PRÉSENTÉ PAR DRUELLE NICOLAS

TP-AD DS





POUR CE TP NOUS AURONS BESOIN DE 2 MACHINES :



Une machine windows server 2019 qui va nous permettre de mettre en place l'AD DS Ainsi qu'une machine windows 10 qui va permettre de tester les utilisateurs ainsi que la connection au domaine



ADRESSAGE IP DU SERVEUR

Dans un premier temps nous allons configurer l'adresse ip ainsi que le nom du serveur

Propriétés de : Protocole Internet	version 4 (TCP/IPv4)	×
Général		
Les paramètres IP peuvent être de réseau le permet. Sinon, vous dev appropriés à votre administrateur	éterminés automatiquement si votre ez demander les paramètres IP réseau.	
Obtenir une adresse IP autor	matiquement	
• Utiliser l'adresse IP suivante :		-
Adresse IP :	192.168.120.1	
Masque de sous-réseau :	255.255.255.0	
Passerelle par défaut :		
Obtenir les adresses des serv	veurs DNS automatiquement	
● Utiliser l'adresse de serveur D	DNS suivante :	-
Serveur DNS préféré :	192.168.120.1	
Serveur DNS auxiliaire :		
🗌 Valider les paramètres en qu	ittant Avancé	
	OK Annule	r

Modification and nom ou du domaine de l'ordinateur X

Vous pouvez modifier le nom et l'appartenance de cet ordinateur. Ces modifications peuvent influer sur l'accès aux ressources réseau.

Nom de l'ordinateur :

Druelle_WindowsServer

Nom complet de l'ordinateur : Druelle_WindowsServer.druelle.com

Domaine :		
druelle.com		
Course de traveil :		
Groupe de travail :		

Autres...

INSTALLATION DE L'ACTIVE DIRECTORY

	Gérer	Outils	Afficher	Aide
Ajoute	er des rôl	les et fonc	tionsalités	
Suppr	imer des	rôles et fo	onctionnalite	és
Ajoute	er des sei	rveurs		
Créer	<mark>un grou</mark> p	pe de serve	eurs	
Propri	étés du (Gestionnai	re de servei	Jr

Assistant Ajout de rôles et de fonctionnalités	– 🗆 ×	Assistant Ajout de rôles et de	e fonctionnalités	- 0 ×	Assistant Ajout de rôles et de fonctionnalités	×
Sélectionner le serveur de destination Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités Confirmation Résultats Nom Druelle_WindowsServer.druelle.c 1 ordinateur(s) trouvé(s) Cette page présente les serveurs nouvellement a incomplète ne sont pas répertoriés.	SERVEUR DE DESTINATION Druelle_WindowsServer.druelle.com	Sélectionner des Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités AD DS Confirmation Résultats	Sélectionnez un ou plusieurs rôles à installer sur le serveur sel Rôles Hyper-V Hyper-V Serveur de télécopie Serveur DHCP Serveur DHCP Serveur DHCP Serveur DHS Serveur Web (IIS) Services AD DS Services de télération Active Directory Lightweight Dire Services AD DS Services AD DS Services de deploiement Windows Services de fichiers et de stockage (1 sur 12 install Services WSUS (Windows Server Update Services)	Ectionné. Description As 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 au processus d'ouverture de session unique.	Ajouter les fonctionnalités requises pour Services A DS ? Vous ne pouvez pas installer Services AD DS sauf si les services a rôle ou les fonctionnalités suivants sont également installés. [Outils] 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 PowerSh • Outils] Centre d'administration Active Direct [Outils] Composants logiciels enfichables et d v Inclure les outils de gestion (si applicable)	e ell ory utils e
< Précédent	Suivant > Installer Annuler		< Précédent Suiva	ant > Installer Annuler		

Pour l'installation de l'active directory nous allons dans un premier temps ajouter une fonctionnalités et nous selectionnons ensuite le serveur ad ds

INSTALLATION DU DNS

UNE FOIS LA CONFIGURATION DE L'IP ET DU NOM RÉALISÉE NOUS ALLONS METTRE EN PLACE LE DNS

📥 Assistant Configuration des serv	ices de domaine Active Directory				5 <u>—</u> 3		×
\searrow							
Options suppléme	entaires				SE Druelle_W	RVEUR C	CIBLE
Configuration de déploie Options du contrôleur de Options DNS	Vérifiez le nom NetBIOS attribu Le nom de domaine NetBIOS :	é au domaine e	et modifiez-le si né ELLE	cessaire.			
Options supplémentaires							
Chemins d'accès							
Examiner les options							
Vérification de la configur							
Installation							
Résultats							
	En savoir plus sur d'autres optic	ons					
		< Précéden	t Suivant >	In	staller	Annule	er

📥 Assistar
Conf
Config
Optio
Op
Optio
Chem
Exami
Vérific
Install
Résult

Dans un premier temps nous allons configurer une nouvelle forêt avec le nom de notre domaine ici "druelle.com"



istant Configuration des services de domaine Active Directory

SERVEUR CIBLE

Druelle WindowsServer

onfiguration de déploiement

du contrôleur de			
ons DNS	Ajouter un controleur de dor Ajouter un controleur de dor	naine a un domaine existant	
supplémentaires	 Ajouter un nouveau domaine O Ajouter une nouvelle forêt 	a une foret existante	
s d'accès		na sana sana sana sana sana sana sana s	
r les options	Specifiez les informations de doi	naine pour cette operation	
ion de la configur	Nom de domaine racine :	druelle.com	
on			
5			

< Précédent Suivant > Installer Annuler

Ensuite nous vérifions le nom du domaine netos

INSTALLATION DU DNS

CRÉATION DE LA ZONE DE RECHERCHE

📓 Gestion de stratégie	de groupe		- 🗆 X	🏯 Gestionnaire DNS	- 🗆 X	Assistant Nouvelle zone X
Image: Fichier Action A Image: Fichier Action Action Action Action A Image: Fichier Action Actio	ffichage Fenêtre ? Image: senerce in the senerce	s Délégation	- 5 ×	Fichier Action Affichage ? Image: Provide the state of the state		Type de zone Le serveur DNS prend en charge différents types de zones et de stockages.
 Domaines druelle.co Def Dor Obj Filtr Obj Filtr Sites Modélisatio Résultats d 	m Domaine : drue Modifier Appliqué Lien activé Enregistrer le rapport Affichage Nouvelle fenêtre à partir d'ici Supprimer Renommer Actualiser Aide	belogditti sile.com du domaine (DRUELLE\Admins du domaine) 2024 14:09:34 2024 14:16:18 0 (SYSVOL) 3 (SYSVOL) 340-016D-11D2-945F-00C04FB984F9}		 Zones de recherche direc msdcs.druelle.com druelle.com Zones de recherche invelle zones. Chaque zone stocke des informations relatives à un continue Points d'api Nouvelle zone Actualiser Aide 	n d'un espace de noms DNS en nou plusieurs domaines DNS cliquez sur Nouvelle zone.	 Sélectionnez le type de zone que vous voulez créer : ② Zone principale Crée une copie d'une zone qui peut être mise à jour directement sur ce serveur. O Zone secondaire Crée une copie de la zone qui existe sur un autre serveur. Cette option aide à équilibrer la charge de travail des serveurs principaux et autorise la gestion de la tolérance de pannes. O Zone de stub Crée une copie d'une zone contenant uniquement des enregistrements Nom de serveur (NS), Source de nom (SOA), et éventuellement des enregistrements « glue Host (A) ». Un serveur contenant une zone de stub ne fait pas autorité pour cette zone. > Enregistrer la zone dans Active Directory (disponible uniquement si le serveur DNS est un contrôleur de domaine accessible en écriture)
< Renomme la sélection en	>			< > Actualise la sélection actuelle.		< Précédent Suivant > Annuler

Ensuite nous allons crée une nouvelle zone de recherche dans notre dns ce qui nous servira plus tard pour la vérification de la connexion poste dns.

INSTALLATION DU DNS CRÉATION DE LA ZONE DE RECHERCHE

Assistant Nouvelle zone	×	Assistant Nouvelle zone X
Étendue de la zone de réplication de Active Directory Vous pouvez sélectionner la façon dont les données DNS doivent être répliquées sur votre réseau.		Nom de la zone de recherche inversée Une zone de recherche inversée traduit les adresses IP en noms DNS.
Choisissez la façon dont les données de la zone doivent être répliquées :		Choisissez si vous souhaitez créer une zone de recherche inversée pour les adresses IPv4
Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans cette fo druelle.com	rêt :	ou les adresses IPv6.
Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine : druelle.com		Ozone de recherche inversée IPv4
Vers tous les contrôleurs de ce domaine (compatibilité avec Windows 2000) : druelle.com		○ Zone de recherche inversée IPv6
 Vers tous les contrôleurs de domaine spécifiés dans l'étendue de cette partition d'annuaire : 		
	~	
< Précédent Suivant > Annu	ıler	< Précédent Suivant > Annuler

Dans la nouvelle zone nous allons crée la zone de recherche inversée en ipv4 en y renseignant l'adresse ip du réseau.

Pou	ur identifier la zone de recherche inversé	ée, entrez l'ID réseau ou le nom de la	zone.
۲	ID réseau :		
	192 .168 .120 .		
	L'ID réseau est la partie des adresses I	P qui appartient à cette zone. Entrez	l'ID
		1	
	réseau dans son ordre normal (non inve	ersé).	
	réseau dans son ordre normal (non inve	ersé).	Day
	réseau dans son ordre normal (non inve Si vous utilisez un zéro dans l'ID réseau exemple, l'ID réseau 10 crée la zone 10	ersé). 1, il va apparaître dans le nom de la zo).in-addr.arpa, l'ID réseau 10.0 crée l	one. Par la zone
	réseau dans son ordre normal (non inve Si vous utilisez un zéro dans l'ID réseau exemple, l'ID réseau 10 crée la zone 10 0.10.in-addr.arpa.	ersé). 1, il va apparaître dans le nom de la zo).in-addr.arpa, l'ID réseau 10.0 crée l	one. Par la zone
0	réseau dans son ordre normal (non inve Si vous utilisez un zéro dans l'ID réseau exemple, l'ID réseau 10 crée la zone 10 0.10.in-addr.arpa. Nom de la zone de recherche inversée :	ersé). 1, il va apparaître dans le nom de la zo).in-addr.arpa, l'ID réseau 10.0 crée l	one. Par la zone
0	réseau dans son ordre normal (non inve Si vous utilisez un zéro dans l'ID réseau exemple, l'ID réseau 10 crée la zone 10 0.10.in-addr.arpa. Nom de la zone de recherche inversée : 120.168.192.in-addr.arpa	ersé). 1, il va apparaître dans le nom de la zo).in-addr.arpa, l'ID réseau 10.0 crée l	one. Par la zone
0	réseau dans son ordre normal (non inve Si vous utilisez un zéro dans l'ID réseau exemple, l'ID réseau 10 crée la zone 10 0.10.in-addr.arpa. Nom de la zone de recherche inversée : 120.168.192.in-addr.arpa	ersé). 1, il va apparaître dans le nom de la zo 0.in-addr.arpa, l'ID réseau 10.0 crée l	one. Par la zone
0	réseau dans son ordre normal (non inve Si vous utilisez un zéro dans l'ID réseau exemple, l'ID réseau 10 crée la zone 10 0.10.in-addr.arpa. Nom de la zone de recherche inversée : 120.168.192.in-addr.arpa	ersé). 1, il va apparaître dans le nom de la zo).in-addr.arpa, l'ID réseau 10.0 crée l	one. Par la zone
0	réseau dans son ordre normal (non inve Si vous utilisez un zéro dans l'ID réseau exemple, l'ID réseau 10 crée la zone 10 0.10.in-addr.arpa. Nom de la zone de recherche inversée : 120.168.192.in-addr.arpa	ersé). 1, il va apparaître dans le nom de la zo).in-addr.arpa, l'ID réseau 10.0 crée l	one. Par la zone

INSTALLATION DU DNS CRÉATION DE LA ZONE DE RECHERCHE

Assistant Nouvelle zone X	د Gestionnaire DNS			– 🗆 🗙	Nouvel enregistrement de ressource X
Miseà niveau dynamique Vous pouvez spécifier que cette zone DNS accepte les mises à jour sécurisées,	Fichier Action Affichage ?		10.00	Loss and	Pointeur (PTR)
non sécurisées ou non dynamiques.		Nom Type	Données	Horodate	Adresse IP de l'hôte :
Les mises à jour dynamiques permettent au client DNS d'enregistrer et de mettre à jour de manière dynamique leurs enregistrements de ressources avec un serveur DNS dès qu'une modification a lieu.	Zones de recherche direct Signature de recherche direct Signature de recherche direct Signature de recherche inve	(identique au dossier parent) Source de	nom (SOA) [1], druelle_ e noms (NS) druelle_wind	windowsserver statique dowsserver.dr statique	Nom de domaine pleinement qualifié (FQDN) : 1.120.168.192.in-addr.arpa
Sélectionnez le type de mises à jour dynamiques que vous souhaitez autoriser :	120.168.192.in-	Mettre à iour un fichier de données du serveur			Nom de l'hôte :
N'autoriser que les mises à jour dynamiques sécurisées (recommandé pour Active Directory)	 Points d'approbati Redirecteurs cond 	Charger à nouveau			druelle_windowsserver.druelle.com Parcourir
Cette option n'est disponible que pour les zones intégrées à Active Directory.		Nouvel alias (CNAME)			
O Autoriser à la fois les mises à jours dynamiques sécurisées et non sécurisées Les mises à jour dynamiques d'enregistrement de ressources sont acceptées à partir de n'importe quel client.		Nouvelle délégation Nouveaux enregistrements DNSSEC	>		Autoriser tout utilisateur identifié à mettre à jour tous les enregistrements
Cette option peut mettre en danger la sécurité de vos données car les mises à jour risquent d'être acceptées à partir d'une source non approuvée.		Toutes les tâches	>		enregistrements DNS pour un nouveau nom.
🔿 Ne pas autoriser les mises à jour dynamiques		Affichage	>		
Les mises à jour dynamiques des enregistrements de ressources ne sont pas acceptées par cette zone. Vous devez mettre à jour ces enregistrements manuellement.		Supprimer Actualiser Exporter la liste			
< Précédent Suivant > Annuler	<	Propriétés		>	OK Annuler

Une fois la nouvelle zone crée nous allons ajouté l'adresse ip de notre domaine en cliquant sur "nouveau pointeur".



QUEL SONT LES SERVICES INSTALLÉS ?



- Sur le serveur il y'a 3 services d'installés :
- L'ad ds qui va servir à répertorier les postes / utilisateurs qui se seront sur le domaie -Le dns qui va servir à faire la connection entre les postes et le domaine
 - Le service de fichiers et de stockage qui va permettre de réaliser les partages de fichier.

CONNECTION POSTE CLIENT AU RÉSEAU

Propriétés de : Protocole Internet version 4 (TCP/IPv4)

X

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.

Obtenir une adresse IP automatiquement

• Utiliser l'adresse IP suivante :

Adresse IP :

Masque de sous-réseau :

Passerelle par défaut :

255 . 255 . 255 . 0

192.168.120.2

Obtenir les adresses des serveurs DNS automatiquement

Serveur DNS auxiliaire :	192 . 168	3.120.1	
Valider les paramètres en quittant Avancé			
	ittant	Ava	ancé
	1	192 . 168	192 . 168 . 120 . 1

Vous ordina resso	pouvez modifier le r ateur. Ces modificati urces réseau.	nom et l'appartenar ions peuvent influe	nce de cet r sur l'accès aux
Nom	de l'ordinateur :		
Wind	dows01		
Mer	mbre d'un) Domaine :		Autres
	druelle.com		
		2	
С) Groupe de travail :		
С	WORKGROUP		

VERIFICATION DE LA CONNECTIVITÉ

Invite de commandes - nslookup

Nicrosoft Windows [version 10.0.19043.928]
(c) Microsoft Corporation. Tous droits réservés.
::\Users\sio>nslookup
Serveur par dÚfaut : druelle_windowsserver.druelle.com
Address: 192.168.120.1
* -

Pour vérifier la connectivité entre le poste et le domaine nous réalisons la commande "nslookup" sur le poste client. Nous pouvons voir ici que le poste est connecté au domaine car celui-ci à "druelle windowsserver.druelle.com" pour serveur par défaut.



QUI PEUT INTÉGRER LE POSTE DANS LE DOMAINE



Les personnes qui peuvent intégrer les postes dans le domain sont les utilisateurs possédant des droits administrateur

DRUELLE\ADMINISTRATEUR

DRUELLE\administrateur Administrateur

RÉCAPITULATIF DES POSTES SUR LE DOMAINE

Utilisateurs et ordinateurs Active Directory		<u></u>	×
Fichier Action Affichage ?	manifest and a state		
🗢 🄶 🔀 📰 🗎 🗐 🖸 🕞 🛛 🖬	浅 📚 🛅 🍸 💆 🍇		
 Utilisateurs et ordinateurs Active Requêtes enregistrées druelle.com Builtin Computers Domain Controllers ForeignSecurityPrincipal: Managed Service Accour Users 	Type Description		
< >		10	

Pour voir le récapitulatif des postes nous allons dans l'outil "utilisateurs et ordinateurs active directory" dans la catégorie "computers". Nous pouvons voir ici que notre poste "windows01" est connecté sur celui-ci



CRÉATION D'UTILISATEURS

(= =	2 📅 🖌 🖬 🗶 🛙	0 🔒 🛛	🗊 🗏 📚 🗊 🔻 🗾 🗞		
Utilisat (Utilisat (Utilisat) (Ut	eurs et ordinateurs Active quêtes enregistrées telle.com Builtin Computers Domain Controllers ForeignSecurityPrincipal: Managed Service Accour Uters Délégation de contr Rechercher	Nom Accès compatible pré-Windows 2000 Accès DCOM service de certificats Administrateurs Administrateurs Hyper-V Duplicateurs Générateurs d'approbations de forêt entrante Groupe d'accès d'autorisation Windows ôle		Type Groupe de séc Groupe de séc pe de séc pe de séc pe de séc pe de séc	Description Un groupe de compatil Les membres de ce gro Les membres du group Les membres de ce gro Prend en charge la répl Les membres de ce gro Groupe intégré utilisé p Les membres du group Des membres de ce gro Les membres peuvent a Les membres pouvent a
	Nouveau > Toutes les tâches > Propriétés	Ordinateur Contact Groupe InetOrgPerson			
< Crée un noi	Alde	Opérateu Opérateu Opérateu Serveurs / Serveurs (Constructions) Serveurs (Constructions)	msDS-KeyCredential msDS-ResourcePropertyList msDS-ShadowPrincipalContainer msImaging-PSPs Alias de file d'attente MSMQ Imprimante Utilisateur	pe de séc pe de séc pe de séc pe de séc pe de séc	Les membres de ce gro Les membres du group Les membres peuvent a Les serveurs de ce grou Les membres de ce grou Les serveurs de ce grou

Créer da	ans: druelle.	com/Users		
Prénom :	jean		Initiales :	
Nom :				
Nom complet :	jean			
Nom d'ouverture d	de session de	l'utilisateur :		
jean		@druelle.c	com	~
Nom d'ouverture d	de session de	l'utilisateur (antérie	eur <mark>à Windows</mark> 20	00) :
DRUELLE		jean		

Pour la création d'utilisateur nous allons dans l'outil "utilisateurs et ordinateurs d'active directory" dans "users" nous créons un nouvel utilisateur et y renseignons ses informations ici "jean" ainsi qu'un mot de passe ici "azerty123%"

Mot de passe :	•••••
Confirmer le mot de passe :	•••••
✓ Le mot de passe n'expire Le compte est désactivé	jamais

CRÉATION D'UTILISATEURS





Vos informations



 \mathbb{R}

FICHIER DISPONIBLE SUR LE RÉSEAU

<u> </u>		×
Fichier Accueil Partage Affichage		~ ?
$\leftarrow \rightarrow \checkmark \uparrow \blacksquare > $ Réseau > 192.168.120.1 > $\checkmark \circlearrowright \land \land$ Rechercher dans : 192.168.120	.1	
Accès rapide netlogon sysvol		
🔜 Bureau 💉 🤏		
🕂 Téléchargements 🖈		
🖹 Documents 🖈		
📰 Images		
Musique		
Vidéos Vidéos		
Ce PC		
💣 Réseau		
2 élément(s)		== 📰



Sur le réseau il y'a 2 dossiers de disponible de base qui sont le "netlogon" et le "sysvol".

QU'EST CE QUE LE "NETLOGON" ET LE "SYSVOL"

Le netlogon est un dossier essentiel au bon fonctionnement du contrôleur de dommaine.

Le netlogon est aussi un protocol qui permet la création de canaux de communication sécurisées ainsi que les opérations d'authentification du domaine

Le sysvol est une collection de dossiers, de points d'analyse du système de fichiers et de paramètres de stratégie de groupe. Dans se dossier Nous pouvons y retrouver une copie des paramètres et des scripts de stratégie de groupe du contrôleurs de domaine





MODIFICATION DE LA SÉCURITÉ DES MOTS DE PASSE

 A Forét : druelle.com A Domaines A druelle.com Defruite C Defruite C 	Étendue Détails Paramètres Domaine : druel	Délégation	
> 📑 Obj > 🚔 Filtr 🛩 > 🛅 Obj > 🏭 Sites # Modélisatic Résultats d	Modifier Appliqué Lien activé Enregistrer le rapport Affichage > Nouvelle fenêtre à partir d'ici Supprimer Renommer Actualiser Aide	du domaine (DRUELLE\Admins du domaine) 2024 14:09:34 2024 14:16:18 0 (SYSVOL) 3 (SYSVOL) 340-016D-11D2-945F-00C04FB984F9)	
	Renommer Actualiser Aide	~	

Pour la modification de la sécurité des mots de passe nous allons dans l'outil "gestion de stratègie de groupe" et modifions le "domain policy".



Une fois cela fait une fenêtre va s'ouvrir qui est l'éditeur des stratégies de groupe une fois dans celui-ci nous allons dans les stratègies de mot de passe et apportons les modifications. ici nous mettons en place une durée de vie de 30 jours ainsi que la durée de l'historique de 24 jours qui est la durée maximal possible. Nous mettons aussi en place la taille du mot de passe minimal à 3 caractères sans compléxité ce qui n'est pas conseillé pour des question de sécurité

CRÉATION ET CONNECTION D'UN NOUVEL UTILISATEUR

Nouvel objet - Utilisateur	× Nouvel objet - Utilisateur	Paramètres	- 🗆 X
Créer dans : druelle.com/Users	Créer dans : druelle.com/Users	C Accueil Rechercher un paramètre	✓ Vos informations
Prénom : sio Initiales : Nom :	Mot de passe : Confirmer le mot de passe : L'utilisateur doit changer le mot de passe à la prochaine ouverture	RE Vos informations E-mail et comptes e de session Q Options de connexion	SIO DRUELLE\sio
Nom d'ouverture de session de l'utilisateur : sio @druelle.com Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) : DRUELLE\	Le mot de passe n'expire jamais	Accès Professionnel ou Scolaire Synchroniser vos paramètres	Créer votre avatar Oméra Rechercher une image
< Précédent Suivant > Anne	uler < Précédent Suivant >	Annuler	Obtenir de l'aide

Afin de vérifié les nouvelles modifications de la sécurité des mots de passe nous allons crée un utilisateur "sio" qui aura pour mot de passe "sio" nous pouvons voir sur les screens si-dessus que l'utilisateur a bien été crée et que nous avons pu nous connecté au poste