Creation d'une infrastructure AD

Emetteur(s) : SAVIARD Matthieu Direction XX Destinataire(s) : CFA INSTA

Date: 03/12/2023

<u>Objet</u> : Mise en place d'un contrôleur de domaine primaire, ainsi qu'un serveur DHCP failover et un DNS secondaire

Sommaire

Introduction	. 1
Préréquis	. 1
Contrôleur de domaine primaire	. 1
Configuration du VLAN	. 2
Configuration du VLAN	. 2
Tapez le titre du chapitre (niveau 3)	. 3
Tapez le titre du chapitre (niveau 1)	. 4
Tapez le titre du chapitre (niveau 2)	. 5
Tapez le titre du chapitre (niveau 3)	. 6

Introduction Préréquis

Un domaine AD va être déployé pour la société sitka qui veut se munir d'un intranet pour la gestion et le déploiement de son infrastructure informatique. Le cahier des charges est le

suivant :

- Un contrôleur de domaine racine, un service DNS, DHCP et AD
- Un DNS auxiliaire de réplication
- Un DHCP auxiliaire en cas de panne du contrôleur de domaine racine

Nous aurons donc besoin des prérequis suivants :

- 3 machines Windows Server 2022
- Un VLAN commun pour les 3 serveurs
- Une machine Windows 10 pour vérifier notre installation

3. Création du contrôleur de domaine

Nous allons donc lancer une machine Windows Server 2022 et lui donner la configuration suivante :

- VLAN : sitka.local
- IP:172.20.0.1/24
- Firewall : désactivé

Et ensuite nous allons installer les services AD, DNS et DHCP

a. Configuration du VLAN

WINSERV-01	
Power on this virtual ma	achine
🔽 Edit virtual machine set	tings
Devices	
📟 Memory	2 GB
Processors	2
Hard Disk (NVMe)	60 GB
💿 CD/DVD (SATA)	Auto detect
💾 Floppy	Auto detect
Potwork Adapter	NAT
🚭 USB Controller	Present
් Sound Card	Auto detect
🖶 Printer	Present
Display	Auto detect
 Description 	
Type here to enter a descrip machine.	ption of this virtual

On va aller dans \rightarrow Edit virtual machine settings

lardware Options	
Device	Summary
📟 Memory	2 GB
Processors	2
Hard Disk (NVMe)	60 GB
💿 CD/DVD (SATA)	Auto detect
Floppy	Auto detect
Network Adapter	NAT
🚭 USB Controller	Present
🕼 Sound Card	Auto detect
🖶 Printer	Present
Display	Auto detect

Ensuite cliquer sur Network adaptater

Hardware Options		
Device Memory Processors Hard Disk (NVMe) CD/DVD (SATA) Floppy Network Adapter USB Controller Sound Card Printer Display	Summary 2 GB 2 60 GB Auto detect Auto detect Present Auto detect Present Auto detect	Device status Connected Connect at power on Network connection Bridged: Connected directly to the physical network Replicate physical network connection state NAT: Used to share the host's IP address Host-only: A private network shared with the host Custom: Specific virtual network VMnet0 LAN segment: LAN Segments

A gauche, on va changer le NAT en LAN segment, et choisir la vlan « sitka.local »

LAN segment:			
sitka.local			\sim
		LAN Segments	Advanced
Ensuite,cliquer sur	OK en ba	s à droite	

b. Configuration de la machine

On va commencer par changer le nom de la machine :

Tablaau da bard	PROPRIÉTÉS			
Serveur local Tous les serveurs Services de fichiers et d	Nom de l'ordinateur Groupe de travail	WIN-NU6LL1L8K79 WORKGROUP	Dernières mises à jour installées Windows Update Dernière recherche de mises à jour :	Jamais Télécharger les mises à jour uniquement à l'aide de Windows Update Jamais
	Pare-feu Microsoft Defender Gestion à distance Bureau à distance Association de cartes réseau Ethernet0	Public : Actif Activé Désactivé Desactivé Adresse IPv4 attribuée par DHCP, Compatible IPv6	Antivirus Microsoft Defender Commentaires et diagnostics Configuration de sécurité renforcée d'Internet Explorer Fuseau horaire ID de produit (Product ID)	Protection en temps réel : activée Paramètres Actif (UTC+01:00) Bruxelles, Copenhague, Madrid, Paris Non activé
	Version du système d'exploitation Informations sur le matériel	Microsoft Windows Server 2022 Datacenter VMware, Inc. VMware20,1	Processeurs Mémoire installée (RAM) Espace disque total	Intel(R) Core(TM) i5-8365U CPU @ 1.60GHz, Intel(R) Core(TM) i5-8365U C 2 Go 59,68 Go

Dans le gestionnaire de serveur, cliquer sur « Nom de l'ordinateur »

Groupe de travair .	Worndhoor	
Pour renommer cet ordinateur ou changer de domaine		Modifier
ou de groupe de travail, e	alquez sur mouner.	

Sur la fenêtre qui apparait, cliquer sur modifier

Nom de l'ordinateur :		
winserv01		
Nom complet de l'ordinateur : winserv01		
		Autres
Membre d'un		
O Domaine :		
Groupe de travail :		
WORKGROUP		
	OK	Annuler

On va appeler notre contrôleur racine winserv01, faire OK

Le PC va demander de redémarrer, mais cliquer sur « redémarrer ultérieurement », on va d'abord finir la configuration du PC

On va ensuite désactiver le pare feu :

Dans le gestionnaire de serveurs, cliquer sur « Public : actif »

Pare-feu Microsoft Defender Public : Actif

Réseau avec domaine

Le pare-feu est activé.

😢 Réseau privé

Le pare-feu est activé.

S Réseau public (actif)

Le pare-feu est activé.

Les pare feu est activé partout, nous allons donc le désactiver partout

Réseaux avec domaine actifs

Non connecté

Pare-feu Microsoft Defender

Aide à protéger votre appareil sur un réseau avec domaine.



Réseaux privés actifs

Non connecté

Pare-feu Microsoft Defender

Aide à protéger votre appareil sur un réseau privé.



Désactivé

Réseaux publics actifs

🏗 Réseau

Pare-feu Microsoft Defender

Aide à protéger votre appareil sur un réseau public.



Désactivé

Nous avons donc désactivé le pare feu, cela sera très utile pour nos machines et les pinger entre elles.

Nous allons ensuite configurer l'IP du serveur :

Aller sur la carte Ethernet 0 et cliquer sur « Addresse IPv4 attribuée par DHCP ... »

Ethernet0 Adresse IPv4 attribuée par DHCP, Compatible IPv6 I

Faire clique droit → propriétés



Puis décocher l'ipv6 « Protocole Internet version 6 »



Et ensuite cliquer sur « Protocole Internet version 4 » et faire « propriétés » π

onnexion en utilisant :	Propriétés de : Protocole Internet version 4 (TCP/IPv4) X
Intel(R) 82574L Gigabit Network Connection	Général Configuration alternative
Configurer ette connexion utilise les éléments suivants : Partage de fichiers et imprimantes Réseaux Microsoft Planificateur de paquets QoS Protocole Internet version 4 (TCP/IPv4) Protocole de multiplexage de carte réseau Microsoft Pilote de protocole LLDP Microsoft Protocole Internet version 6 (TCP/IPv6) Répondeur de découverte de la topologie de la couche de liaison Installer Désinstaller Propriétés Description Protocole TCP/IP (Transmission Control Protocol/Internet Protocol). Protocole de réseau étendu par défaut permettant la communication entre différents réseaux interconnectés.	Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.
OK Annuler	Valider les paramètres en quittant Avancé
ent 1 élément sélectionné	OK Annuler
WIN NUSU 10/20 11710 France Mailestelles	

Cela va ouvrir la page de droite, nous allons donc configurer statiquement notre configuration de serveur

Notre réseau étant l'addresse 172.20.0/24 nous allons donner au serveur l'addresse 172.20.0.1/24

Il sera sa propre passerelle, et aura un DNS auxiliaire 172.20.0.2/24 et une passerelle par défaut de 172.20.0.254/24

Obtenir une adresse IP automatiquement

Otiliser l'adresse IP suivante :	
Adresse IP :	172.20.0.1
Masque de sous-réseau :	255.255.255.0
Passerelle par défaut :	172.20.0.254
Obtenir les adresses des serveur	s DNS automatiquement
Serveur DNS préféré :	172.20.0.1
Serveur DNS auxiliaire :	172.20.0.2
Valider les paramètres en quittar	nt Avancé
	OK Annuler

Ce qui donne ca, ensuite faire OK et redémarrer la machine

La machine est prête, nous allons ensuite configurer le service AD

3) Configuration et installation du service AD

Nous allons donc installer les services de notre machine. Pour aller plus vite, nous allons directement installer les services AD,DNS et DHCP

Cliquer sur gérer \rightarrow « Ajouter des rôles et fonctionnalités »

- 🔊 I	<u> </u>	Gérer	Outils	Afficher	Aide
		Ajouter des ré	les et fonc	tionnalités	
		Supprimer de	s rôles et fo	onctionnalit	és
		Ajouter des se	erveurs		
		Créer un grou	pe de serve	eurs	
ses à jour uniqu		Propriétés du	Gestionnai	re de serve	ur

Cette page va ensuite s'ouvrir

📥 Assistant Ajout de rôles et de fonctionnalités

– 🗆 🗙

Avant de commencer

SERVEUR DE DESTINATION winserv01

Avant de commencer Type d'installation	Cet Assistant permet d'installer des rôles, des services de rôle ou des fonctionnalités. Vous devez déterminer les rôles, services de rôle ou fonctionnalités à installer en fonction des besoins informatiques de votre organisation, tels que le partage de documents ou l'béhergement d'un site Web.
Sélection du serveur	de votre organisation, tels que le partage de documents ou mebergement d'un site web.
Rôles de serveurs	Pour supprimer des rôles, des services de rôle ou des fonctionnalités : Démarrer l'Assistant de Suppression de rôles et de fonctionnalités
Fonctionnalités	Avant de continuer, vérifiez que les travaux suivants ont été effectués :
Confirmation	• Le compte d'administrateur persède un mot de passe fort
Résultats	 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 satisfaite, fermez l'Assistant, exécutez les étapes, puis relancez l'Assistant.
	Cliquez sur Suivant pour continuer.
	Ignorer cette page par défaut
	< Précédent Suivant > Installer Annuler

Cliquer sur Suivant \rightarrow Suivant \rightarrow Suivant

Ensuite, sélectionner AD DS, DHCP et DNS

SERVEUR DE DESTINATION winserv01

Х

Sélectionner des rôles de serveurs



Faire Suivant \rightarrow Suivant \rightarrow Suivant \rightarrow Suivant \rightarrow Suivant \rightarrow Installer

Une fois installé faire → fermer

Nous avons donc tous les services installés, nous allons ensuite créer un utilisateur Administrateur avec un mot de passe sur notre machine, pour qu'en suite cela se synchronise sur notre AD

Aller « dans gestion de l'ordinateur »



Aller dans « Utilisateurs et Groupes » puis « Utilisateurs » puis faire clique droit et faire « Définir le mot de passe »

ł	Gestion de l'ordinateur (local)	Nom	Nom complet	Descripti	on
	 V Outils système V Planificateur de tâches 	Administra	Définir le mot de passe	e	d'utilisateur utilisateur q
i	> 11 Observateur d'événeme 2 Dossiers partagés	🛃 Invité	Toutes les tâches	> e	d'utilisateur
í	Vilisateurs et groupes l	👺 msaviard	Supprimer	e	d'utilisateur
1	Groupes		Renommer		
j	> 🔊 Performance		Propriétés		
	 Gestionnaire de périphé Stockage 		Aide		
	> 🐌 Sauvegarde Windows S				
	Gestion des disques Services et applications				

Ensuite, cliquer sur « continuer »

Définir	le mot de passe pour Administrateur	×			
<u>^</u>	La réinitialisation de ce mot de passe peut provoquer des pertes de données irréversible pour ce compte d'utilisateur. Pour des raisons de sécurité, Windows protège certaines informations en interdisant leur accès si le mot de passe du compte d'utilisateur est réinitialisé.	s			
	Cette perte de données se produira lorsque l'utilisateur fermera sa session.				
	Cette commande ne doit être utilisée que dans le cas où un utilisateur a oublié son mot de passe ou ne dispose pas de disque de réinitialisation du mot de passe. Si cet utilisateur a créé un disque de réinitialisation du mot de passe, il est recommandé d'utiliser celui-ci pour réinitialiser le mot de passe.				
	Si l'utilisateur connaît le mot de passe et veut le modifier, il doit ouvrir une session, puis appuyer sur CTRL+ALT+SUPPR et cliquer sur Modifier le mot de passe.				
	Pour obtenir plus d'informations, cliquez sur Aide.				
	Continuer Annuler Aide				

On va ensuite mettre @Azerty123

Une fois le mot de passe changé, on va supprimer la session actuelle, mais d'abord nous allons nous déconnecter de notre session et se connecter sur la session « Administrateur »

Cliquer sur « Se déconnecter »



Puis se connecter sur la nouvelle session :



Une fois sur la session, sur le gestionnaire de serveurs, nous allons donc pouvoir commencer à configurer l'AD

En haut à droite, il y aura une icone jaune, cliquer dessus

Configuration post-déploiement

Configuration requise pour : Services AD DS à WINSERV01

Promouvoir ce serveur en contrôleur de domaine

Détails de la tâche

Faire « promouvoir ce serveur en contrôleur de domaine »

La Assistant Configuration des services de domaine Active Directory						\times
Configuration de déploie Options du contrôleur de Options supplémentaires Chemins d'accès Examiner les options Vérification de la configur Installation Résultats	piement onner l'opération de déploiement uter un contrôleur de domaine à uter un nouveau domaine à une f uter une nouvelle forêt ez les informations de domaine p e domaine racine :	un domaine existant forêt existante our cette opération sitka.loca		SER	RVEUR CI	IBLE rv01
	< Pré	cédent Suivant >	Installe	r	Annule	r

renseigner « sitka.local » et faire suivant

La Assistant Configuration des servi	ices de domaine Active Directory		—		\times
Assistant Configuration des servi Options du contrô Configuration de déploie Options du contrôleur de Options DNS Options supplémentaires Chemins d'accès Examiner les options Vérification de la configur	ices de domaine Active Directory Dieur de domaine Sélectionner le niveau fonctionnel de la r Niveau fonctionnel de la forêt : Niveau fonctionnel du domaine : Spécifier les fonctionnalités de contrôleu Serveur DNS (Domain Name System)]	SERVEUR (winse	X IIBLE 2rv01	
Examiner les options Vérification de la configur Installation	 Serveur DNS (Domain Name System) Catalogue global (GC) Contrôleur de domaine en lecture se 	ule (RODC)			
Résultats	Taper le mot de passe du mode de resta Mot <u>d</u> e passe :	uration des services d'annuaire (DSRM)		
	<u>C</u> onfirmer le mot de passe :	•••••]		
	En savoir plus sur les options pour le cor	ntrôleur de domaine			
	< <u>P</u> ré	cédent Sui <u>v</u> ant > Instal	ler	Annul	er

Renseigner le mot de passe des services d'annuaires (mettre ici @Azerty123)

Faire Suivant

📥 Assistant Configuration des serv	ices de domaine Active Directory	- 🗆 ×
Options DNS		SERVEUR CIBLE winserv01
Il est impossible de créer u	ne délégation pour ce serveur DNS car la zone parente faisant autori	té est introu Afficher plus 🛛 🗙
Configuration de déploie Options du contrôleur de Options DNS	Spécifier les options de délégation DNS Créer une délégation DNS	
Options supplémentaires Chemins d'accès		
Examiner les options Vérification de la configur Installation		
	En savoir plus sur la délégation DNS	
	< Précédent Suivant >	Installer Annuler

Faire « Suivant »

La Assistant Configuration des servi	ces de domaine Active Directory		_		×
Options suppléme Configuration de déploie Options du contrôleur de Options DNS	Vérifiez le nom NetBIOS attribué au doma Le nom de domaine NetBIOS :	iine et modifiez-le si nécess SITKA	aire.	SERVEL W	JR CIBLE /inserv01
Options supplémentaires Chemins d'accès Examiner les options Vérification de la configur Installation Résultats					
	En savoir plus sur d'autres options				
	< Préc	édent Suivant >	Installer	Ar	nuler

faire Suivant \rightarrow Suivant \rightarrow Installer jusqu'ici

Vérification de la configuration requise

SERVEUR CIBLE winserv01

Toutes les vérifications de la configuration requise ont donné satisfaction. Cliquez sur Installer pour comme Afficher plus						
Configuration de déploieLa configuration requise doit être validée avant que les services de domaine Active Directory soient installés sur cet ordinateur						
Options DNS	Réexécuter la vérification de la configuration requise					
Options supplémentaires						
Chemins d'accès Ovir les résultats						
Examiner les options						
Vérification de la configur défaut nomme « Autoriser les algorithmes de chiffrement compatibles avec Windows NT 4.0 ». Ce paramètre empêche l'utilisation d'algorithmes de chiffrement faibles lors						
Installation de l'établissement de sessions sur canal sécurisé.						
Résultats	ésultats Pour plus d'informations sur ce paramètre, voir l'article 942564 de la Base de connaissances (http://go.microsoft.com/fwlink/?Linkld=104751).					
Il est impossible de créer une délégation pour ce serveur DNS car la zone parente faisant autorité est introuvable ou elle n'exécute pas le serveur DNS Windows. Si vo procédez à l'intégration avec une infrastructure DNS existante, vous devez						
Si vous cliquez sur Installer, le serveur redémarre automatiquement à l'issue de l'opération promotion.						
	En savoir plus sur les conditions préalables					
	< Précédent Suivant > Installer Annuler					

Puis faire Installer

Une fois l'installation finie, le PC va redémarrer. Nous avons donc ensuite réalisé l'implantation du contrôleur de domaine et la création de notre domaine.

Voici le script que génère le windows serveur :

Import-Module ADDSDeployment

Install-ADDSForest`

- -CreateDnsDelegation:\$false`
- -DatabasePath "C:\Windows\NTDS"`
- -DomainMode "WinThreshold" `
- -DomainName "sitka.local" `
- -DomainNetbiosName "SITKA" `
- -ForestMode "WinThreshold" `
- -InstallDns:\$true`

- -LogPath "C:\Windows\NTDS"`
- -NoRebootOnCompletion:\$false`
- -SysvolPath "C:\Windows\SYSVOL"`
- -Force:\$true

Nous allons donc pouvoir configurer notre service DHCP :

Avec notre service DHCP installés précédemment, on a la même icone que pour l'AD

Cliquer sur \rightarrow « Termination la configuration DHCP »



Faire suivant

Autorisation	
Description	Spécifiez les informations d'identification à utiliser pour autoriser ce serveur DHCP dans les services
Autorisation	AD DS.
Résumé	 Utiliser les informations d'identification de l'utilisateur suivant Nom d'utilisateur : SITKA\Administrateur Utiliser d'autres informations d'identification Nom d'utilisateur : Spécifier Ignorer l'autorisation AD
	< Précédent Suivant > Valider Annuler

Valider, cela utilisera les informations d'identification de notre utilisateur puis faire « Fermer »

Ensuite, en haut à droite, cliquer sur « outils » et « dhcp »



Nous avons donc enfin notre service DHCP qui est prêt à être configuré



Nous avons donc un service IPv4 et IPv6

Nous allons donc créer une étendue, ce sera l'étendue des IP qui seront distribuées à notre réseau.

Voici le tableau de notre réseau avant toute configuration :

raile clique di oit sui 1847 Nouvelle eteridu	Faire clic	que droit s	sur IPv4→	Nouvelle	étendue
---	------------	-------------	-----------	----------	---------

Nouvelle étendue...

Faire « Suivant » et nommer ainsi :

Assistant Nouvelle étendue

Nom de l'étendue

Vous devez fournir un nom pour identifier l'étendue. Vous avez aussi la possibilité de fournir une description.

Tapez un nom et une description pour cette étendue. Ces informations vous permettre d'identifier rapidement la manière dont cette étendue est utilisée dans le réseau.

Nom :

Description :

VLAN 10

Administration

Faire suivant \rightarrow

Assistant Nouvelle étendue	
Plage d'adresses IP Vous définissez la plage d'adresses en identifiant un jeu d'adresses IP consécutives.	
Paramètres de configuration pour serveur DHCP Entrez la plage d'adresses que l'étendue peut distribuer. Adresse IP de 172 . 20 . 0 . 1 début : Adresse IP de fin : 172 . 20 . 0 . 254 Paramètres de configuration qui se propagent au client DHCP.	1
Longueur : 24 Masque de 255 . 255 . 0 sous-réseau :	
< Précédent Suivant > Annuler	

Faire « Suivant »

On va ensuite rajouter des addresses IP à exclure. Nous allons donc exclure la plage 172.20.0.1-172.20.0.20 car ce seront les adresses de serveur et elles seront en statiques. On va également exclure l'adresse du routeur 172.20.0.254.

Ajout d'exclusions et de retard

Les exclusions sont des adresses ou une plage d'adresses qui ne sont pas distribuées par le serveur. Un retard est la durée pendant laquelle le serveur retardera la transmission d'un message DHCPOFFER.



Aulesse IP de debut .	Adresse IP de fin :		
		Ajouter	
Plage d'adresses exclue :			
172.20.0.1 sur 172.20.0.1	20	Supprimer	
Adresse 172.20.0.254			
		Retard du sous-rése	eau en
		millisecondes :	
		0 -	
)			

Ensuite faire « Suivant »

On va mettre le bail à 4 jours

Durée du bail

La durée du bail spécifie la durée pendant laquelle un client peut utiliser une adresse IP de cette étendue.



La durée du bail doit théoriquement être égale au temps moyen durant lequel l'ordinateur est connecté au même réseau physique. Pour les réseaux mobiles constitués essentiellement par des ordinateurs portables ou des clients d'accès à distance, des durées de bail plus courtes peuvent être utiles.

De la même manière, pour les réseaux stables qui sont constitués principalement d'ordinateurs de bureau ayant des emplacements fixes, des durées de bail plus longues sont plus appropriées.

Définissez la durée des baux d'étendue lorsqu'ils sont distribués par ce serveur.

Limitée à :

Jours : Heures :	Minutes :			
		< Précédent	Suivant >	Annuler

Faire Suivant \rightarrow Suivant

Puis mettre le routeur qui sera configuré sur les machines :

Adresse IP :	
	Ajouter
172.20.0.254	Supprimer
	Monter
	Descendre

Puis faire Suivant → Suivant → Teminé

Ensuite, le service DHCP activé

5) Service DNS

Nous allons donc configurer le service DNS, tout d'abord aller dans Gérer → DNS

Analyseur de performances
Centre d'administration Active Directory
Configuration du système
Défragmenter et optimiser les lecteurs
DHCP
Diagnostic de mémoire Windows
DNS
Domaines et approbations Active Directory
Éditeur du Registre
Gestion de l'ordinateur
Gestion des stratégies de groupe

Comme on peut le voir, en créant notre domaine, cela a crée une zone de recherche directe automatiquement. Nous allons donc créer une zone de recherche inversée (celle qui traduit les noms en IP)

Faire clic droit sur « zone de recherche inversée » et cliquer sur « nouvelle zone »

Assistant Nouvelle zone



Cette fenêtre va s'ouvrir, puis cliquer sur « suivant », puis cliquer sur « zone principale » puis faire « suivant »

X

Assistant Nouvelle zone

Type de zone

Le serveur DNS prend en charge différents types de zones et de stockages.



Х

Sélectionnez le type de zone que vous voulez créer :

Zone principale

Crée une copie d'une zone qui peut être mise à jour directement sur ce serveur.

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.

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)

nuler	A	Suivant >	< Précédent

Puis laisser sur le choix initialement coché puis faire « suivant »

Assistant Nouvelle zone

Étendue de la zone de réplication de Activ Vous pouvez sélectionner la façon dont les d sur votre réseau.	e Directory onnées DNS do	ivent être répliquée	es internet
Choisissez la façon dont les données de la zo	one doivent être	répliquées :	
 Vers tous les serveurs DNS exécutés sur d sitka.local 	es contrôleurs c	le domaine dans c	ette forêt :
Vers tous les serveurs DNS exécutés sur d sitka.local	es contrôleurs c	le domaine dans c	e domaine :
○ Vers tous les contrôleurs de ce domaine (or la contrôleurs)	compatibilité ave	c Windows 2000)	: sitka.local
 Vers tous les contrôleurs de domaine spéc d'annuaire : 	ifiés dans l'éten	due de cette partiti	on
	< Précédent	Suivant >	Annuler

-

Faire « suivant	»	car	on	veut	en	IPv4
-----------------	---	-----	----	------	----	------

Nom de la zone de recherche inversée

Une zone de recherche inversée traduit les adresses IP en noms DNS.



ou les adresses IPv6.		
Sone de recherche inversée IPv4		
O Zone de recherche inversée IPv6		

On va ensuite déclarer l'ID de réseau, sachant que notre réseau est de 172.20.0.0 On va donc mettre 172.20.0.X , et ensuite faire « suivant » Assistant Nouvelle zone

Nom de la zone de recherche inversée Une zone de recherche inversée traduit	e les adresses IP en noms DNS.
 Pour identifier la zone de recherche inverse ID réseau : 172 .20 .0 L'ID réseau est la partie des adresse dans son ordre normal (non inversé Si vous utilisez un zéro dans l'ID réseau sone de recherche inversé 0.10.in-addr.arpa. 	ersée, entrez l'ID réseau ou le nom de la zone. es IP qui appartient à cette zone. Entrez l'ID réseau). eau, il va apparaître dans le nom de la zone. Par e 10.in-addr.arpa, l'ID réseau 10.0 crée la zone
0.20.172.in-addr.arpa	e :

Ensuite, cocher la seconde case, on veut ca pour que les enregistrements DNS apparaissent bien dans les enregistrements puis faire « suivant »

< Précédent

Suivant >

Annuler

 \times

ribbibitunit ribbibitunit zone

Mise à Vo no	niveau dynamique lus pouvez spécifier que cette zone DI n sécurisées ou non dynamiques.	NS accepte les mises	à jour sécurisées	S,
Les mise manière modifica	es à jour dynamiques permettent au dynamique leurs enregistrements de ation a lieu.	client DNS d'enregistr e ressources avec un	er et de mettre à serveur DNS dès	jour de s qu'une
Sélectio	nnez le type de mises à jour dynamiq	ues que vous souhai	tez autoriser :	
N'auto Active	oriser que les mises à jour dynamique e Directory)	es sécurisées (recom	mandé pour	
Cett	e option n'est disponible que pour les	zones intégrées à Ac	tive Directory.	
Autor Les n'im	iser à la fois les mises à jours dynami mises à jour dynamiques d'enregistre porte quel client.	ques sécurisées et ne ement de ressources	on sécurisées sont acceptées à	partir de
	Cette option peut mettre en danger risquent d'être acceptées à partir d	r la sécurité de vos de l'une source non app	onnées car les mi rouvée.	ses à jour
 Ne pa Les r cette 	s autoriser les mises à jour dynamiqu mises à jour dynamiques des enregis 2 zone. Vous devez mettre à jour ces	ies trements de ressourc enregistrements mar	ces ne sont pas a nuellement.	cceptées par
		< Précédent	Suivant >	Annuler
		< Precedent	Suivant >	Annule

Puis faire « terminer »

Une fois notre DNS configuré, nous allons donc autoriser les transferts de zone sur la zone de recherche primaire, et ensuite sur la zone de recherche inversée

Cliquer sur zone de recherche direct \rightarrow sitka.local \rightarrow clique droit (propriétés)

Ensuite sur la fenêtre qui apparait, cliquer sur Transfert de zone et cocher « Autoriser les transferts de zone » puis « vers n'importe quel serveur »

X

Pro	priétés	de :	sitka.	local
	0110100		Di ci com	0.001

transfert de zone t la demande.	envoie une copie de la zone aux serveu	rs qui en
Autoriser les transf	ferts de zone :	
Vers n'importe	quel serveur	
O Uniquement ve	rs les serveurs listes dans l'onglet Serveu	irs de noms
	rs les serveurs suivants	
A 1		complet du
Adresse IP	Nom de domaine	complet du
Adresse IP	Nom de domaine	complet du
Adresse IP	Nom de domaine	complet du
Adresse IP	Nom de domaine	
Adresse IP	Nom de domaine	complet du
Adresse IP	Nom de domaine	complet du
Adresse IP	Nom de domaine	Modifier
Adresse IP	Nom de domaine	Modifier
Pour spécifier de	s serveurs secondaires à notifier lors	Modifier

?

X

Faire « appliquer » et ensuite appuyer sur « OK »

Ensuite réitérer la même chose, sur le dossier des recherches inversées

Notre contrôleur de domaine est donc prêt, nous allons donc pouvoir configurer notre deuxième VM, le DNS secondaire

5) DNS Secondaire

Pour faire le DNS secondaire, nous allons donc configurer une nouvelle machine avec les configurations suivantes :

IP : 172.20.0.2 VLAN : sitka.local Firewall : désactivé

On teste le ping :



Tout est ok, on va donc installer un service DNS

Une fois installé, nous arrivons ici:



Nous allons donc créer une zone de recherche directes secondaire, faire clique droit

➔ Nouvelle zone

Assistant Nouvelle zone		\times	
	Bienvenue !		
	Cet Assistant vous permet de créer une nouvelle zone pour le serveur DNS.		
	Une zone traduit les noms DNS en données relatives, telles que des adresses IP ou des services réseau.		
	Cliquez sur Suivant pour continuer.		
	< Précédent Suivant > Annuler		

Faire « suivant », « zone secondaire » puis « suivant »

○ Zone principale	
Crée une copie d'une zone qu	i peut être mise à jour directement sur ce serveur.
Sone secondaire	
Crée une copie de la zone qui la charge de travail des server pannes. O Zone de stub	existe sur un autre serveur. Cette option aide à équilibre urs principaux et autorise la gestion de la tolérance de
Crée une copie d'une zone co (NS), Source de nom (SOA), e Un serveur contenant une zor	ntenant uniquement des enregistrements Nom de serve et éventuellement des enregistrements « glue Host (A) ». ne de stub ne fait pas autorité pour cette zone.
Crée une copie d'une zone co (NS), Source de nom (SOA), e Un serveur contenant une zon Enregistrer la zone dans Active contrôleur de domaine accessit	ntenant uniquement des enregistrements Nom de serve et éventuellement des enregistrements « glue Host (A) », ne de stub ne fait pas autorité pour cette zone. Directory (disponible uniquement si le serveur DNS est u ple en écriture)

Nous allons ensuite appeler cette zone « sitka.local » et ensuite renseigner 172.20.0.1, le serveur réponds donc

Nom de la zone

Quel est le nom de la nouvelle zone ?



Х

	Le nom de la autorité. Il pe d'une partie zone n'est pa	a zone spécifie la eut s'agir du nor du nom de dom as le nom du sei	a partie de l'esp n de domaine c aine (par exem rveur DNS.	ace de noms DNS de votre société (p ple, nouvelle_zon	pour laquelle par exemple, m e.microsoft.co	ce serveur fait nicrosoft.com) ou m). Le nom de
	Nom de la zo	one :				
	sitka.local					
				< Précédent	Suivant >	Annuler
Assista	nt Nouvelle zone				×	
Serv	eurs DNS maîtres la zone secondaire es	st copiée à partir d'un c	ou de plusieurs serveu	irs DNS.		
0	Spécifiez les serveurs cont contactés dans l'o	DNS à partir desquels v ordre indiqué.	vous voulez copier la z	zone. Les serveurs		
5	erveurs maîtres :					
	Adresse IP	Nom de domaine	Validé	Supprimer		
	Cliquez ici pour ajo	winserv01.sitka.lo	OK	Monter		
				Descendre		
			< Précédent Sui	ivant > Annuler		

Ensuite, faire « Suivant » et faire « Terminé »

Nous avons donc crée la première zone, nous allons donc créer la zone secondaire inversée



Aller sur « zone de recherche inversée » puis faire « nouvelle zone »

Ensuite faire « suivant » et cocher « zone secondaire »

Type de zone

Le serveur DNS prend en charge différents types de zones et de stockages.



Sélectionnez le type de zone que vous voulez cré	éer :		
 Zone principale Crée une copie d'une zone qui peut être mise 	e à jour dire	ctement sur ce se	rveur.
 Zone secondaire Crée une copie de la zone qui existe sur un a la charge de travail des serveurs principaux e pannes. Zone de stub Crée une copie d'une zone contenant unique (NS), Source de nom (SOA), et éventuelleme 	eutre serveur et autorise la ement des er ent des enreg	r. Cette option aid gestion de la tole pregistrements No gistrements « glue	e à équilibrer érance de om de serveur e Host (A) ».
 Enregistrer la zone dans Active Directory (disp contrôleur de domaine accessible en écriture) 	onible unique	ement si le servei	ur DNS est un
<	Précédent	Suivant >	Annuler

Faire « suivant » et « zone de recherche inversée IPv4 »

 \times

Nom de la zone de recherche inversée

Une zone de recherche inversée traduit les adresses IP en noms DNS.

Choisissez si vous souhaitez créer une zone de recherche inversée pour les adresses IPv4 ou les adresses IPv6.

Zone de recherche inversée IPv4

○ Zone de recherche inversée IPv6

		< Précédent	Suivant >		Annuler
--	--	-------------	-----------	--	---------



Faire « suivant » et renseigner l'ID réseau 172.20.0.X

Assistant Nouvelle zone

Nom de la zone de recherche inversée Une zone de recherche inversée traduit les a	dresses IP en noms DNS.
 Pour identifier la zone de recherche inversée ID réseau : 172 .20 .0 L'ID réseau est la partie des adresses IP dans son ordre normal (non inversé). Si vous utilisez un zéro dans l'ID réseau, i exemple, l'ID réseau 10 crée la zone 10.i 	, entrez l'ID réseau ou le nom de la zone. qui appartient à cette zone. Entrez l'ID réseau l va apparaître dans le nom de la zone. Par n-addr.arpa, l'ID réseau 10.0 crée la zone
0.10.in-addr.arpa. ○ Nom de la zone de recherche inversée :	
0.20.172.in-addr.arpa	
	< Précédent Suivant > Annuler

Faire suivant et renseigner le serveur maitre 172.20.0.1

Cliquez ici pour entrer une date.

 \times

Assistant Nouvelle zone				\times
Serveurs DNS maîtres La zone secondaire es	st copiée à partir d'un o	u de plusieurs serveurs	DNS.	
Spécifiez les serveurs sont contactés dans l'o	DNS à partir desquels v ordre indiqué.	ous voulez copier la zo	ne. Les serveurs	
Serveurs maîtres :			_	
Adresse IP	Nom de domaine	Validé	Supprimer	
<cliquez ajo<="" ici="" pour="" th=""><th>uter une adresse IP ou</th><th>un nom DNS></th><th></th><th></th></cliquez>	uter une adresse IP ou	un nom DNS>		
☑ 172.20.0.1	winserv01.sitka.lo	OK	Monter	
			Descendre	
	[< Précédent Suiva	ant > Ann	uler

Faire suivant et terminé

Le serveur DNS auxiliaire est donc bien setup, et l'on peut vérifier en créant un enregistrement de service sur le serveur maitre et vérifier qu'il se réplique bien sur le deuxième DNS

🛔 Gestionnaire DNS			- 0	×
Fichier Action Affichage ?				
 DNS WINSERV01 Zones de recherche direc insdcs.sitka.local isitka.local Zones de recherche inver 0.20.172.in-addr.arpa Points d'approbation Redirecteurs conditionne 	Nom _msdcs _sites _tcp _udp DomainDnsZones ForestDnsZones (identique au dossier parent) (identique au dossier parent)	Type Source de nom (SOA) Serveur de noms (NS) Hôte (A) Hôte (A) Hôte (A)	Données [23], winserv01.sitka.local., h winserv01.sitka.local. 172.20.0.1 172.20.0.1 172.20.0.2	Horodateu statique statique 28/10/202: statique 28/10/202:

On voit bien que le DNS 02 est bien apparu dans les enregistrements de service du DNS 01

(autoriser les mises à jour non sécurisées et dynamiques)

6) DHCP failover

Pour le basculement, on va faire une troisième machine

IP : 172.20.0.3 VLAN : sitka.local Firewall : désactivé

Nous allons également installer le service DHCP sur la machine, mais ne pas le configurer. Le DHCP est donc installé sur la machine

Nous allons donc aller sur le contrôleur de domaine, racine, dans le DHCP aux étendues



Sur étendues, faire clic droit → configurer un basculement

ensuite, cliquer sur serveur partenaire \rightarrow ajouter un serveur et renseigner l'ip 172.20.0.3

specifier le serveur	partenaire à utiliser pour le t	basculement	C.
Indiquez le nom d'hô configuration du basc	te ou l'adresse IP du serveur DH culement.	CP partenaire à ι	tiliser pour la
Vous pouvez effectue basculement existant liste des serveurs DH	er votre sélection parmi la liste de , ou vous pouvez rechercher et s CP autorisés.	s serveurs avec u électionner le ser	ne configuration de veur approprié dans la
Vous pouvez égalem	ent taper <mark>l</mark> e nom d'hôte ou l'adre	sse IP du serveu	partenaire.
Serveur partenaire :	winserv03.sitka.local	•	Ajouter un serveur
cas echeantj.			

Faire « suivant » et remplir les informations suivantes

Configurer un basculement

Créer une relation de basculement

	~		
R	2	5	n.
L		N	
		÷	

Créer une relation de basculement avec le	artenaire winserv03.sitka.local
Nom de la relation :	WINSERV01-WINSERV03-FAILOVER
Délai de transition maximal du client (MCLT) :	1 heures 0 minutes
Mode :	Serveur de secours
Configuration du serveur de secours Rôle du serveur partenaire :	Veille
Adresses réservées pour le serveur de secours :	5 * %
Intervalle de basculement d'état :	60 minutes
Activer l'authentification du message	
Secret partagé :	*****

Faire suivant et terminer

Progression de la co	onfiguration du basculement.	
e journal ci-dessou lu basculement, air	is montre la progression des d nsi que les erreurs rencontrées	iverses tâches de configu
	•	
Aioutor dos átonde	use sur la convour partonairo	Páussita
Désactiver des été	endues sur le serveur partenaire	aire Réussite
200000000000000000000000000000000000000	ondado dan lo derroar partone	
Création de la con	nfig. du basculement sur le se	rveur partenaireRéu
Création de la con Création de la con	nfig. du basculement sur le se nfiguration du basculement su	rveur partenaireRéu ir le serveur hôteRéu
Création de la con Création de la con Activer des étendu	nfig. du basculement sur le se nfiguration du basculement su ues sur le serveur partenaire	rveur partenaireRéu ir le serveur hôteRéu Réussite
Création de la con Création de la con Activer des étendu Réussite de la cor	nfig. du basculement sur le se nfiguration du basculement su ues sur le serveur partenaire nfiguration du basculement.	rveur partenaireRéu ir le serveur hôteRéu Réussite
Création de la con Création de la con Activer des étendu Réussite de la cor	nfig. du basculement sur le se nfiguration du basculement su ues sur le serveur partenaire nfiguration du basculement.	rveur partenaireRéu Ir le serveur hôteRéu Réussite
Création de la con Création de la con Activer des étendu Réussite de la cor	nfig. du basculement sur le se nfiguration du basculement su ues sur le serveur partenaire nfiguration du basculement.	rveur partenaireRéu ir le serveur hôteRéu Réussite

Ensuite, le failover est configuré. On peut rajouter le serveur failover dans le serveur racine pour voir si cela a bien marché

Cliquer ici et faire clic droit

« ajouter un serveur » Mettre le nom du serveur et voici le résultat :

