PAGE DE GARDE DU DOSSIER PROFESSIONNEL

BREVET DE TECHNICIEN SUPÉRIEUR SERVICES INFORMATIQUES AUX ORGANISATIONS

Session 2026

DOSSIER PROFESSIONNEL

NOM : VIAUD

Prénom : Julien

Établissement de formation (sur un seul des deux exemplaires du dossier)

Visa du représentant de l'équipe pédagogique attestant la réalité des activités professionnelles décrites dans le dossier (sur un seul des deux exemplaires du dossier) :

Nom et qualité du signataire	Date	Signature
BOLLIN Antonin Formateur SIO SISR	23/04/2026	

Attestation sur l'honneur pour les candidats individuels (sur un seul des deux exemplaires du dossier) :

Je soussigné(e), Nom , Prénom , certifie que les activités décrites ainsi que les différentes informations reproduites dans ce dossier reflètent les activités professionnelles que j'ai personnellement réalisées au cours de ma formation.

Fait à **La Roche sur Yon**
Date **28/04/2026**

Signature 

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2026**

ANNEXE VII-1-A : Fiche descriptive de réalisation professionnelle (recto)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	**N° réalisation : 1**
Nom, prénom : VIAUD Julien	**N° candidat : 2543700461**
Épreuve ponctuelle ☒ **Contrôle en cours de formation** ☐	**Date :** 28 / 04 / 2026

Organisation support de la réalisation professionnelle
JLNetwork

Intitulé de la réalisation professionnelle
BASTION

Période de réalisation : 2025/2026 **Lieu :** Fab'Academy La Roche sur Yon
Modalité : ☒ **Seul(e)** ☐ **En équipe**

Compétences travaillées

☒ Concevoir une solution d'infrastructure réseau

☒ Installer, tester et déployer une solution d'infrastructure réseau

☒ Exploiter, dépanner et superviser une solution d'infrastructure réseau

Conditions de réalisation[1] (ressources fournies, résultats attendus)

Ressources fournies :

- Serveur physique hébergeant Proxmox VE avec l'ensemble des VMs du projet Oasis déjà déployées
- Infrastructure réseau segmentée en VLANs via switchs Cisco Catalyst 1000 Series et pfSense
- Active Directory déjà en place sur SRV-AD (oasis.jln, 192.168.4.1, Windows Server 2022)
- VLAN 14 (Management, 192.168.14.0/24) dédié à l'administration, passerelle pfSense (192.168.15.253)
- Plan d'adressage défini : bastion IP 192.168.15.15/24, postes admins VLAN 14
- ISO Windows Server 2022 Standard et drivers VirtIO disponibles dans Proxmox

Résultats attendus :

- Le bastion constitue le point d'entrée unique et contrôlé vers tous les serveurs administrés (VLAN 4 et VLAN 10)
- L'accès RDP au bastion est restreint aux seuls postes du VLAN 14 (Management)
- Toutes les connexions sont tracées dans l'Observateur d'événements Windows (IDs 4624, 4625, 4634)
- Rebond RDP vers serveurs Windows (SRV-AD, SRV-AD02) et SSH vers serveurs Linux depuis le bastion
- Bannière d'avertissement légale s'affiche avant chaque authentification RDP

[1] En référence aux *conditions de réalisation et ressources nécessaires* du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.

Description des ressources documentaires, matérielles et logicielles utilisées[2]

Ressources matérielles :

- VM BASTION sur Proxmox : Windows Server 2022 Standard, 2 vCPU, 4 Go RAM, 60 Go disque VirtIO, 1 interface VLAN 14
- Switchs Cisco Catalyst 1000 Series (SWITCH-JLN-1 et SWITCH-JLN-2) assurant la segmentation VLAN
- Postes administrateurs (VLAN 14) utilisés pour les tests de connexion RDP au bastion

Ressources logicielles :

- Proxmox VE – création de la VM (ISO WS 2022 + ISO drivers VirtIO)
- Windows Server 2022 Standard – rôle RDS (RDSH), pare-feu Windows, GPO (gpedit.msc), Observateur d'événements
- PowerShell – New-NetIPAddress, New-NetFirewallRule, auditpol, Add-Computer
- pfSense – règles de filtrage RDP (port 3389) depuis VLAN 14 uniquement, blocage accès directs
- Active Directory (oasis.jln) – jonction domaine, groupe Admins_Bastion, GPO mot de passe fort
- mstsc.exe / PuTTY – rebond RDP et SSH vers serveurs cibles depuis le bastion

Ressources documentaires :

- Documentation Microsoft – rôle RDS sur Windows Server 2022, GPO, pare-feu Windows
- Documentation pfSense – règles de filtrage inter-VLAN

Modalités d'accès aux productions[3] et à leur documentation[4]

Tous les accès aux serveurs se font via le bastion (RDP sur le bureau de votre poste). Vous utiliserez le compte AD « jury » — MDP : L@5896YHplm. Les mots de passe des serveurs sont sur le KeePass situé sur le bureau de votre bastion. L'ensemble des documents sont à votre disposition dans Nextcloud. Vous avez accès à Nextcloud via l'URL https://192.168.4.2/ ou http://srv-nextcloud.oasis.jln/

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2026**

ANNEXE VII-1-A : Fiche descriptive de réalisation professionnelle (verso, éventuellement pages suivantes)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

[2] Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

[3] Conformément au référentiel du BTS SIO « *Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve.* ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.

[4] Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemples schéma complet de réseau mis en place et configurations des services.

Descriptif de la réalisation professionnelle, y compris les productions réalisées et schémas explicatifs

Contexte :

L'infrastructure réseau du projet Oasis est déployée sur deux sites interconnectés : le siège de Paris et l'agence de Marseille, reliés par un lien WAN (VLAN 110, plage 10.110.110.0/24). Chaque site est segmenté en plusieurs VLANs afin d'isoler les services (serveurs, clients, WiFi employés, WiFi visiteurs, management).

Dans ce contexte, l'administration à distance des serveurs (VLAN 4 pour Marseille, VLAN 10 pour Paris) doit être sécurisée, centralisée et traçable. Un bastion a été déployé sous Windows Server 2022 Standard dans le VLAN 14 (Management). L'accès au bastion s'effectue via le protocole RDP (Remote Desktop Protocol) grâce au rôle « Services Bureau à distance » activé sur le serveur. Ce bastion constitue le point d'entrée unique et contrôlé vers l'ensemble des serveurs administrés.

Problématique :

Le bastion RDP doit répondre aux exigences suivantes :

- Constituer le seul point d'accès autorisé vers les serveurs des VLAN 4 et VLAN 10,
- N'autoriser les connexions RDP entrantes que depuis les postes du VLAN 14 (Management),
- Restreindre l'accès aux seuls comptes dédiés Active Directory avec des mots de passe forts,
- Journaliser toutes les connexions entrantes et sortantes pour garantir la traçabilité,
- Bloquer tout accès direct depuis le VLAN 14 vers les serveurs cibles sans passer par le bastion,
- Afficher une bannière d'avertissement légale avant chaque authentification.

Étude des solutions / choix de la solution

Plusieurs solutions ont été envisagées pour sécuriser l'accès aux serveurs administrés :

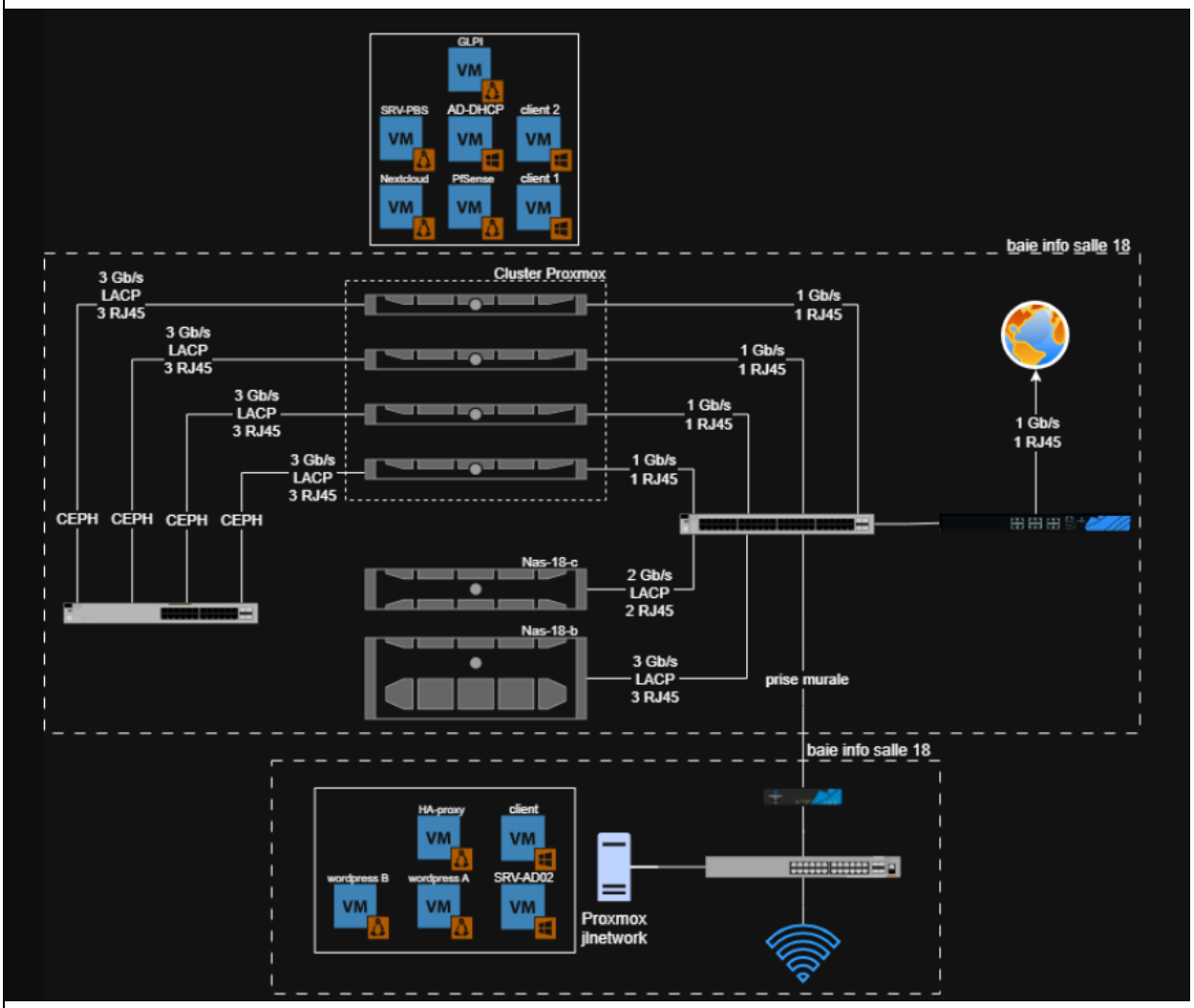
Critère	Bastion RDP (WS 2022)	VPN SSL (pfSense)	Jump Server Linux (SSH)
Coût	Inclus (licence existante)	Inclus (licence FW)	Gratuit
Intégration AD	Native (GPO, NLA, RBAC)	Partielle	Limitée
Protocole	RDP (port 3389) + SSH possible	SSL/TLS	SSH uniquement
Accès graphique	Oui (Bureau à distance complet)	Non (CLI/web)	Non
Sécurité	Très élevée	Élevée	Très élevée
Traçabilité	Journaux Windows (4624/4625)	Logs pfSense	auth.log
Facilité d'usage	Élevée (interface graphique)	Moyenne	Faible (CLI)
Retenu	✓OUI	Non	Non

Le bastion RDP sous Windows Server 2022 a été retenu car l'infrastructure repose sur un environnement principalement Windows (Active Directory, serveurs Windows). Cette solution offre une interface graphique complète pour l'administration, une intégration native à l'Active Directory et une traçabilité assurée par les

journaux Windows natifs. Elle est également compatible avec l'administration des serveurs Linux via un client SSH lancé depuis le bastion.

Plan physique

Le bastion est une machine virtuelle Windows Server 2022 hébergée sur l'hyperviseur Proxmox. Il dispose d'une seule interface réseau, connectée au VLAN 14 (Management) avec l'adresse IP 192.168.15.15/24. La passerelle de ce VLAN est pfSense (192.168.15.253), qui contrôle l'intégralité des flux entre le VLAN 14 et les autres VLANs.



Plan logique

Les flux autorisés dans l'infrastructure sont les suivants :

- Poste admin (VLAN 14) → Bastion (192.168.15.15, port 3389) : connexion RDP autorisée par pfSense,
- Bastion → SRV-AD (192.168.4.1, port 3389) et SRV-AD02 (192.168.10.1, port 3389) : rebond RDP autorisé,
- Bastion → Serveurs Linux VLAN 4 (192.168.4.2 à .4.6, port 22) : connexion SSH autorisée,
- Bastion → Serveurs Linux VLAN 10 (192.168.10.2 à .10.4, port 22) : connexion SSH autorisée,
- Poste admin → Serveurs VLAN 4 / VLAN 10 (accès direct) : bloqué par pfSense (règles 6 et 7),
- Tout autre flux non répertorié : bloqué par défaut (deny all implicite).

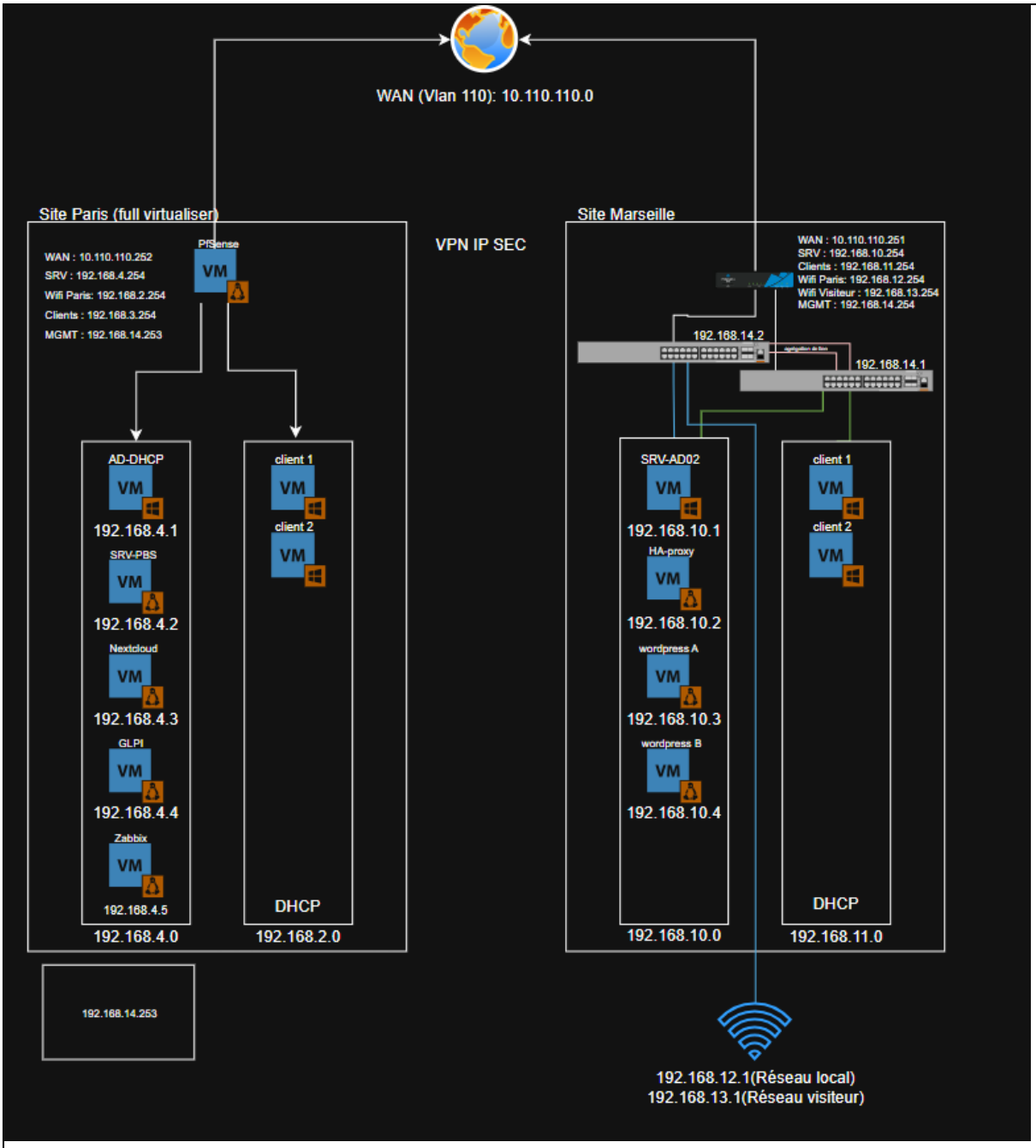


Tableau des VLANs

VLAN	Nom	Réseau	Passerelle	Rôle
2	OPNsense_Wifi	192.168.2.0/24	192.168.2.254	WiFi employés Marseille
3	OPNsense_Client	192.168.3.0/24	192.168.3.254	Clients Marseille – DHCP .3.1→.3.100
4	OPNsense_srv	192.168.4.0/24	192.168.4.254	Serveurs Marseille
10	Stormshield_srv	192.168.10.0/24	192.168.10.254	Serveurs Paris
11	Stormshield_Client	192.168.11.0/24	192.168.11.254	Clients Paris – DHCP
12	Stormshield_Wifi	192.168.12.0/24	192.168.12.254	WiFi Paris employés – DHCP

13	Stormshield_Visit.	192.168.13.0/24	192.168.13.254	WiFi Paris visiteurs – DHCP
14	Stormshield_MGMT	192.168.14.0/24	192.168.14.254	Management équipements réseau
110	WAN	10.110.110.0/24	10.110.110.254	Liaison WAN inter-sites (simulée)

Plan d'adressage

Équipement	Adresse IP	Masque	Passerelle	Réseau / Rôle
Bastion (WS 2022)	192.168.15.15	/24	192.168.15.253	VLAN 14 – MGMT
pfSense_MGMT (passerelle)	192.168.15.253	/24	—	VLAN 14 – MGMT
SWITCH-JLN-1	192.168.14.1	/24	192.168.14.254	VLAN 14 – MGMT
SWITCH-JLN-2	192.168.14.2	/24	192.168.14.254	VLAN 14 – MGMT
SRV-AD (cible RDP)	192.168.4.1	/24	192.168.4.254	VLAN 4 – Serveurs Marseille
SRV-Nextcloud (cible SSH)	192.168.4.2	/24	192.168.4.254	VLAN 4 – Serveurs Marseille
SRV-PBS (cible SSH)	192.168.4.3	/24	192.168.4.254	VLAN 4 – Serveurs Marseille
SRV-GLPI (cible SSH)	192.168.4.4	/24	192.168.4.254	VLAN 4 – Serveurs Marseille
SRV-ZABBIX (cible SSH)	192.168.4.5	/24	192.168.4.254	VLAN 4 – Serveurs Marseille
SRV-SYSLOG (cible SSH)	192.168.4.6	/24	192.168.4.254	VLAN 4 – Serveurs Marseille
SRV-AD02 (cible RDP)	192.168.10.1	/24	192.168.10.254	VLAN 10 – Serveurs Paris
HA-PROXY (cible SSH)	192.168.10.2	/24	192.168.10.254	VLAN 10 – Serveurs Paris
WORDPRESS-A (cible SSH)	192.168.10.3	/24	192.168.10.254	VLAN 10 – Serveurs Paris
WORDPRESS-B (cible SSH)	192.168.10.4	/24	192.168.10.254	VLAN 10 – Serveurs Paris
Poste admin (exemple)	192.168.14.50	/24	192.168.14.254	VLAN 14 – MGMT

Déroulement de la mission en lien avec les compétences

Étape 1 – Création de la VM sur Proxmox

La première étape a consisté à créer la machine virtuelle qui hébergera le bastion sur l'hyperviseur Proxmox. Les paramètres de la VM ont été définis comme suit :

- Nom de la VM : BASTION,
- Système d'exploitation : Windows Server 2022 Standard (ISO montée dans Proxmox),
- Ressources allouées : 2 vCPU, 4 Go de RAM, 60 Go de disque (VirtIO SCSI),
- Interface réseau : 1 carte VirtIO connectée au VLAN 14 (Management),

- L'ISO de Windows Server 2022 a été montée dans le lecteur CD/DVD virtuel de la VM,
- L'ISO des drivers VirtIO a également été montée pour assurer la compatibilité des pilotes réseau et disque sous Windows.

Étape 2 – Installation de Windows Server 2022

Une fois la VM créée et démarrée, l'installation de Windows Server 2022 a été réalisée manuellement depuis l'ISO :

- Sélection de la langue, du fuseau horaire et du format clavier (Français),
- Type d'installation : Installation personnalisée (nouvelle installation),
- Édition choisie : Windows Server 2022 Standard (Expérience utilisateur) — interface graphique complète,
- Installation des drivers VirtIO pendant l'installation (pilote de disque VirtIO SCSI requis pour détecter le disque virtuel),
- Définition du mot de passe du compte Administrateur local (mot de passe complexe, 16 caractères minimum),
- Après installation, mise à jour complète de Windows via Windows Update avant toute configuration.

Renommage du serveur pour l'identifier clairement dans l'infrastructure :

```
Rename-Computer -NewName "BASTION" -Restart
```

Étape 3 – Configuration réseau et jonction au domaine

Après l'installation, l'interface réseau a été configurée avec une adresse IP statique correspondant au plan d'adressage du VLAN 14 :

Configuration de l'adresse IP via PowerShell :

```
New-NetIPAddress -InterfaceAlias 'Ethernet' -IPAddress 192.168.15.15 -PrefixLength 24 -DefaultGateway 192.168.15.253
Set-DnsClientServerAddress -InterfaceAlias 'Ethernet' -ServerAddresses 192.168.4.1
```

192.168.4.1 = SRV-AD (serveur DNS du domaine oasis.local)

Vérification de la connectivité vers le contrôleur de domaine et la passerelle pfSense :

```
Test-Connection 192.168.4.1   # Ping vers SRV-AD
Test-Connection 192.168.15.253 # Ping vers pfSense
```

Jonction du bastion au domaine Active Directory oasis.local :

```
Add-Computer -DomainName "oasis.local" -Credential (Get-Credential) -Restart
```

Les informations d'identification d'un compte administrateur du domaine sont demandées.

Après redémarrage, vérification de la jonction au domaine :

```
(Get-WmiObject Win32_ComputerSystem).Domain
```

La commande doit retourner : oasis.local

Création du groupe de sécurité « Admins_Bastion » dans l'Active Directory, regroupant uniquement les comptes d'administration autorisés à se connecter au bastion. Chaque administrateur dispose d'un compte nominatif dédié (ex. j.viaud_admin), distinct de son compte utilisateur standard. Le compte Administrateur local est désactivé :

```
Disable-LocalUser -Name 'Administrateur'
```

Étape 4 – Installation du rôle Services Bureau à distance (RDS)

Le rôle « Services Bureau à distance » a été installé afin d'autoriser les connexions RDP entrantes depuis les postes administrateurs. L'installation a été réalisée via le Gestionnaire de serveur :

- Ouverture du Gestionnaire de serveur → Ajouter des rôles et fonctionnalités,
- Type d'installation : Installation basée sur un rôle ou une fonctionnalité,
- Rôle sélectionné : Services Bureau à distance,
- Sous-rôle activé : Hôte de session Bureau à distance (RDSH),
- Validation et installation, puis redémarrage du serveur.

Vérification du bon démarrage du service via PowerShell :

```
Get-Service -Name TermService
```

Le statut doit être « Running » et le type de démarrage « Automatic ».

Étape 5 – Sécurisation de l'accès RDP

Plusieurs paramètres de sécurité ont été configurés pour renforcer la protection des connexions RDP :

Activation de l'authentification au niveau du réseau (NLA) :

- Panneau de configuration → Système → Paramètres d'utilisation à distance,
- Option activée : « Autoriser les connexions uniquement depuis les ordinateurs exécutant Bureau à distance avec authentification au niveau du réseau »,
- La NLA impose l'authentification Active Directory avant l'ouverture de toute session graphique, réduisant l'exposition aux attaques.

Restriction des utilisateurs autorisés à se connecter en RDP :

- Seuls les membres du groupe « Admins_Bastion » (créé dans l'AD oasis.local) sont autorisés,
- Ajout du groupe via : Propriétés système → Utilisation à distance → Sélectionner des utilisateurs.

Politique de mot de passe fort appliquée via GPO (Éditeur de gestion des stratégies de groupe) :

- Longueur minimale : 12 caractères,
- Complexité requise : majuscules, minuscules, chiffres et caractères spéciaux obligatoires,
- Durée de vie maximale du mot de passe : 90 jours,
- Verrouillage du compte après 5 tentatives d'authentification échouées pendant 30 minutes.

Étape 6 – Configuration du pare-feu Windows

Le pare-feu Windows Defender a été configuré pour restreindre les connexions RDP entrantes (port 3389) aux seuls hôtes du VLAN 14. Toute tentative depuis un autre réseau est bloquée, même si pfSense laissait passer le trafic (défense en profondeur).

Configuration via PowerShell :

```
# Suppression de la règle RDP par défaut (trop permissive)
Remove-NetFirewallRule -DisplayName 'Bureau à distance - Mode utilisateur
(TCP-In)' -ErrorAction SilentlyContinue

# Création d'une règle RDP restrictive : VLAN 14 uniquement
New-NetFirewallRule -Name 'RDP-VLAN14-Only' ``
  -DisplayName 'RDP entrant – VLAN 14 uniquement' ``
  -Direction Inbound -Protocol TCP -LocalPort 3389 ``
  -RemoteAddress 192.168.14.0/24,192.168.15.0/24 ``
  -Action Allow
```

Récapitulatif des règles du pare-feu Windows :

Nom de la règle	Direction	Port	Proto	Action	Description
RDP-VLAN14-Only	Entrante	3389	TCP	✓ ALLOW	Autoriser RDP uniquement depuis 192.168.14.0/24 et 192.168.15.0/24
SSH-Sortant-VLAN4	Sortante	22	TCP	✓ ALLOW	Autoriser SSH vers VLAN 4 (192.168.4.0/24)
SSH-Sortant-VLAN10	Sortante	22	TCP	✓ ALLOW	Autoriser SSH vers VLAN 10 (192.168.10.0/24)
RDP-Sortant-Cibles	Sortante	3389	TCP	✓ ALLOW	Autoriser RDP vers serveurs Windows cibles
Bloquer-RDP-Autres	Entrante	3389	TCP	✕ BLOCK	Bloquer toute connexion RDP hors VLAN 14

Étape 7 – Règles de filtrage sur pfSense

pfSense (192.168.15.253) constitue la passerelle du VLAN 14 et assure le filtrage de tous les flux entre ce VLAN et les autres VLANs de l'infrastructure. Les règles ont été configurées dans l'interface web de pfSense (Firewall → Rules → VLAN14) selon le principe du moindre privilège : tout ce qui n'est pas explicitement autorisé est bloqué.

Tableau des règles configurées sur pfSense (ordre de priorité croissant) :

N°	Source	Destination	Port	Proto	Action	Description
1	192.168.14.0/24 (VLAN 14)	192.168.15.15 (Bastion)	3389	TCP	✓ ALLOW	Autoriser RDP depuis les postes admins vers le bastion
2	192.168.15.15 (Bastion)	192.168.4.1 (SRV-AD)	3389	TCP	✓ ALLOW	Autoriser rebond RDP bastion → SRV-AD
3	192.168.15.15 (Bastion)	192.168.10.1 (SRV-AD02)	3389	TCP	✓ ALLOW	Autoriser rebond RDP bastion → SRV-AD02 Paris
4	192.168.15.15 (Bastion)	192.168.4.0/24 (VLAN 4)	22	TCP	✓ ALLOW	Autoriser SSH bastion → serveurs Linux Marseille
5	192.168.15.15 (Bastion)	192.168.10.0/24 (VLAN 10)	22	TCP	✓ ALLOW	Autoriser SSH bastion → serveurs Linux Paris
6	192.168.14.0/24 (VLAN 14)	192.168.4.0/24 (VLAN 4)	Tous	Tous	✕BLOCK	Bloquer tout accès direct postes admins → VLAN 4
7	192.168.14.0/24 (VLAN 14)	192.168.10.0/24 (VLAN 10)	Tous	Tous	✕BLOCK	Bloquer tout accès direct postes admins → VLAN 10

8	Tous	Tous	Tous	Tous	✕BLOCK	Règle implicite : bloquer tout le reste (deny all)

Les règles 1 à 5 autorisent uniquement les flux strictement nécessaires à l'administration via le bastion. Les règles 6 et 7 bloquent tout accès direct des postes administrateurs vers les serveurs cibles, forçant le passage par le bastion. La règle 8 (deny all implicite) bloque tout trafic non couvert par les règles précédentes.

Étape 8 – Journalisation et traçabilité

La traçabilité de toutes les connexions au bastion est assurée par les journaux Windows natifs. Toutes les ouvertures et fermetures de session RDP sont enregistrées dans le journal « Sécurité » de l'Observateur d'événements.

Activation de l'audit des ouvertures de session via PowerShell :

```
auditpol /set /subcategory:"Logon" /success:enable /failure:enable
auditpol /set /subcategory:"Other Logon/Logoff Events" /success:enable
/failure:enable
```

Événements clés enregistrés dans le journal Sécurité (Observateur d'événements) :

- ID 4624 : Ouverture de session réussie — indique l'heure, le compte utilisé et l'adresse IP source,
- ID 4625 : Échec d'ouverture de session — utile pour détecter des tentatives d'intrusion,
- ID 4634 : Fermeture de session — enregistre la fin de chaque session RDP,
- ID 4779 : Déconnexion d'une session Bureau à distance,
- ID 4648 : Tentative de connexion avec des informations d'identification explicites.

Consultation des dernières connexions réussies via PowerShell :

```
Get-EventLog -LogName Security -InstanceId 4624 -Newest 20 | Format-List
TimeGenerated, Message
```

Étape 9 – Bannière d'avertissement légale

Une bannière d'avertissement légale a été configurée via une stratégie de groupe (GPO) afin qu'elle s'affiche avant chaque connexion RDP au bastion. Elle informe l'utilisateur que l'accès est réservé aux personnes autorisées et que toutes les sessions sont enregistrées.

Configuration via l'Éditeur de stratégie de groupe locale (gpedit.msc) :

- Chemin : Configuration ordinateur → Paramètres Windows → Paramètres de sécurité → Stratégies locales → Options de sécurité,
- Paramètre « Ouverture de session interactive : titre du message » → valeur : ACCÈS RESTREINT – PROJET OASIS,
- Paramètre « Ouverture de session interactive : texte du message » → valeur :

```
Vous vous connectez à un équipement d'administration sécurisé du projet
Oasis.
L'accès est strictement réservé au personnel autorisé.
Toutes les sessions sont enregistrées et surveillées.
Tout accès non autorisé fera l'objet de poursuites judiciaires.
```

Étape 10 – Administration des serveurs cibles depuis le bastion

Une fois connecté au bastion en RDP depuis son poste administrateur, l'utilisateur dispose d'un environnement Windows complet depuis lequel il peut administrer tous les serveurs cibles de l'infrastructure.

Administration des serveurs Windows (via RDP depuis le bastion) :

- Lancement du client Bureau à distance natif (mstsc.exe) depuis le bureau du bastion,
- Saisie de l'adresse IP du serveur cible (ex. 192.168.4.1 pour SRV-AD, 192.168.10.1 pour SRV-AD02),
- Authentification avec le compte dédié (ex. j.viaud_admin@oasis.local).

Administration des serveurs Linux (via SSH depuis le bastion) :

- Utilisation du client PuTTY installé sur le bastion, ou du client SSH natif Windows (PowerShell),
- Connexion vers les serveurs Linux cibles : SRV-PBS (192.168.4.3), SRV-Nextcloud (192.168.4.2), SRV-GLPI (192.168.4.4), SRV-ZABBIX (192.168.4.5), SRV-SYSLOG (192.168.4.6), HA-PROXY (192.168.10.2), WORDPRESS-A (192.168.10.3), WORDPRESS-B (192.168.10.4),
- Authentification par compte dédié avec mot de passe fort.

Exemple de connexion SSH depuis le bastion (PowerShell) :

```
ssh adminsisr@192.168.4.3
```

Connexion SSH vers SRV-PBS depuis le bastion

À aucun moment les postes administrateurs ne se connectent directement aux serveurs cibles. Le bastion est le seul intermédiaire autorisé, ce qui garantit la traçabilité et la sécurité de toutes les sessions d'administration.

Tests

Les tests suivants ont été réalisés pour valider le bon fonctionnement du bastion RDP et des règles de filtrage associées :

Test réalisé	Résultat attendu	Résultat obtenu	Statut
Connexion RDP depuis poste admin (VLAN 14) → Bastion 192.168.15.15	Session Bureau à distance ouverte	Session RDP ouverte	✓OK
Connexion RDP refusée depuis VLAN 3 (clients)	Connexion bloquée par pfSense	Connection timed out	✓OK
Connexion RDP refusée depuis VLAN 4 (serveurs)	Connexion bloquée par pfSense	Connection timed out	✓OK
Connexion RDP depuis le bastion → SRV-AD (192.168.4.1)	Session Bureau à distance ouverte	Session RDP ouverte	✓OK
Connexion RDP depuis le bastion → SRV-AD02 Paris (192.168.10.1)	Session Bureau à distance ouverte	Session RDP ouverte	✓OK
Connexion SSH depuis le bastion → SRV-PBS (192.168.4.3)	Session SSH ouverte	Session SSH ouverte	✓OK
Connexion SSH depuis le bastion → HA-PROXY (192.168.10.2)	Session SSH ouverte	Session SSH ouverte	✓OK

Accès RDP direct poste admin → SRV-AD sans passer par le bastion	Bloqué par pfSense (règle 6)	Connection timed out	✓OK
Tentative de connexion RDP avec un compte non autorisé	Accès refusé – Logon failure	Logon failure	✓OK
Vérification ID 4624 dans l'Observateur d'événements	Trace de connexion RDP réussie visible	Événement présent	✓OK
Vérification ID 4625 dans l'Observateur d'événements	Tentative échouée enregistrée	Événement présent	✓OK
Bannière d'avertissement affichée avant l'authentification	Message légal affiché	Bannière affichée	✓OK

Conclusion

Cette mission m'a permis de déployer un bastion RDP complet sur Windows Server 2022, depuis la création de la VM sur Proxmox jusqu'à la configuration finale des règles de sécurité. J'ai mis en œuvre l'ensemble de la chaîne suivante :

- Création et installation de la VM Windows Server 2022 sur Proxmox avec montage d'ISO et drivers VirtIO,
- Configuration réseau statique (VLAN 14, IP 192.168.15.15) et jonction au domaine Active Directory oasis.local,
- Installation et configuration du rôle Services Bureau à distance (RDS) pour l'accès RDP,
- Sécurisation de l'accès RDP : NLA, groupe Admins_Bastion, mots de passe forts par GPO,
- Configuration du pare-feu Windows (règle RDP restreinte au VLAN 14),
- Mise en place des règles de filtrage sur pfSense : autorisation des flux légitimes et blocage de tout accès direct aux serveurs cibles,
- Journalisation complète des connexions via l'Observateur d'événements Windows (IDs 4624, 4625, 4634…),
- Affichage d'une bannière d'avertissement légale via GPO avant chaque connexion,
- Administration des serveurs Windows cibles en RDP et des serveurs Linux en SSH depuis le bastion.

Le bastion constitue ainsi le point d'entrée unique, sécurisé et traçable vers l'ensemble des serveurs administrés des VLAN 4 et VLAN 10, garantissant la confidentialité, l'intégrité et la disponibilité de l'infrastructure réseau du projet Oasis.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2026**

ANNEXE VII-1-A : Fiche descriptive de réalisation professionnelle (recto)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	**N° réalisation : 2**
Nom, prénom : VIAUD Julien	**N° candidat : 2543700461**
Épreuve ponctuelle ☒ **Contrôle en cours de formation** ☐	**Date :** 28 / 04 / 2026

Organisation support de la réalisation professionnelle
JLNetwork

Intitulé de la réalisation professionnelle
DHCP

Période de réalisation : 2025/2026 **Lieu :** Fab'Academy La Roche sur Yon
Modalité : ☒ **Seul(e)** ☐ **En équipe**

Compétences travaillées

☒ Concevoir une solution d'infrastructure réseau

☒ Installer, tester et déployer une solution d'infrastructure réseau

☒ Exploiter, dépanner et superviser une solution d'infrastructure réseau

Conditions de réalisation[5] (ressources fournies, résultats attendus)

Ressources fournies :

- SRV-AD (192.168.4.1, WS 2022) déjà déployé avec AD DS et DNS du domaine oasis.jln
- VLAN 3 (clients Marseille, 192.168.3.0/24) et VLAN 4 (serveurs, 192.168.4.0/24) segmentés
- pfSense configuré comme passerelle inter-VLAN (192.168.3.254) et capable d'assurer le DHCP Relay
- Postes clients Windows sur le VLAN 3 pour les tests de distribution DHCP
- Plan d'adressage défini : pool 192.168.3.1–192.168.3.100, passerelle 192.168.3.254, DNS 192.168.4.1

Résultats attendus :

- Les clients VLAN 3 obtiennent automatiquement une IP dans la plage 192.168.3.1–192.168.3.100
- Paramètres distribués : masque 255.255.255.0, passerelle 192.168.3.254, DNS 192.168.4.1, suffixe oasis.jln
- Serveur DHCP autorisé dans l'AD (protection anti-rogue DHCP)
- Baux visibles et gérables dans la console DHCP Windows (dhcpmgmt.msc)

[5] En référence aux *conditions de réalisation et ressources nécessaires* du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.

Description des ressources documentaires, matérielles et logicielles utilisées[6]

Ressources matérielles :

- VM SRV-AD sur Proxmox : WS 2022, 2 vCPU, 4 Go RAM, connectée VLAN 4 (192.168.4.1)
- pfSense : pare-feu inter-VLAN faisant office d'agent relais DHCP (DHCP Relay) entre VLAN 3 et VLAN 4
- Postes clients Windows (VLAN 3) pour les tests de distribution DHCP

Ressources logicielles :

- Windows Server 2022 – rôle DHCP Server, console dhcpmgmt.msc
- PowerShell – Install-WindowsFeature, Add-DhcpServerInDC, Add-DhcpServerv4Scope, Set-DhcpServerv4OptionValue, Get-DhcpServerv4Lease
- pfSense – DHCP Relay (Services → DHCP Relay) et règles UDP ports 67/68 inter-VLAN

Ressources documentaires :

- Documentation Microsoft – rôle DHCP Server sur Windows Server 2022, cmdlets PowerShell DHCP
- Documentation pfSense – DHCP Relay et règles de filtrage inter-VLAN

Modalités d'accès aux productions[7] et à leur documentation[8]

Productions réalisées :

- Dossier U6 complet – DHCP (VIAUD_Julien_DOSSIER_U6_DHCP.docx) : fonctionnement DORA, 6 étapes, tableau étendue, règles pfSense, tests
- Captures d'écran : console DHCP (étendue_DHCP_CLIENT, pool 192.168.3.1–192.168.3.100, options 003/006/015, baux actifs)
- Schémas : plan physique (SRV-AD VLAN 4, pfSense relais, clients VLAN 3) et plan logique (flux DORA)

Accès aux productions :

- Support numérique personnel (clé USB / stockage en ligne) présenté lors de l'épreuve

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2026**

ANNEXE VII-1-A : Fiche descriptive de réalisation professionnelle (verso, éventuellement pages suivantes)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

[6] Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

[7] Conformément au référentiel du BTS SIO « *Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve.* ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.

[8] Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemples schéma complet de réseau mis en place et configurations des services.

Descriptif de la réalisation professionnelle, y compris les productions réalisées et schémas explicatifs

Contexte :

L'infrastructure réseau du projet Oasis est déployée sur deux sites interconnectés : le siège de Paris et l'agence de Marseille. Sur le site de Marseille, le réseau est segmenté en plusieurs VLANs, dont le VLAN 3 dédié aux postes clients (192.168.3.0/24). Ces postes doivent obtenir automatiquement une configuration réseau (adresse IP, masque, passerelle, serveur DNS) sans intervention manuelle.

Pour répondre à ce besoin, le rôle DHCP Server a été installé sur le serveur SRV-AD (192.168.4.1), qui héberge déjà le contrôleur de domaine Active Directory et le serveur DNS du domaine oasis.jln. Ce choix permet de centraliser les services d'infrastructure sur un seul serveur et de bénéficier de l'intégration native entre DHCP, DNS dynamique et Active Directory.

Problématique :

Le serveur DHCP doit répondre aux exigences suivantes :

- Distribuer automatiquement des adresses IP aux clients du VLAN 3 (plage 192.168.3.1 – 192.168.3.100),
- Fournir aux clients l'ensemble des paramètres réseau : masque, passerelle (192.168.3.254) et serveur DNS (192.168.4.1),
- Distribuer le suffixe DNS du domaine (oasis.jln) pour la résolution de noms,
- Être autorisé dans l'Active Directory pour éviter tout serveur DHCP non autorisé (rogue DHCP),
- Permettre la vérification et la gestion des baux via la console DHCP Windows.

Étude des solutions / choix de la solution

Plusieurs solutions ont été envisagées pour distribuer les adresses IP aux clients du VLAN 3 :

Critère	DHCP sur SRV-AD (WS 2022)	DHCP sur pfSense	DHCP dédié (serveur séparé)
Coût	Inclus (licence existante)	Gratuit	Licence supplémentaire
Intégration AD	Native (DNS dynamique, GPO)	Absente	Partielle
Centralisation	Oui (même serveur que l'AD)	Séparé du reste	Séparé, administration dédiée
Gestion	Console DHCP Windows (GUI)	Interface web pfSense	Console DHCP Windows (GUI)
Disponibilité	Liée au serveur AD	Indépendante	Indépendante
Complexité	Faible	Faible	Moyenne
Retenu	✓OUI	Non	Non

Le rôle DHCP Server sur SRV-AD a été retenu car SRV-AD héberge déjà l'Active Directory et le DNS. L'intégration native entre DHCP et AD permet d'autoriser le serveur dans le domaine (protection contre les serveurs DHCP non autorisés) et d'activer la mise à jour DNS dynamique. Cette solution centralise les services d'infrastructure sans coût supplémentaire.

Fonctionnement du protocole DHCP

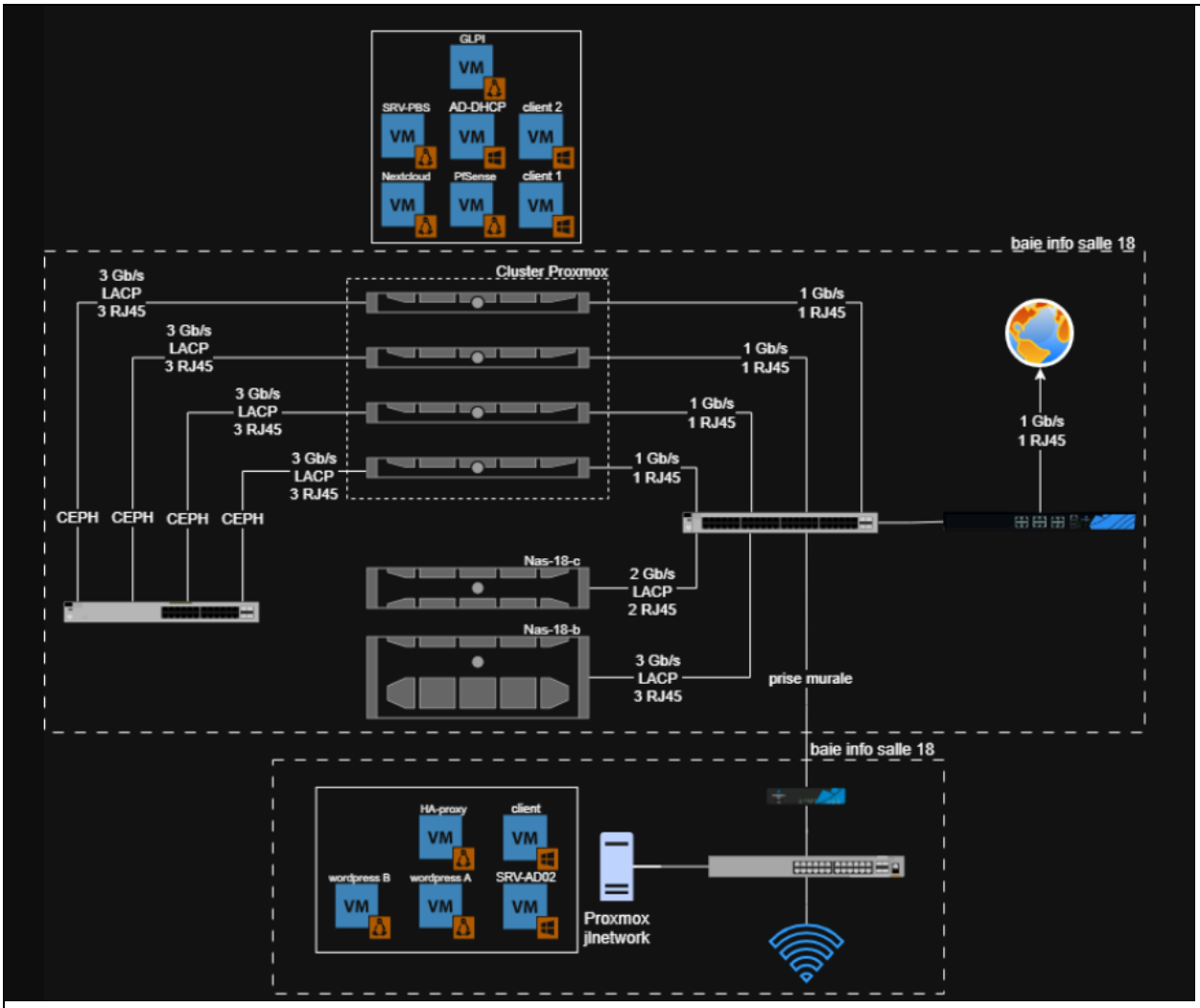
Le protocole DHCP (Dynamic Host Configuration Protocol) permet l'attribution automatique d'une configuration réseau à un client. Il repose sur un échange en quatre étapes, appelé processus DORA :

Étape	Source	Destination	Port	Proto	Description
DISCOVER	Client (0.0.0.0)	255.255.255.255 (broadcast)	67	UDP	Le client diffuse une demande d'adresse IP
OFFER	SRV-AD (192.168.4.1)	255.255.255.255 (broadcast)	68	UDP	Le serveur DHCP propose une adresse IP au client
REQUEST	Client (0.0.0.0)	255.255.255.255 (broadcast)	67	UDP	Le client confirme son acceptation de l'offre
ACK	SRV-AD (192.168.4.1)	Client	68	UDP	Le serveur confirme et valide le bail DHCP

Dans l'infrastructure du projet Oasis, le client (VLAN 3) émet ses messages en broadcast sur le réseau local. pfSense, configuré comme agent relais DHCP (DHCP Relay), retransmet ces messages au serveur DHCP (SRV-AD, 192.168.4.1) situé dans le VLAN 4. Le serveur répond directement au client avec les paramètres configurés dans l'étendue.

Plan physique

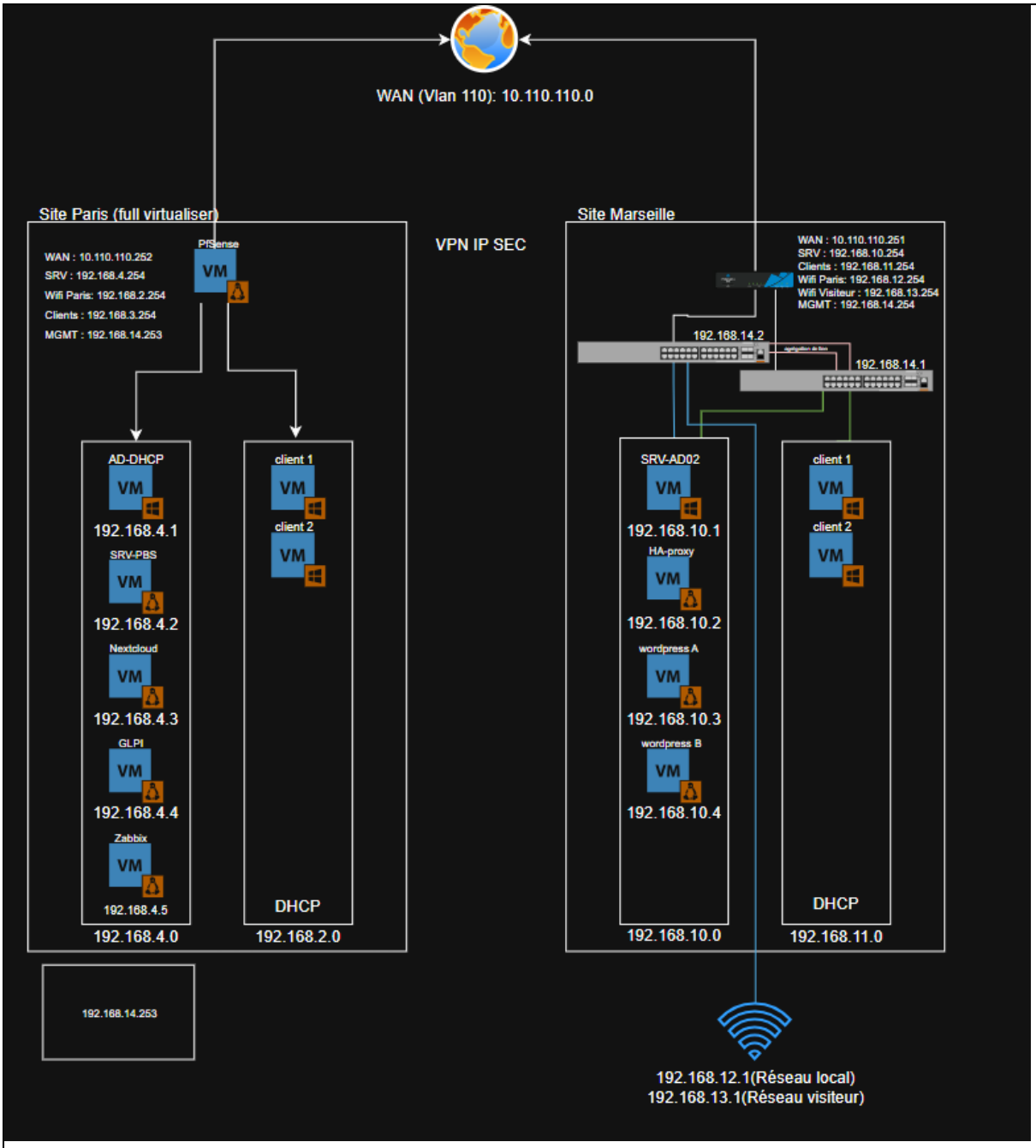
Le rôle DHCP est installé sur SRV-AD (192.168.4.1), une machine virtuelle hébergée sur Proxmox, connectée au VLAN 4 (Serveurs Marseille). Les clients qui reçoivent les adresses DHCP sont connectés au VLAN 3. La communication entre les deux VLANs est assurée par pfSense, configuré en agent relais DHCP pour retransmettre les requêtes des clients du VLAN 3 vers SRV-AD dans le VLAN 4.



Plan logique

Le flux DHCP entre le client et le serveur fonctionne de la manière suivante dans l'infrastructure :

- Le client (VLAN 3) émet une requête DHCP DISCOVER en broadcast (UDP port 67),
- pfSense (agent relais DHCP, 192.168.3.254) intercepte le broadcast et le retransmet en unicast vers SRV-AD (192.168.4.1, UDP port 67),
- SRV-AD répond avec une offre DHCP OFFER contenant les paramètres de l'étendue 192.168.3.0,
- Le client envoie un DHCP REQUEST pour confirmer l'offre, pfSense relaye vers SRV-AD,
- SRV-AD envoie un DHCP ACK pour valider le bail. Le client est configuré.



Plan d'adressage

Équipement	Adresse IP	Masque	Passerelle	Réseau / Rôle
SRV-AD / DHCP (même VM)	192.168.4.1	/24	192.168.4.254	VLAN 4 – Serveurs Marseille
pfSense_Client (GW VLAN 3)	192.168.3.254	/24	—	VLAN 3 – Passerelle clients
Pool DHCP – début	192.168.3.1	/24	—	VLAN 3 – Première IP distribuée
Pool DHCP – fin	192.168.3.100	/24	—	VLAN 3 – Dernière IP distribuée
Client 1 (exemple)	192.168.3.x (DHCP)	/24	192.168.3.254	VLAN 3 – Clients Marseille
Client 2 (exemple)	192.168.3.x (DHCP)	/24	192.168.3.254	VLAN 3 – Clients Marseille

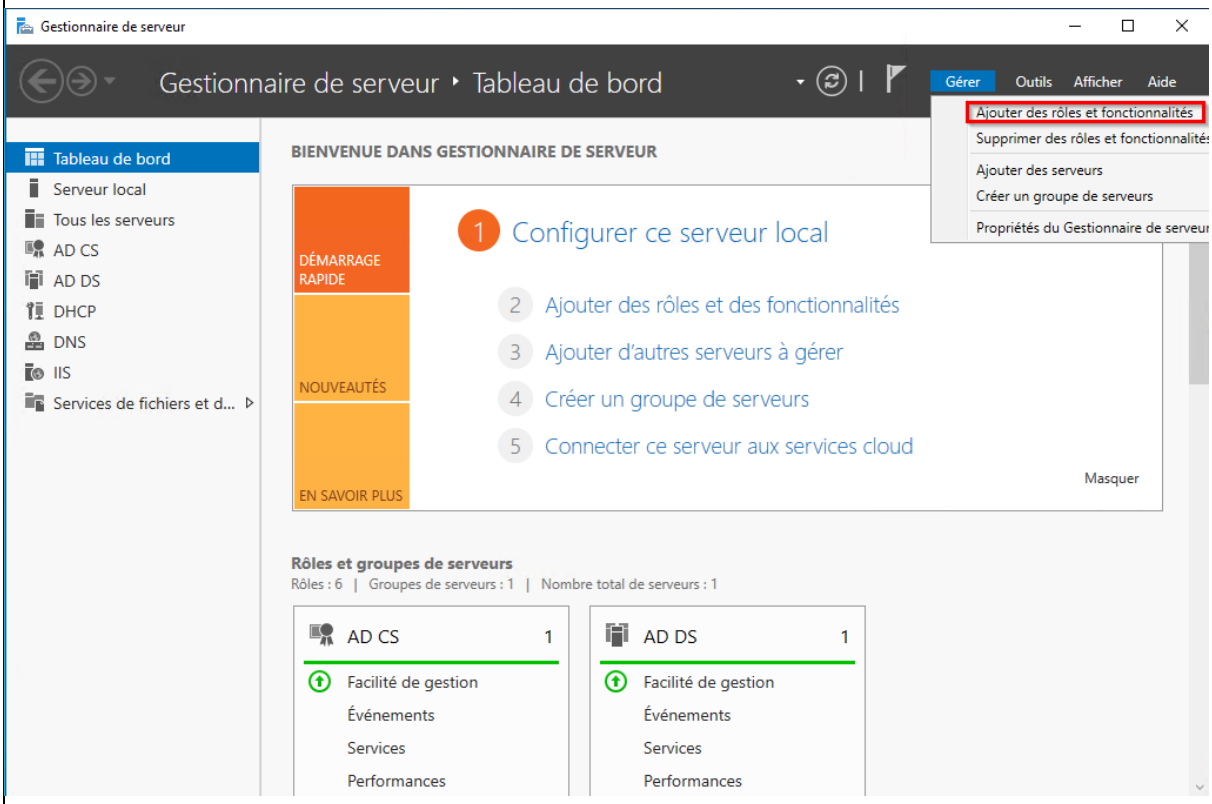
Déroulement de la mission en lien avec les compétences

Étape 1 – Installation du rôle DHCP Server sur SRV-AD

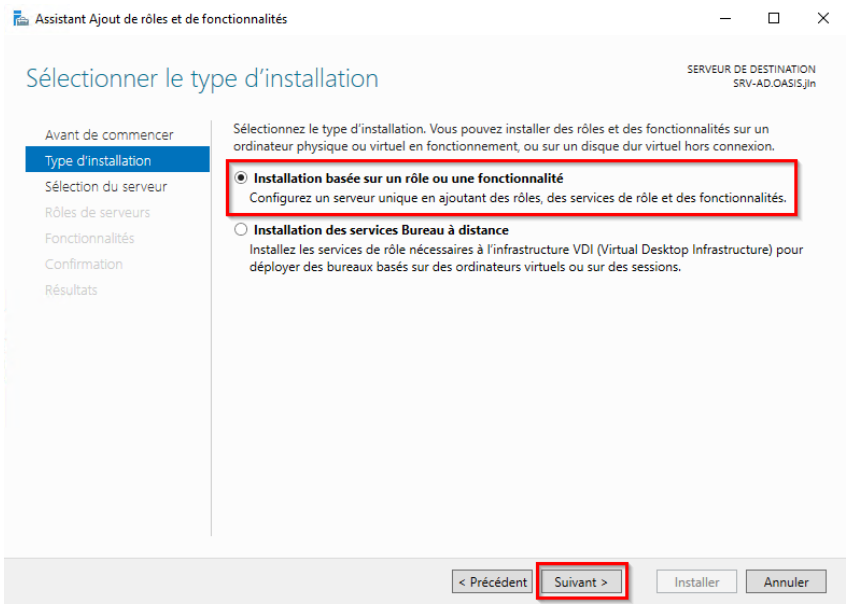
Le rôle DHCP Server a été ajouté sur SRV-AD via le Gestionnaire de serveur. SRV-AD héberge déjà les rôles AD DS (Active Directory Domain Services) et DNS, ce qui facilite l'intégration des trois services sur une même machine.

Installation via le Gestionnaire de serveur :

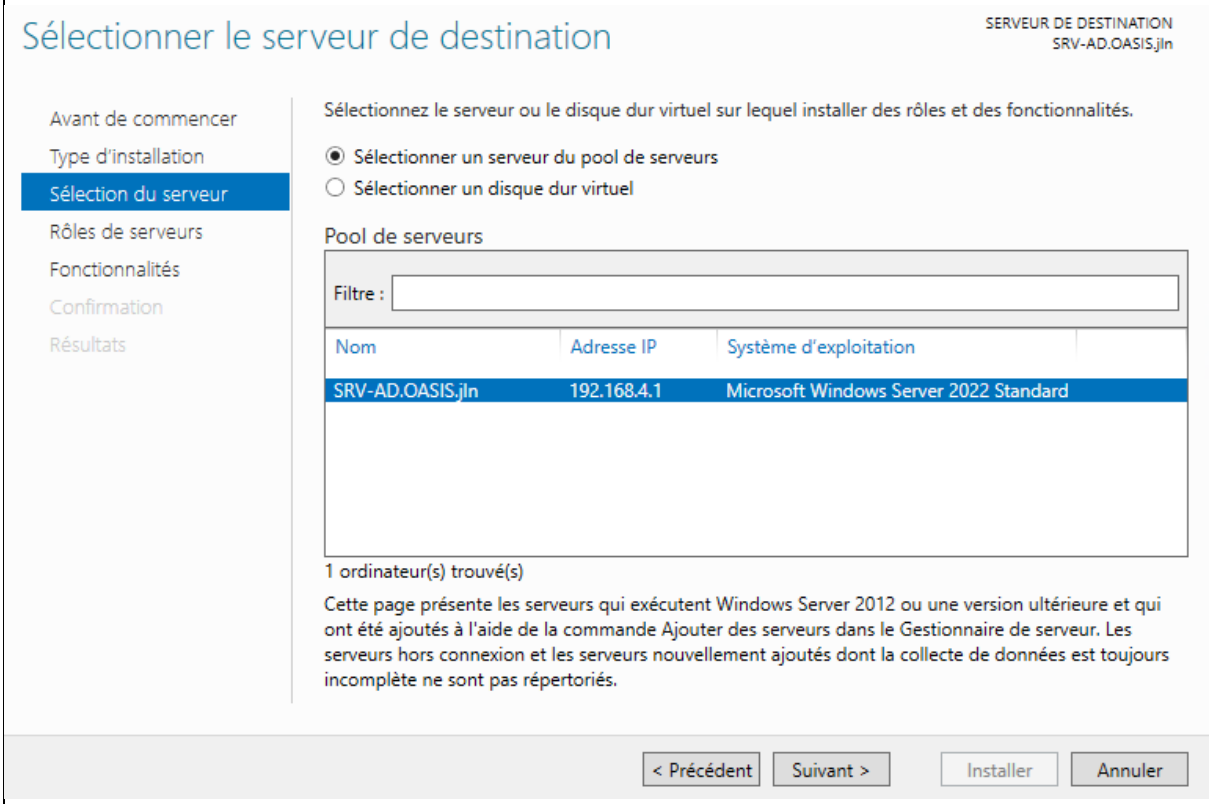
- Ouverture du Gestionnaire de serveur → Ajouter des rôles et fonctionnalités,



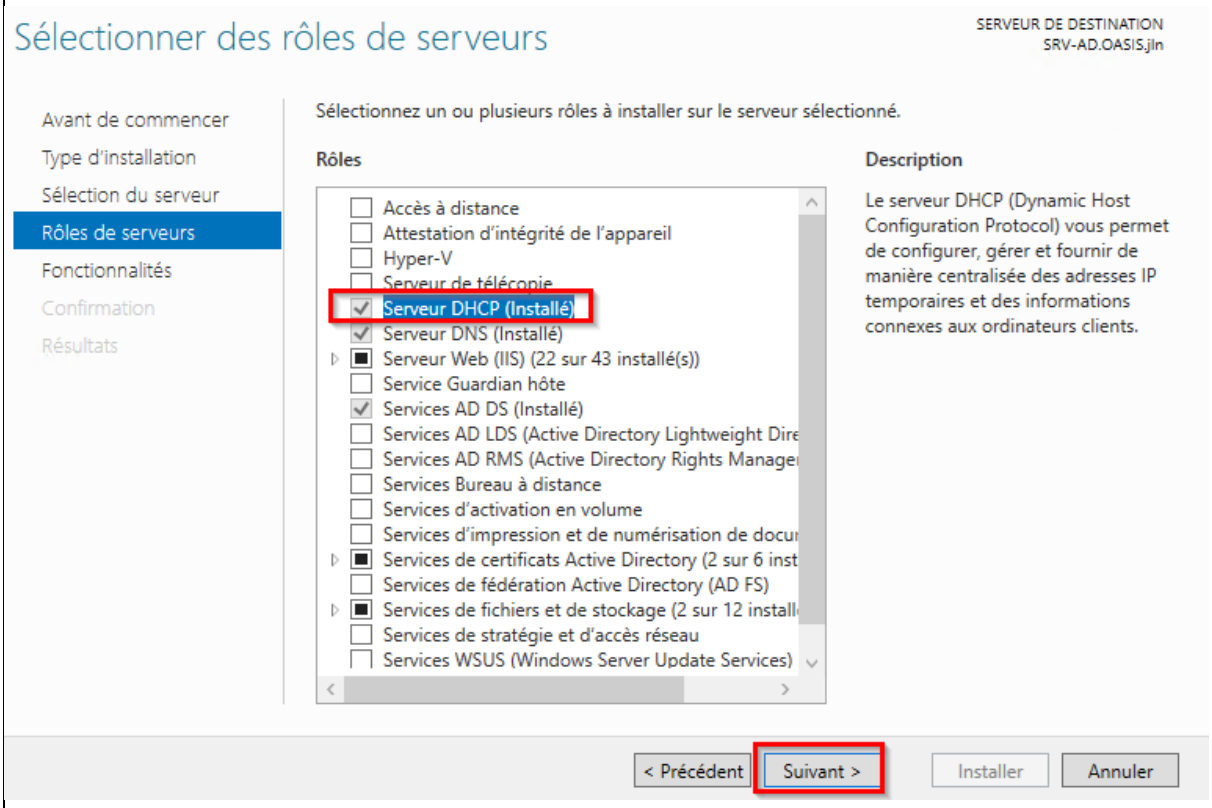
-
- Type d'installation : Installation basée sur un rôle ou une fonctionnalité,



- Sélection du serveur : srv-ad.oasis.jln (192.168.4.1),



- Rôle sélectionné : Serveur DHCP,



- Validation et installation, puis cliquer sur « Terminer la configuration DHCP » dans la notification post-installation.

Installation équivalente via PowerShell :

```
Install-WindowsFeature -Name DHCP -IncludeManagementTools
```

Vérification du démarrage du service :

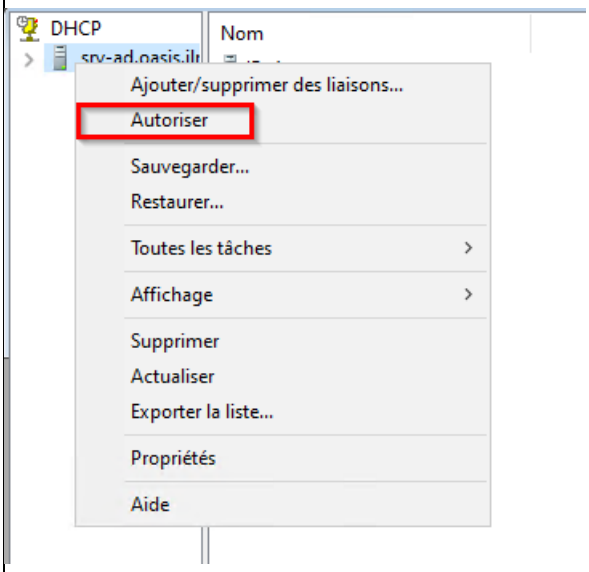
```
Get-Service -Name DHCPServer
```

Étape 2 – Autorisation du serveur DHCP dans l'Active Directory

Dans un environnement Active Directory, un serveur DHCP doit être explicitement autorisé pour pouvoir distribuer des adresses IP. Cette mesure protège le réseau contre les serveurs DHCP non autorisés (rogue DHCP) qui pourraient distribuer des paramètres réseau incorrects aux clients.

Autorisation du serveur DHCP depuis la console DHCP :

- Ouverture de la console DHCP (dhcpmgmt.msc),
- Clic droit sur le serveur srv-ad.oasis.jln → Autoriser,



- Après quelques secondes, l'icône du serveur passe au vert, confirmant l'autorisation dans l'AD.

Autorisation équivalente via PowerShell :

```
Add-DhcpServerInDC -DnsName "srv-ad.oasis.jln" -IPAddress 192.168.4.1
```

Vérification de l'autorisation :

```
Get-DhcpServerInDC
```

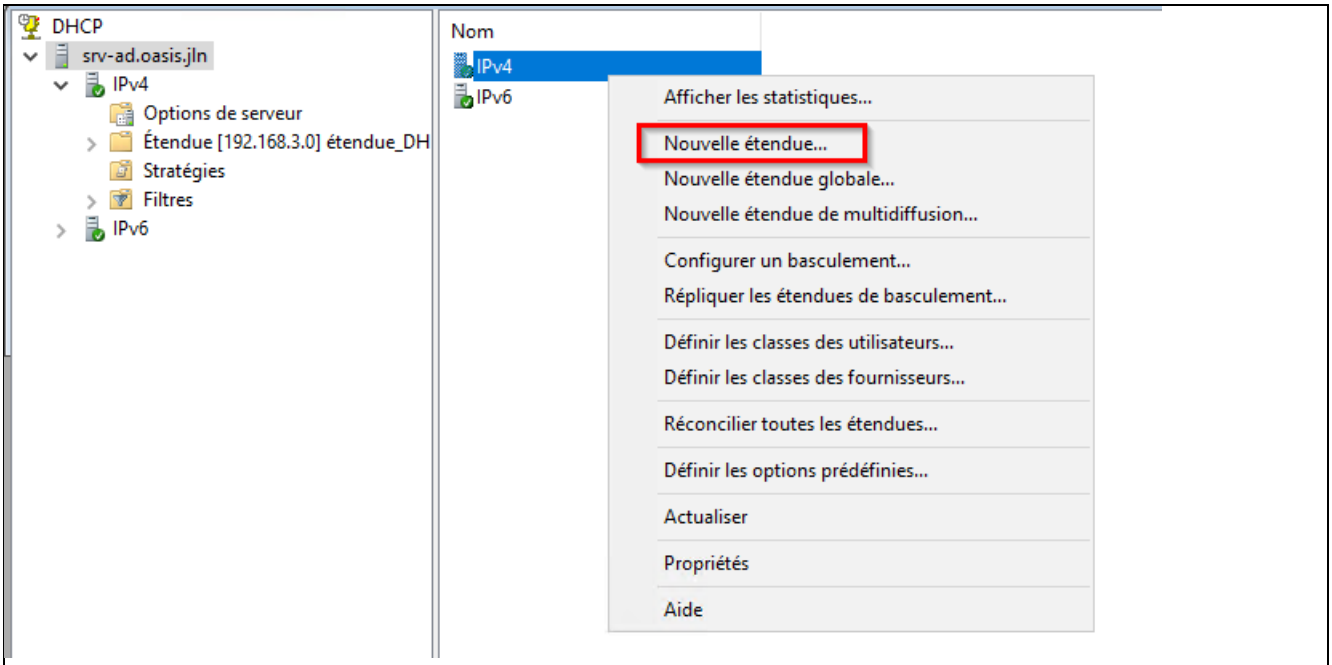
La commande doit retourner l'entrée srv-ad.oasis.jln avec l'IP 192.168.4.1.

Étape 3 – Création de l'étendue DHCP

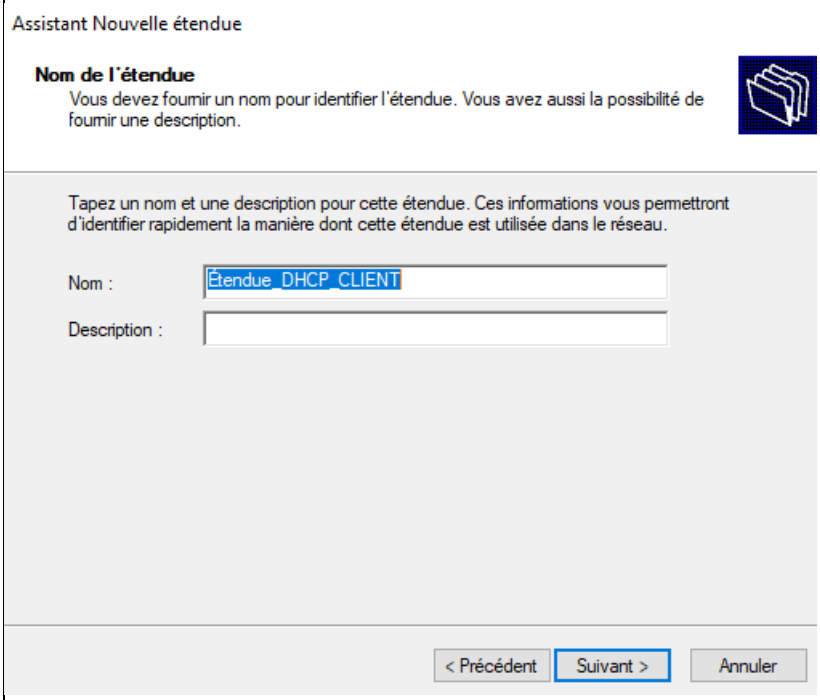
Une étendue DHCP correspond à une plage d'adresses IP qu'un serveur DHCP peut distribuer aux clients d'un sous-réseau donné. L'étendue a été créée pour le VLAN 3 (réseau clients Marseille, 192.168.3.0/24).

Création de l'étendue via la console DHCP :

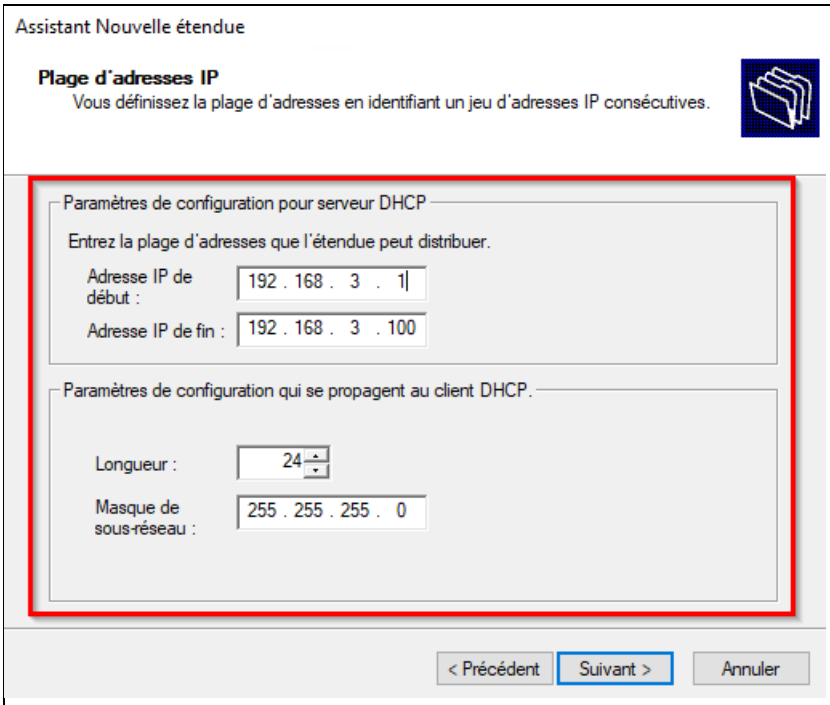
- Dans la console DHCP → IPv4 → clic droit → Nouvelle étendue,



- Nom de l'étendue : Étendue_DHCP_CLIENT,



- Adresse IP de début : 192.168.3.1,
- Adresse IP de fin : 192.168.3.100,
- Masque de sous-réseau : 255.255.255.0,



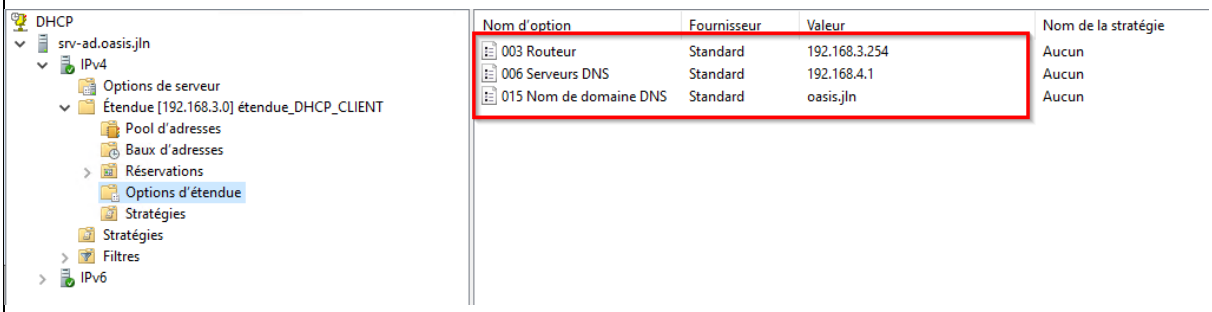
- Aucune plage d'exclusion (toutes les adresses du pool sont distribuables),
- Durée du bail : 8 jours (valeur par défaut conservée).

Étape 4 – Configuration des options de l'étendue

Les options DHCP permettent de distribuer aux clients, en même temps que leur adresse IP, des paramètres réseau supplémentaires indispensables au bon fonctionnement de leur connexion. Les options suivantes ont été configurées pour l'étendue 192.168.3.0 :

Configuration des options via la console DHCP :

- Dans la console DHCP → Étendue [192.168.3.0] → Options d'étendue → clic droit → Configurer les options,
- Option 003 (Routeur) : 192.168.3.254 → passerelle pfSense du VLAN 3, permettant aux clients d'atteindre les autres réseaux,
- Option 006 (Serveurs DNS) : 192.168.4.1 → SRV-AD, permettant aux clients de résoudre les noms du domaine oasis.jln et les noms Internet,
- Option 015 (Nom de domaine DNS) : oasis.jln → suffixe DNS distribué aux clients pour la résolution de noms courts.



Configuration équivalente via PowerShell :

```
# Option 003 – Passerelle
Set-DhcpServerv4OptionValue -ScopeId 192.168.3.0 -OptionId 3 -Value
192.168.3.254


# Option 006 – Serveur DNS
```

```
Set-DhcpServerv4OptionValue -ScopeId 192.168.3.0 -OptionId 6 -Value
192.168.4.1

# Option 015 – Suffixe DNS
Set-DhcpServerv4OptionValue -ScopeId 192.168.3.0 -OptionId 15 -Value
'oasis.jln'
```

Récapitulatif de la configuration complète de l'étendue :

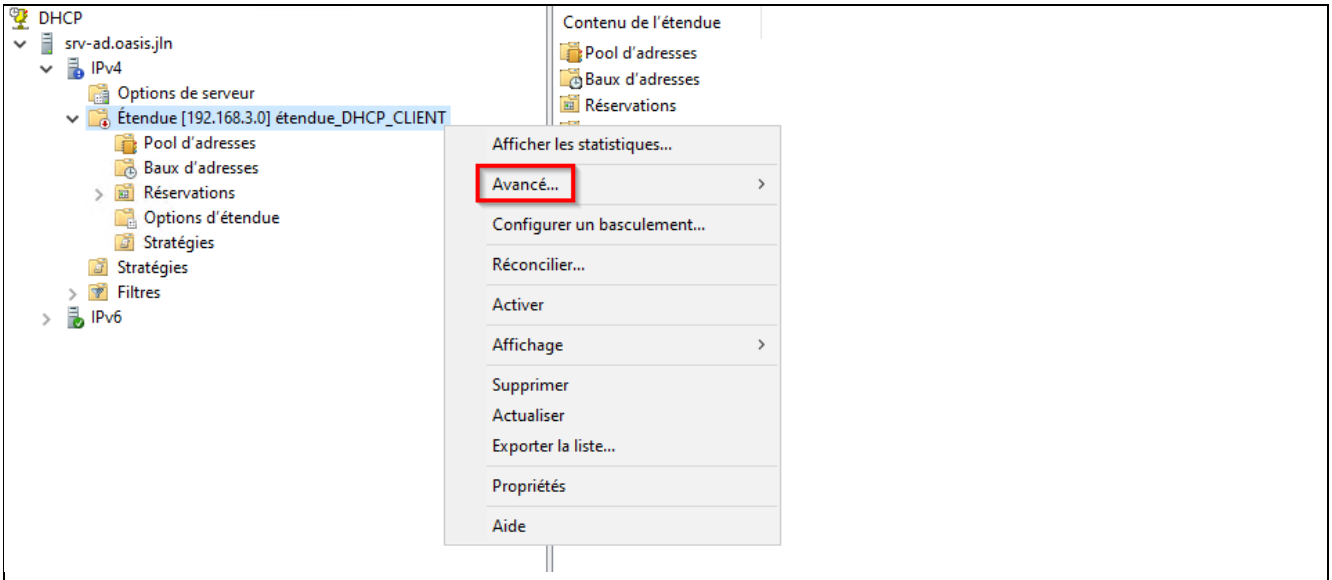
Paramètre	Valeur configurée	Rôle
Nom de l'étendue	Étendue_DHCP_CLIENT	Identification de l'étendue dans la console
Réseau concerné	192.168.3.0 / 255.255.255.0	VLAN 3 – Clients Marseille
Adresse de début	192.168.3.1	Première adresse du pool distribuable
Adresse de fin	192.168.3.100	Dernière adresse du pool distribuable
Masque de sous-réseau	255.255.255.0 (/24)	Masque distribué aux clients
Durée du bail	8 jours (valeur par défaut)	Durée pendant laquelle l'IP est réservée au client
Option 003 – Routeur	192.168.3.254 (pfSense)	Passerelle par défaut distribuée aux clients
Option 006 – DNS	192.168.4.1 (SRV-AD)	Serveur DNS distribué aux clients
Option 015 – Domaine	oasis.jln	Suffixe DNS distribué aux clients
Réservations	Aucune	Pas d'adresse réservée par adresse MAC
État de l'étendue	Active	L'étendue distribue des adresses

Étape 5 – Activation de l'étendue et vérification

Après la création et la configuration de l'étendue, celle-ci a été activée afin que le serveur DHCP commence à distribuer des adresses aux clients du VLAN 3.

Activation via la console DHCP :

- Clic droit sur l'étendue Étendue_DHCP_CLIENT → Activer,
- L'icône de l'étendue passe au vert, confirmant son activation.



Activation équivalente via PowerShell :

```
Set-DhcpServerv4Scope -ScopeId 192.168.3.0 -State Active
```

Vérification de la configuration complète de l'étendue :

```
Get-DhcpServerv4Scope -ScopeId 192.168.3.0
Get-DhcpServerv4OptionValue -ScopeId 192.168.3.0
```

Consultation des baux actifs (adresses distribuées aux clients connectés) :

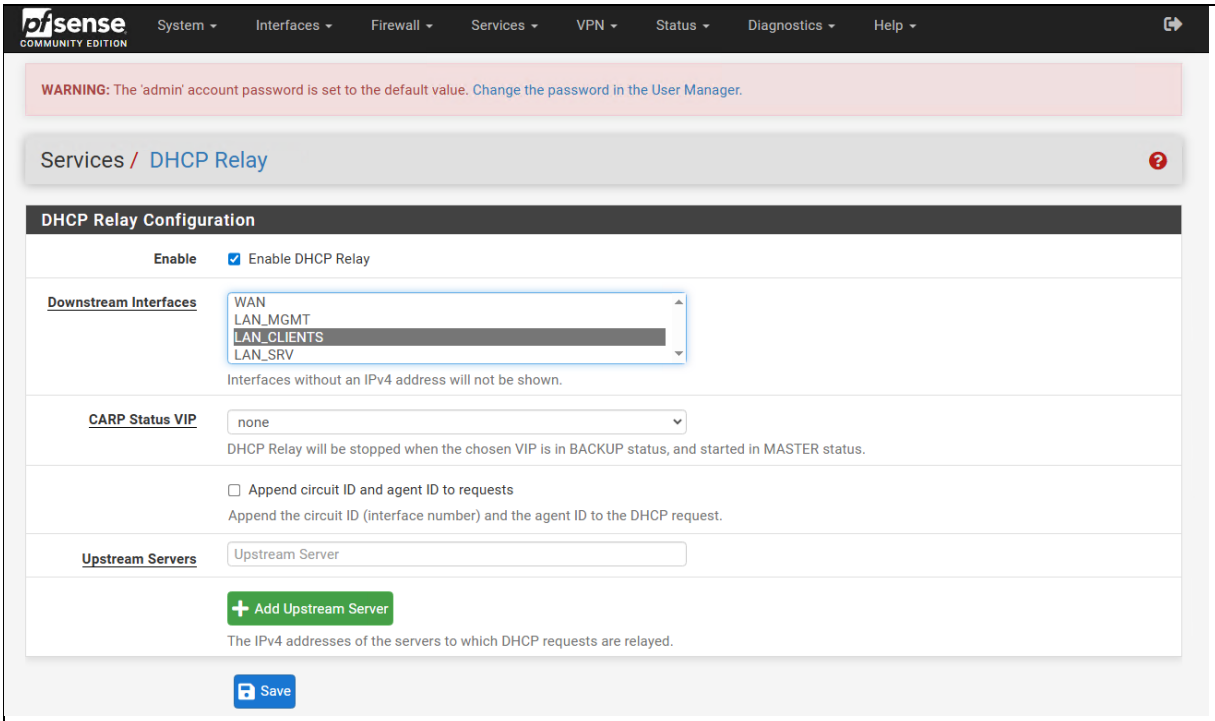
```
Get-DhcpServerv4Lease -ScopeId 192.168.3.0
```

Étape 6 – Règles de filtrage pfSense associées

Le serveur DHCP (SRV-AD, 192.168.4.1) est situé dans le VLAN 4, tandis que les clients sont dans le VLAN 3. Les requêtes DHCP étant des broadcasts, ils ne traversent pas naturellement les frontières de VLAN. pfSense a donc été configuré en tant qu'agent relais DHCP (DHCP Relay) pour retransmettre les requêtes des clients vers SRV-AD.

Configuration du relais DHCP sur pfSense :

- Interface web pfSense → Services → DHCP Relay,
- Activation du relais DHCP sur l'interface VLAN 3 (OPNsense_Client, 192.168.3.254),
- Serveur DHCP de destination : 192.168.4.1 (SRV-AD).



Règles de filtrage pfSense nécessaires au fonctionnement du DHCP :

N°	Source	Destination	Port	Proto	Description
1	192.168.3.0/24 (VLAN 3)	192.168.4.1 (SRV-AD)	67	UDP	Autoriser requêtes DHCP relayées par pfSense vers SRV-AD
2	192.168.4.1 (SRV-AD)	192.168.3.0/24 (VLAN 3)	68	UDP	Autoriser réponses DHCP de SRV-AD vers les clients
3	192.168.3.254 (pfSense)	192.168.4.1 (SRV-AD)	67	UDP	Autoriser le relais DHCP depuis pfSense vers SRV-AD

Ces règles garantissent que les échanges DHCP (DISCOVER, OFFER, REQUEST, ACK) peuvent transiter correctement entre le VLAN 3 et le VLAN 4 via pfSense, sans exposer le serveur DHCP à d'autres VLANs.

Tests

Les tests suivants ont été réalisés pour valider le bon fonctionnement du serveur DHCP et de la distribution d'adresses aux clients du VLAN 3 :

Test réalisé	Résultat attendu	Résultat obtenu	Statut
Vérification du service DHCP Server sur SRV-AD	Service démarré et en cours d'exécution	Status : Running	✓OK
Connexion d'un client sur le VLAN 3 (adresse DHCP)	Adresse IP attribuée dans la plage 192.168.3.1 – 192.168.3.100	IP 192.168.3.x attribuée	✓OK
Vérification du masque de sous-réseau reçu	255.255.255.0	255.255.255.0	✓OK

Vérification de la passerelle reçue (option 003)	192.168.3.254 (pfSense_Client)	192.168.3.254	✓OK
Vérification du serveur DNS reçu (option 006)	192.168.4.1 (SRV-AD)	192.168.4.1	✓OK
Vérification du suffixe DNS reçu (option 015)	oasis.jln	oasis.jln	✓OK
Ping depuis le client → passerelle 192.168.3.254	Réponse reçue	Reply from 192.168.3.254	✓OK
Ping depuis le client → SRV-AD 192.168.4.1	Réponse reçue (routage inter-VLAN)	Reply from 192.168.4.1	✓OK
Résolution DNS depuis le client (nslookup oasis.jln)	Résolution correcte via 192.168.4.1	Réponse DNS valide	✓OK
Vérification du bail dans la console DHCP (Baux d'adresses)	Bail visible avec l'IP et le nom du client	Bail présent	✓OK
Renouvellement du bail depuis le client (ipconfig /renew)	Même IP ou nouvelle IP attribuée dans la plage	IP renouvelée	✓OK
Libération du bail (ipconfig /release)	Adresse libérée, plus d'IP active	Bail libéré	✓OK

Conclusion

Cette mission m'a permis de déployer et de configurer un serveur DHCP complet sur Windows Server 2022, intégré au contrôleur de domaine Active Directory existant (SRV-AD, 192.168.4.1). J'ai mis en œuvre l'ensemble des étapes suivantes :

- Installation du rôle DHCP Server sur SRV-AD via le Gestionnaire de serveur,
- Autorisation du serveur DHCP dans l'Active Directory pour prévenir les serveurs DHCP non autorisés,
- Création de l'étendue Étendue_DHCP_CLIENT (192.168.3.1 – 192.168.3.100) pour le VLAN 3,
- Configuration des options de l'étendue : passerelle (192.168.3.254), DNS (192.168.4.1), suffixe DNS (oasis.jln),
- Activation de l'étendue et vérification des baux distribués dans la console DHCP,
- Configuration du relais DHCP sur pfSense et des règles de filtrage associées pour permettre la communication inter-VLAN entre les clients (VLAN 3) et le serveur DHCP (VLAN 4).

Les clients du VLAN 3 obtiennent désormais automatiquement leur configuration réseau complète dès leur connexion, garantissant un déploiement rapide et une gestion centralisée des adresses IP au sein de l'infrastructure du projet Oasis.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS — SESSION 2026

ANNEXE VII-7 : Modèle d'attestation de respect de l'annexe II.E – Environnement technologique pour la certification du référentiel

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

CONTRÔLE DE L'ENVIRONNEMENT TECHNOLOGIQUE

En référence à l'annexe II.E « Environnement technologique pour la certification » du référentiel du BTS SIO

Identification[1]	**Fab'Academy - Pôle formation UIMM // La Roche-Sur-Yon** **2543700461** **Julien VIAUD**	**SISR**

1. Environnement commun aux deux options

1.1 L'environnement technologique supportant le système d'information de l'organisation cliente comporte au moins :

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Un service d'authentification	Active Directory Domain Services (AD DS) sous Windows Server 2022.	
Un SGBD	MySQL (via MariaDB) - GLPI	
Un accès sécurisé à internet	Pare-feu matériel (Stormshield).	
Un environnement de travail collaboratif	Nextcloud	
Deux serveurs, éventuellement virtualisés, basés sur des systèmes d'exploitation différents, dont l'un est un logiciel libre (*open source)*	1. Windows Server 2022 (Propriétaire) 2. Debian 12 (*open source)*	

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Une solution de sauvegarde	Proxmox backup Serveur	
Des ressources dont l'accès est sécurisé et soumis à habilitation	Partage de fichier sur nexcloud via des droits affecter à l'utilisateur	
Deux types de terminaux dont un mobile (type *smartphone* ou encore tablette)	Pc portable -	

1.2 Des outils sont mobilisés pour la gestion de la sécurité :

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Gestion des incidents	GLPI	
Détection et prévention des intrusions	Filtrage via le par feu	
Chiffrement	Certificat via Active Directory Certificate Services (ADCS)	
Analyse de trafic	Wireshark	

Rappel : les logiciels de simulation ou d'émulation sont utilisés en réponse à des besoins de l'organisation. Ils ne peuvent se substituer complètement à des équipements réels dans l'environnement technologique d'apprentissage.

2. Éléments spécifiques à l'option « Solutions d'infrastructure, systèmes et réseaux » (SISR)

Rappel de l'annexe II.E du référentiel : « ***Une solution d'infrastructure réduite à une simulation par un logiciel ne peut être acceptée.*** »

2.1 L'environnement technologique supportant le système d'information de l'organisation cliente comporte au moins :

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Un réseau comportant plusieurs périmètres de sécurité	Segmentation VLAN	
Un service rendu à l'utilisateur final respectant un contrat de service comportant des contraintes en termes de sécurité et de haute disponibilité	Serveur lamp (Wordpress) + HA proxy	
Un logiciel d'analyse de trames	Wireshark.	
Un logiciel de gestion des configurations	GPO	
Une solution permettant l'administration à distance sécurisée de serveurs et de solutions techniques d'accès	RDP -->Le bastion	
Une solution permettant la supervision de la qualité, de la sécurité et de la disponibilité des équipements d'interconnexion, serveurs, systèmes et services avec remontées d'alertes	Serveur Zabbix avec agent	
Une solution garantissant des accès sécurisés à un service, internes au périmètre de sécurité de l'organisation (type intranet) ou externes (type internet ou extranet)	HTTPS (glpi)	
Éléments	**Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)**	**Remarques de la commission d'interrogation**
Une solution garantissant la continuité d'un service	HA proxy + rendondance des switchs + routeurs ha	
Une solution garantissant la tolérance de panne de systèmes serveurs ou d'éléments d'interconnexion	RAID 5 (minimum 3 disques) + rendondance des switchs + routeurs ha	
Une solution permettant la répartition de charges entre services, serveurs ou éléments d'interconnexion	Protocole HSRP + rendondance des switchs + routeurs ha	

2.2 La structure et les activités de l'organisation s'appuient sur au moins une solution d'infrastructure opérationnelle parmi les suivantes :

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Une solution permettant la connexion sécurisée entre deux sites distants	Un VPN ipsec	
Une solution permettant le déploiement des solutions techniques d'accès	Serveur Windows Deployment Services	
Une solution gérée à l'aide de procédures automatisées écrites avec un langage de *scripting*	Scripts GPO	
Une solution permettant la détection d'intrusions ou de comportements anormaux sur le réseau	IDS, syslog	