	
Options supplémentaires Chemins d'accès Examiner les options Vérification de la configur Installation Résultats	Niveau fonctionnel du domaine : Windows Servi 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 servi Mot de passe :	ices d'annuaire (DSRM)	
	En savoir plus sur les options pour le contrôleur de doma	aine ant > Installer Annuler	

•

• Terminez la configuration et redémarrez le serveur. (laissez la configuration par défaut)

Š	Assistant Configuration des servic	es de domaine Active Directory	-		×	
b	Options DNS		S WIN-3	ERVEUR 0DAQOI	CIBLE FUFB9	
H	🛕 Il est impossible de créer une	délégation pour ce serveur DNS car la zone parente faisant autorité est intro	Affiche	r plus	×	
D Pr	Configuration de déploie Options du contrôleur de Options DNS Options supplémentaires Chemins d'accès Examiner les options Vérification de la configur Installation Résultats	Spécifier les options de délégation DNS				
		En savoir plus sur la délégation DNS				
		< Précédent Suivant > Insta	ller	Annu	ler	

🏊 Assistant Configuration des servi	-		×	
Options suppléme	entaires	SE WIN-30	RVEUR C DAQOFL	IBLE JFB9
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 si nécessaire. Le nom de domaine NetBIOS : LAN			
	En savoir plus sur d'autres options			
	< Précédent Suiv t > Ins	taller	Annule	er

📥 Assistant Configuration des servi	ices de domaine Active Directory		-		×
Chemins d'accès			SE WIN-30	RVEUR (CIBLE UFB9
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 :	de données AD DS, des fichiers journ C:\Windows\NTDS C:\Windows\NTDS C:\Windows\SYSVOL	naux et de SYS1		
	En savoir plus sur les chemins d'accè	Is Active Directory			
	<	Précédent Sivant >	Installer	Annul	er





Installation	SERVEUR CIBLE WIN-30DAQOFUFB9
Configuration de déploie Options du contrôleur de Options DNS Options supplémentaires Chemins d'accès Examiner les options Vérification de la configur Installation Résultats	État d'avancement
	En savoir plus sur les options d'installation
Assistant Configuration des services de Résultats	< <p></p>
Assistant Configuration des services de Résultats	< <tr> < Précédent Suivant > Installer Annuler e domaine Active Directory - × •</tr>
Assistant Configuration des services de Résultats Configuration de déploie Options du contrôleur de Options DNS Options supplémentaires Chemins dacrès	< Précédent
Assistant Configuration des services de Résultats Ce serveur a été correctement corr Configuration de déploie Options du contrôleur de Options DNS Options supplémentaires Chemins d'accès Examiner les options Vérification de la configur Installation Résultats	< <p> Yrécédent Suivant > Installer Annuler Annuler Serveux Directory Serveux CIBLE WIN-30DAQOFUEB9 figuré en tant que contrôleur de domaine Afficher plus × Afficher les résultats détaillés de l'opération Les contrôleurs de domaine Windows Server 2022 offrent un paramètre de sécurité par défaut nommé « Autoriser les algorithmes de chiffrement compatibles avec Windows NT 4.0 ». Ce paramètre empèche l'utilisation d'algorithmes de chiffrement faibles lors de l'établissement de sessions sur canal sécurisé. Vous allez être déconnecté L'ordinateur est redémarré car les services de domaine Active Directory ont été installés ou supprimés. Fermer</p>
Assistant Configuration des services de Résultats Ce serveur a été correctement cor Configuration de déploie Options du contrôleur de Options DNS Options supplémentaires Chemins d'accès Examiner les options Vérification de la configur Installation Résultats	< <tr>< Précédent</tr>



1. Création d'une OU (Unité Organisationnelle)

• Recherchez Active Directory utilisateurs, et ouvrez l'outil.

🔁 Gestionnaire de serveur		- 0 ×					
Gestionna	aire de serveur • Tableau de bord	🔹 🍘 🚩 Gérer 🛛 Outils Afficher Aide					
Tableau de bord	BIENVENUE DANS GESTIONNAIRE DE SERVEUR	Analyseur de performances Centre d'administration Active Directory Configuration du système					
Serveur local Tous les serveurs AD DS DNS Services de fablique ad de balance	DÉMARRAGE RAPIDE	Déragmenter et optimiser les lecteurs Diagnostic de mémoire Windows DNS Domaines et approbations Active Directory Éditeur du Registre					
■ Services de lichiers et d ν	Ajouter d'autres serveurs à gérer Créer un groupe de serveurs	Gestion de l'ordinateur Gestion des stratégies de groupe Informations système Initiateur /SCSI Lecteur de récupération					
	COnnecter de serveur aux services cloud	Modification ADSI Module Active Directory pour Windows PowerShell Moniteur de ressources Nettoyage de disque Observateur d'événements ODBC Data Sources (32-bit)					
	Image: Services and the state of the services o	Pare-feu Windows Defender avec fonctions avancées de sécurité Planificateur de tâches Sauvegarde Windows Server Services Services de composants Services Microsoft Azure Sites et services Active Directory Sources de données ODBC (64 bits) Stratégie de sécurité locale Utilisateurs et ordinateurs Active Directory Windows PowerShell Windows PowerShell (x86)					

- 1. Créer une nouvelle Unité Organisationnelle (OU) :
- Dans le volet de gauche, faites un clic droit sur le nom de votre domaine (par exemple, exemple.local).
- Sélectionnez Nouveau > Unité d'organisation.
- Donnez un nom à l'OU, comme RH, IT, ou Comptabilité.
- Cochez l'option Protéger contre une suppression accidentelle (recommandé).
- Cliquez sur **OK**.
- 2. Vérifier l'apparition de l'OU :
- L'OU apparaît sous le domaine dans la structure hiérarchique.

Utilisateurs et ordinateurs Active	e Directory			-	×
Fichier Action Affichage ?					
← → 💼 Q 🕞 🛛 📰	8 2 1 7 2	3			
Utilisateurs et ordinateurs Active Computers Computer	Nom alan.local Requêtes en	Type Domaine	Description Dossier pour stocker vos.		
< >>					

2. Création d'un utilisateur dans l'OU

1. Naviguer jusqu'à l'OU cible :

• Dans la console, cliquez sur l'OU que vous venez de créer.

Page | 21

Thomas Kireche

2. Créer un utilisateur :

- Faites un clic droit dans l'espace vide de l'OU.
- Sélectionnez **Nouveau** > **Utilisateur**.

3. Remplir les informations de l'utilisateur :

- **Prénom :** Entrez le prénom.
- **Nom :** Entrez le nom.
- Nom d'ouverture de session : Saisissez un identifiant unique (exemple : jdupont).

4. Configurer le mot de passe :

- Définissez un mot de passe pour l'utilisateur.
- Options disponibles :
 - L'utilisateur doit changer son mot de passe à la prochaine ouverture de session : recommandé.
 - L'utilisateur ne peut pas changer le mot de passe : pour des comptes spécifiques.
 - Le mot de passe n'expire jamais : à éviter pour des utilisateurs standards.
 - Le compte est désactivé : cochez si l'utilisateur ne doit pas encore se connecter.

5. Terminer :

- Cliquez sur **Suivant**, puis sur **Terminer**.
- L'utilisateur apparaît maintenant dans l'OU.

📑 U Fichi	Jtilisa ier	ateurs et ordinateurs Activ	e Directory			-		×
(= =	♦	2 🖂 🖌 🗋 🗙 🛙	.	1 🗏 速 🛍 🎙	r 🖻 🕱			
U > iii > iii > >	tilisat Rec lan	teurs et ordinateurs Active quêtes enregistrées alocal Builtin Computers Domain Controllers ForeignSecurityPrincipal: Managed Service Accour Délégation de con Rechercher	Nom Administrat Administrat Administrat Administrat Administrat Administrat Contrôlour, trôle	Type Utilisateur Groupe de séc Groupe de séc	Description Compte d'utilisateur d'a Les membres de ce grou Administrateurs désigné Administrateurs désigné Administrateurs désigné Tous les contrôleurs de Les membres de ce grou Les membres de ce grou			~
< Crée u	in no	Nouveau Toutes les tâches Affichage Actualiser Exporter la liste Propriétés Aide Aide	Protected Serveurs R teneur.	Ordinateur Contact Groupe InetOrgPerson msDS-KeyCrede msDS-Resourcef msDS-ShadowPr msImaging-PSP Alias de file d'att Imprimante Utilisateur	ntial PropertyList rincipalContainer s eente MSMQ			~
oleau o rveur k us les s) DS ICP IS rvices o		Itelifications at ordinations for Arr Nouvel objet - Utilisateur Créer dans : Ian Jo Prénom : Ithomas Nom : Ithomas Nom d'ouverture de session d Ithomas Nom d'ouverture de session d LAN\	cal/Users cal/Us	itiales : witiales : Windows 2000) : Suivant > Anni Groupe de séc Groupe de séc	 on bbres qui ont un trateurs désigné trateurs désigné trateurs désigné trateurs désigné trateurs désigné tontrôleurs de bbres de ce grou bbres de ce grou bbres de ce grou ts DNS qui sont bbres de ce grou ts DNS qui sont bbres de ce grou te passe des de passe des d'utilisateur inv nvités du doma s stations de tra Les membres de ce group Les serveurs de ce group Les membres qui ont un Tous les utilisateurs du d 		×	Activat 00454-

	Utilisateurs et ordinateurs Active	Directory			-	×	
pleau o	Fichier Action Affichage ?						
rveur l	🗢 🔿 🙍 📅 🤞 🖄 🛛	i 🖪 🗟 🖬	1 🙎 🔌 🛍 🎙	r 🗾 🔍			
rveur li us les s) DS (CP (S rvices)	 Itilisateurs et ordinateurs Active Itilisateurs et ordinateurs Active Requêtes enregistrées Itilin Itilin Computers Domain Controllers ForeignSecurityPrincipal: Managed Service Accour Users 	Nom Administrat Administrat Administrat Contrôleurs .	Type Groupe de séc Groupe de séc	Description Les membres qui ont un Administrateurs désigné Administrateurs désigné Tous les contrôleurs de Les membres de ce grou Les membres de ce grou Les membres de ce grou Croupe des administrate Les clients DNS qui sont Les membres de ce grou Les membres de ce grou Les membres de ce grou Les mots de passe des Compte d'utilisateur inv Tous les invités du doma Toutes les stations de tra Les membres de ce grou Les membres de ce grou		~	Activati
		Serveurs RA	Groupe de séc	Les serveurs de ce group			2
		Utilisateurs	Groupe de séc	Les membres qui ont un			0:03:30
	< >	A Utilisateurs	Groupe de séc	Tous les utilisateurs du d		~	0:03:30

3. Ajouter un poste de travail au domaine

Pré-requis :

Configuration DNS correcte : Le poste doit utiliser comme serveur DNS l'adresse IP de votre contrôleur de domaine (par exemple : 192.168.0.1).

Compte avec droits d'ajout au domaine : Utilisez un compte administrateur du domaine ou avec des permissions spécifiques.

anne an	Modifier la stratégie de groupe Panneau de configuration	>	
	Paramètres		Changer le nom du groupe de travail
	Sérer le groupe familial	>	Panneau de configuration
	Changer le nom du groupe de travail		C Ouvrir
	Paramètres des groupes d'ancrage	>	
	Afficher le groupe de travail dans lequel se trouve l'ordinateur	>	
	Rechercher sur le Web		
	Q groupe - Afficher plus de résultats de recherche	>	
Section 25	Q groupe electrogene	>	
	Q groupe verlaine	>	
	Groupe ADP	>	
	Q groupe bpce	>	
		1.5.16.973	A1
	Q nom du groupe de travail	-	💽 🖻 💁 🔹 🔊 🔹

Rejoindre le domaine :

- Sous Membre de, cochez Domaine.
- Entrez le nom complet du domaine (exemple : exemple.local).
- Cliquez sur OK.



- Une fenêtre apparaît pour entrer un compte autorisé.
- Saisissez un identifiant et mot de passe administrateur du domaine (par exemple : Administrateur ou admin@exemple.local).





Confirmer et redémarrer :

- Un message de confirmation s'affiche indiquant que le poste a rejoint le domaine.
- Cliquez sur OK et redémarrez le poste de travail.

rarametres ropriétés système					
ropriétés système				- 0	X Marine
	>	×	- 0	×	
Modification du nom ou du domaine de l'ordinateur	× on à distance		-		-
Vous pouvez modifier le nom et l'appartenance de cet	ł		chercher	P	100
ordinateur. Ces modifications peuvent influer sur l'accès aux ressources réseau.	r votre			2	
		HOMAS			
Nom de l'ordinateur :		ompte local		_	Sec. 1
admin	U		Thomas		Sp
Nom complet de l'ordinateur : admin	IVIC	partication du nom ou du domaine de l'ordinateur	Compte local		1.
		Vous devez redémarrer votre ordinateur	Administrateur Protégé par mot de	passe	
Autres	la récerc	pour appliquer ces modifications.			
Membre d'un	ie reseau	Avant de redémarrer, enregistrez les fichiers ouverts et			- ×
lan.local	flor	fermez tous les programmes.			
Groupe de travail :	Der	OK2			
LAN					
		tout co que Microsoft			
OK Annuler		r tout ce que microsort			
		raduits et services Microsoft			
		eul compte. Votre compte			
		onnecte aux fichiers, photos,			
OK Annular	Appliquer	ntenus qui vous intéressent le			
Accessionite					
		Autre utilisateur			
		Autre utilisateur			
		Autre utilisateur Ian\thomas Ian\thomas			
		Autre utilisateur Ian\thomas Ian\thomas Ian\thomas			
		Autre utilisateur			
		Connectez-vous à lan Comment me connecter à un autre domaine ?			
		Connectez-vous à lan Comment me connecter à un autre domaine ?			
		Connectez-vous à lan Comment me connecter à un autre domaine ?			



Page | 30 Thomas Kireche 2024