PAGE DE GARDE DU DOSSIER PROFESSIONNEL

BREVET DE TECHNICIEN SUPÉRIEUR
SERVICES INFORMATIQUES AUX ORGANISATIONS

Session 2026

DOSSIER PROFESSIONNEL

NOM : MANAC'H

Prénom : Titouan

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

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

Je soussigné, Manac'h, Titouan, 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 Nantes
Date 21/04/2026

Signature

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2026**

Fiche descriptive de réalisation professionnelle (recto)

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

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	**N° réalisation :**
Nom, prénom : MANAC'H Titouan	**N° candidat : 02542581894**
Épreuve ponctuelle ☐ **Contrôle en cours de formation** ☒	**Date :** 28 / 05 / 2026

Organisation support de la réalisation professionnelle
Entreprise fictive Oasis et prestataire Scylab

Intitulé de la réalisation professionnelle
Mise en place du DHCP Kea

Période de réalisation : *2024 - 2026* ***Lieu : CFA Fab'Academy Bouguenais (UIMM)***
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)
Mise en place d'une solution de DHCP dans l'infrastructure. Afin de répondre aux exigences de OASIS. La solution doit permettre d'assurer le DHCP de l'infrastructure virtualisée et sécurisée, des services essentiels

Description des ressources documentaires, matérielles et logicielles utilisées[2]
Serveurs HP, Proxmox, Kea, Machines Virtuelles clients, Pare-feux

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

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

L'ensemble des documents lié à l'infrastructure sont trouvables sur le site Easi, Cette outils fournit par la Fab'Academy nous sert à stocker nos sauvegardes et documentation sur un espace externe.

Une kdbx contenant les mots de passes est disponible sur la VM CLI-P-MGMT sur le site de Paris.

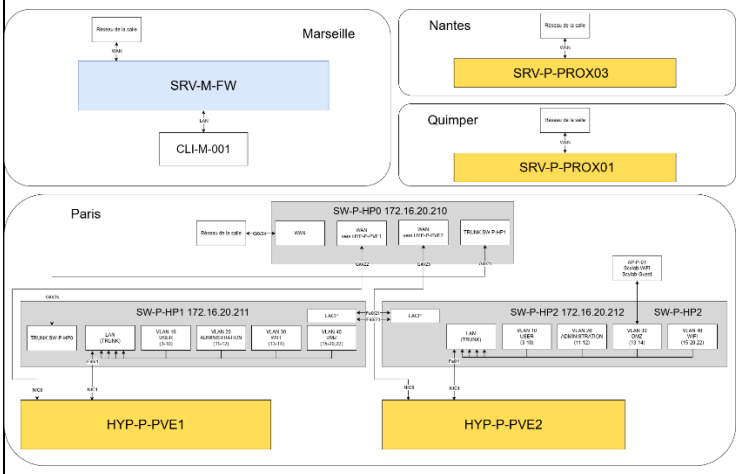
Mot de passe Keepass : Me*duse54-32

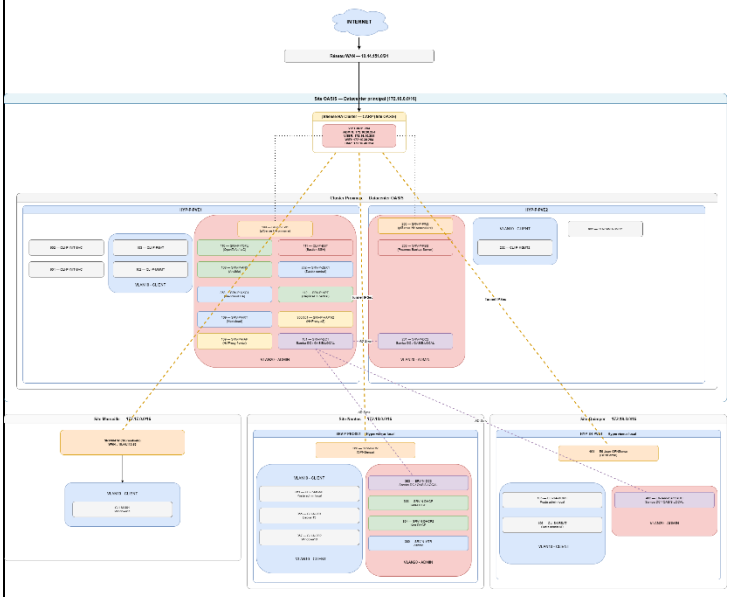
BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2026**

Fiche descriptive de réalisation professionnelle
(verso, éventuellement pages suivantes)

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

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





[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.

BTS Services informatiques aux organisations SESSION 2026
ANNEXE 10-A : Outil d'aide à l'appréciation de l'environnement technologique mobilisé par la personne candidate
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[5]		**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	**Samba AD**	
Un SGBD	**MariaDB**	
Un accès sécurisé à internet	**Firewall pfSense / OPNsense /Stormshieled**	
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)*	**Debian, Windows 11**	

[5] Nom et adresse du centre d'examen ou identification de la personne candidate individuelle (numéro, nom, prénom)

ANNEXE 10-A (suite) : 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)

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 Server	
Des ressources dont l'accès est sécurisé et soumis à habilitation	Nextcloud	
Deux types de terminaux dont un mobile (type *smartphone* ou encore tablette)	Tablette / PC Portable via connexion Wi-Fi	

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	Stormshield	
Chiffrement	SSH, IPsec	
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.

ANNEXE 10-A (suite) : 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)

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	Segmentations VLAN	
Un service rendu à l'utilisateur final respectant un contrat de service comportant des contraintes en termes de sécurité et de haute disponibilité	Nextcloud	
Un logiciel d'analyse de trames	Wireshark	
Un logiciel de gestion des configurations	Ansible	
Une solution permettant l'administration à distance sécurisée de serveurs et de solutions techniques d'accès	SSH	
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	Zabbix	
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)	Firewall OPNsense, pfSense	

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	**RAID 1, Proxmox Backup Server**	
Une solution garantissant la tolérance de panne de systèmes serveurs ou d'éléments d'interconnexion	**RAID 1**	
Une solution permettant la répartition de charges entre services, serveurs ou éléments d'interconnexion	**DHCP, DNS, OPNsense, pfSense (CARP)**	

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	**IPSec**	
Une solution permettant le déploiement des solutions techniques d'accès	**Ansible**	
Une solution gérée à l'aide de procédures automatisées écrites avec un langage de *scripting*	**Ansible**	
Une solution permettant la détection d'intrusions ou de comportements anormaux sur le réseau	**Stormshield**	

Table des matières

1. Rôle fonctionnel du DHCP

1.1 Qu'est-ce que le DHCP ?

Le protocole DHCP (Dynamic Host Configuration Protocol) est un service réseau fondamental qui automatise l'attribution des paramètres de configuration IP aux équipements d'un réseau. Sans lui, chaque poste, serveur ou périphérique devrait être configuré manuellement, ce qui devient rapidement ingérable à l'échelle d'une infrastructure d'entreprise.

1.2 Fonctionnement - Le mécanisme DORA

Lorsqu'un équipement se connecte au réseau, il émet une requête DHCP en broadcast. Le serveur DHCP lui propose une adresse IP disponible, le client accepte l'offre et le serveur confirme l'attribution. Ce mécanisme en 4 étapes, appelé DORA, garantit une attribution rapide et sans conflit d'adresses.

DHCPDISCOVER : Le client diffuse une requête sur le réseau pour localiser un serveur DHCP disponible.

DHCPOFFER : Le serveur propose une adresse IP disponible ainsi que les paramètres réseau associés.

DHCPREQUEST : Le client confirme son choix et demande officiellement l'adresse proposée.

DHCPACK : Le serveur valide l'attribution. Le client peut désormais utiliser l'adresse IP pour la durée du bail.

1.3 Ce que distribue un serveur DHCP

Au-delà de l'adresse IP, le serveur DHCP transmet l'ensemble des paramètres nécessaires à la connectivité des équipements :

- Adresse IP et masque de sous-réseau
- Passerelle par défaut (routeur)
- Serveurs DNS et suffixe de recherche DNS
- Nom de domaine de l'organisation
- Durée de validité du bail (renouvellement et libération automatiques)

1.4 DHCP dans une infrastructure multi-VLAN

Dans un environnement segmenté en VLANs, le serveur DHCP est centralisé et les équipements réseau (pare-feu, routeurs) assurent le relais DHCP (DHCP Relay) pour acheminer les requêtes des clients vers le bon serveur, même lorsqu'ils se trouvent sur des sous-réseaux différents. Sans ce mécanisme de relay, seul le sous-réseau directement connecté au serveur pourrait bénéficier du service DHCP.

1.5 Enjeux de disponibilité

Le service DHCP est critique pour l'infrastructure : une panne entraîne l'impossibilité pour les nouveaux équipements d'obtenir une adresse IP, paralysant leur accès au réseau. Les équipements déjà connectés conservent leur bail jusqu'à son expiration, mais tout nouvel équipement ou toute reconnexion sera bloqué. C'est pourquoi les infrastructures professionnelles exigent une haute disponibilité du service DHCP, avec redondance des serveurs et synchronisation des baux en temps réel.

2. Étude des solutions DHCP

2.1 Critères d'évaluation

Les solutions DHCP ont été évaluées selon les critères suivants :

- Open Source ou sous-licence
- Support de la haute disponibilité
- Flexibilité du stockage des baux (fichier, base de données)
- Complexité de mise en œuvre et de maintenance

2.2 Tableau comparatif

Solution	Open Source	Haute Dispo.	Stockage baux	Complexité	Coût
ISC DHCP	Oui	Répartition de charge (IPv4 uniquement)	Fichier	Faible	Aucun
Dnsmasq	Oui	Non	Mémoire / Fichier	Très faible	Aucun
Kea DHCP	Oui	Répartition de charge **ou** Veille active	Fichier / MySQL / PostgreSQL	Moyen	Aucun
Windows Server DHCP	Non	Répartition de charge **ou** Veille active	Base de données Windows	Moyen	Élevé

2.3 Analyse des solutions

ISC DHCP

Historiquement la référence des serveurs DHCP sous Linux, ISC DHCP est aujourd'hui déclaré en fin de vie par l'ISC (fin de support en 2022). Sa prise en charge de la répartition de charge reste limitée à l'IPv4 et son architecture monolithique ne permet pas d'API REST native. Il n'est plus recommandé pour de nouveaux déploiements.

Dnsmasq

Solution légère intégrant DNS et DHCP, Dnsmasq est adaptée aux petits réseaux mais ne propose aucun mécanisme de haute disponibilité ni d'API. Son utilisation est à réserver aux infrastructures simples ne nécessitant pas de redondance.

Windows Server DHCP

Le service DHCP intégré à Windows Server propose un basculement automatique natif, avec choix entre répartition de charge et veille active, ainsi qu'une administration graphique. Il implique toutefois une licence Microsoft, une dépendance à l'environnement Active Directory et ne s'intègre pas nativement à une infrastructure Linux/Open Source.

Kea DHCP (ISC)

Successeur officiel d'ISC DHCP, Kea propose une architecture modulaire moderne avec prise en charge native de la répartition de charge et de la veille active, une API REST complète, un stockage flexible des baux et une communauté active. Il s'impose comme la solution de référence pour les infrastructures Linux modernes nécessitant haute disponibilité et supervision avancée.

3. Solution DHCP retenue : Kea DHCP

Solution retenue
ISC Kea DHCP déployé en mode Load Balancing (haute disponibilité active/active) sur deux serveurs Debian dédiés, placés dans le VLAN 20 (172.18.20.0/24).

3.1 Justification du choix

- Open Source, activement maintenu par l'ISC, c'est le successeur officiel d'ISC DHCP
- Haute disponibilité native : modes load-balancing et hot-standby avec failover automatique
- API REST intégrée (Control Agent) : supervision et gestion sans redémarrage du service
- Multi-threading activé : performances optimales sur serveurs multicœurs
- Stockage des baux en fichier CSV (memfile) avec nettoyage automatique (LFC)
- Support des réservations statiques par adresse MAC
- Compatible avec les relais DHCP des pare-feux (OPNsense, pfSense)

3.2 Présentation de Kea DHCP

Kea DHCP est un serveur DHCP nouvelle génération développé et maintenu par l'Internet Systems Consortium (ISC), successeur officiel d'ISC DHCP (dhcpd). Conçu dès l'origine pour les environnements de production modernes, Kea apporte une architecture modulaire, une API REST intégrée et des mécanismes natifs de haute disponibilité.

3.3 Fonctions principales

Kea DHCP remplit les rôles suivants au sein de l'infrastructure réseau :

- Attribution dynamique d'adresses IP : distribution automatique d'adresses IP aux hôtes du réseau selon des plages configurées (pools).
- Gestion des baux (leases) : contrôle de la durée de validité des adresses attribuées, renouvellement (renew) et rebind automatiques.
- Réservations statiques : association permanente d'une adresse IP à une adresse MAC, garantissant une adresse fixe à certains équipements.
- Distribution des options DHCP : transmission des paramètres réseau complémentaires (passerelle par défaut, serveurs DNS, nom de domaine, suffixe de recherche DNS).
- Support multi-sous-réseaux : gestion simultanée de plusieurs sous-réseaux et VLANs depuis une configuration centralisée.
- Haute disponibilité (HA) : synchronisation des baux entre serveurs primaire et secondaire, avec basculement automatique en cas de défaillance.
- API REST de contrôle (Control Agent) : interface HTTP/JSON permettant la supervision, la gestion des baux et le rechargement de configuration sans redémarrage.
- Journalisation et statistiques : production de logs détaillés et de métriques accessibles via l'API pour la supervision.

3.4 Modes de haute disponibilité

Mode Standalone

Le serveur DHCP fonctionne de manière autonome, sans redondance. Il est le seul responsable de l'attribution des adresses IP. Ce mode convient aux environnements de petite taille ou aux labs, mais n'offre aucune tolérance aux pannes.

Mode Load Balancing

Les deux serveurs sont actifs simultanément. Le pool d'adresses est divisé en deux partitions (split 128 par défaut), chaque serveur traite la moitié des requêtes. En cas de défaillance d'un serveur, l'autre prend en charge l'intégralité des requêtes automatiquement (auto-failover).

Mode Hot-Standby

Le serveur primaire traite toutes les requêtes, le secondaire reste en veille et synchronise ses baux en temps réel. En cas de défaillance du primaire, le secondaire prend le relais automatiquement. Ce mode est plus simple mais n'utilise pas les ressources du secondaire en fonctionnement normal.

3.5 Plan d'adressage

Rôle	VLAN	Réseau	Passerelle	Remarque
DHCP	VLAN 20	172.18.20.0/24	172.18.20.254	Serveurs Kea
USERS	VLAN 10	172.18.10.0/24	172.18.10.254	Clients DHCP

4. Prérequis à la mise en place de Kea DHCP

4.1 Prérequis matériels et systèmes

- Deux serveurs (physiques ou virtuels) sous Debian 13
- Au minimum 1 vCPU et 512 Mo de RAM par serveur (recommandé : 2 vCPU / 2 Go RAM)
- Interface réseau connectée au VLAN 20 (réseau dédié DHCP : 172.18.20.0/24)
- Accès Internet ou dépôts APT disponibles pour l'installation des paquets
- Accès SSH avec privilèges root ou sudo sur les deux serveurs

4.2 Prérequis réseau

- VLAN 20 opérationnel et routé : les serveurs DHCP doivent être joignables depuis le pare-feu
- Relais DHCP sur le pare-feu autorisant le trafic DHCP (UDP 67/68) entre le VLAN client et les serveurs Kea
- Communication HTTP entre les deux serveurs Kea sur le port 8001 (synchronisation HA)
- Communication HTTP entre le Control Agent et les outils de supervision sur le port 8000
- Résolution DNS fonctionnelle pour le domaine oasis.local (172.18.20.1)

4.3 Prérequis logiciels

- Paquets requis : kea-dhcp4-server, kea-ctrl-agent
- Synchronisation NTP active sur les deux serveurs (recommandé pour la cohérence des baux HA)

4.4 Informations à préparer

Paramètre	Valeur
IP Serveur DHCP 1	172.18.20.20
IP Serveur DHCP 2	172.18.20.21
Passerelle VLAN 20	172.18.20.254
Serveur DNS	172.18.20.1
Domaine	oasis.local
Sous-réseau USERS	172.18.10.0/24 - pool 172.18.10.100-200
Port Control Agent	8000 (HTTP REST)
Port HA (synchronisation)	8001 (HTTP entre serveurs Kea)
Durée bail DHCP	3600 secondes (1 heure)

5. Mise en place de Kea DHCP

5.1 Préparation des serveurs

Effectuer les opérations suivantes sur les deux serveurs (DHCP1 et DHCP2) :

Configuration de l'interface réseau

1. Ouvrir le fichier de configuration réseau :

```
nano /etc/network/interfaces
```

2. Configurer l'interface (exemple pour DHCP1) :

```
auto ens18
iface ens18 inet static
    address 172.18.20.20
    netmask 255.255.255.0
    gateway 172.18.20.254
```

3. Redémarrer le service réseau :

```
systemctl restart networking
```

Mise à jour du système et installation de Kea

```
apt update && apt upgrade -y
apt install -y kea-dhcp4-server kea-ctrl-agent
```

Sauvegarde des fichiers de configuration originaux

```
cp /etc/kea/kea-dhcp4.conf /etc/kea/kea-dhcp4.conf.bak
cp /etc/kea/kea-ctrl-agent.conf /etc/kea/kea-ctrl-agent.conf.bak
```

Préparation du répertoire et du fichier de baux

```
# Créer le fichier de baux (sécurité, Kea peut le créer seul mais pas toujours)
touch /var/lib/kea/kea-leases4.csv
chown _kea:_kea /var/lib/kea/kea-leases4.csv
chmod 0644 /var/lib/kea/kea-leases4.csv

# Restreindre l'accès au fichier de configuration (bonne pratique)
```

```
chown root:_kea /etc/kea/kea-dhcp4.conf
chmod 0640 /etc/kea/kea-dhcp4.conf

# Vérification de la lisibilité par l'utilisateur _kea
su -s /bin/sh -c 'head -n 5 /etc/kea/kea-dhcp4.conf' _kea
```

5.2 Configuration du serveur DHCP

5.2.1 Configuration DHCP - Mode Standalone

Éditer le fichier /etc/kea/kea-dhcp4.conf et remplacer son contenu par :

```
nano /etc/kea/kea-dhcp4.conf
```

```
{
  "Dhcp4": {
    "interfaces-config": {
      "interfaces": [ "ens18" ],
      "dhcp-socket-type": "udp"
    },

    "control-socket": {
      "socket-type": "unix",
      "socket-name": "/run/kea/kea4-ctrl-socket"
    },

    "multi-threading": {
      "enable-multi-threading": true,
      "thread-pool-size": 4,
      "packet-queue-size": 64
    },

    "lease-database": {
      "type": "memfile",
      "name": "/var/lib/kea/kea-leases4.csv",
      "persist": true,
      "lfc-interval": 3600
    },

    "expired-leases-processing": {
      "reclaim-timer-wait-time": 10,
      "flush-reclaimed-timer-wait-time": 25,
      "hold-reclaimed-time": 3600,
      "max-reclaim-leases": 100,
      "max-reclaim-time": 250
    },

    "renew-timer": 1800,
    "rebind-timer": 3150,
```

```
    "valid-lifetime": 3600,

    "option-data": [
      { "name": "domain-name",         "data": "oasis.local" },
      { "name": "domain-name-servers", "data": "172.18.20.1" },
      { "name": "domain-search",       "data": "oasis.local" }
    ],

    "subnet4": [
      {
        "id": 10,
        "subnet": "172.18.10.0/24",
        "pools": [
          { "pool": "172.18.10.100-172.18.10.200" }
        ],
        "option-data": [
          { "name": "routers", "data": "172.18.10.254" }
        ],
        "relay": {
          "ip-addresses": [ "172.18.10.254" ]
        },
        "reservations": [
          {
            "hw-address": "AA:BB:CC:DD:EE:FF",
            "ip-address": "172.18.10.101",
            "hostname": "mon-client"
          }
        ]
      }
    ],

    "loggers": [
      {
        "name": "kea-dhcp4",
        "output-options": [
          {
            "output": "syslog",
            "pattern": "%-5p %m\n"
          }
        ],
        "severity": "INFO",
        "debuglevel": 0
      }
    ]
  }
}
```

5.2.2 Configuration DHCP1 - Mode Load Balancing

Éditer le fichier /etc/kea/kea-dhcp4.conf et remplacer son contenu par :

```
nano /etc/kea/kea-dhcp4.conf
```

```
{
  "Dhcp4": {
    "interfaces-config": {
      "interfaces": [ "ens18" ],
      "dhcp-socket-type": "udp"
    },

    "control-socket": {
      "socket-type": "unix",
      "socket-name": "/run/kea/kea4-ctrl-socket"
    },

    "multi-threading": {
      "enable-multi-threading": true,
      "thread-pool-size": 4,
      "packet-queue-size": 64
    },

    "hooks-libraries": [
      {
        "library": "/usr/lib/x86_64-linux-gnu/kea/hooks/libdhcp_lease_cmds.so"
      },
      {
        "library": "/usr/lib/x86_64-linux-gnu/kea/hooks/libdhcp_ha.so",
        "parameters": {
          "high-availability": [
            {
              "this-server-name": "dhcp1",
              "mode": "load-balancing",

              "multi-threading": {
                "enable-multi-threading": true,
                "http-dedicated-listener": true,
                "http-listener-threads": 0,
                "http-client-threads": 0
              },

              "heartbeat-delay": 10000,
              "max-response-delay": 60000,
              "max-ack-delay": 5000,
              "max-unacked-clients": 10,

              "peers": [
                {
```

```
            "name": "dhcp1",
            "url": "http://172.18.20.20:8001/",
            "role": "primary",
            "auto-failover": true
           },
           {
            "name": "dhcp2",
            "url": "http://172.18.20.21:8001/",
            "role": "secondary",
            "auto-failover": true
           }
         ]
       }
     ]
   }
  }
],

"lease-database": {
  "type": "memfile",
  "name": "/var/lib/kea/kea-leases4.csv",
  "persist": true,
  "lfc-interval": 3600
},

"expired-leases-processing": {
  "reclaim-timer-wait-time": 10,
  "flush-reclaimed-timer-wait-time": 25,
  "hold-reclaimed-time": 3600,
  "max-reclaim-leases": 100,
  "max-reclaim-time": 250
},

"renew-timer": 1800,
"rebind-timer": 3150,
"valid-lifetime": 3600,

"option-data": [
  { "name": "domain-name",        "data": "oasis.local" },
  { "name": "domain-name-servers", "data": "172.18.20.1" },
  { "name": "domain-search",       "data": "oasis.local" }
],

"subnet4": [
  {
    "id": 10,
    "subnet": "172.18.10.0/24",
    "pools": [ { "pool": "172.18.10.100-172.18.10.200" } ],
    "option-data": [ { "name": "routers", "data": "172.18.10.254" } ],
    "relay": { "ip-addresses": [ "172.18.10.254" ] },
```

```
      "reservations": [
       {
        "hw-address": "AA:BB:CC:DD:EE:FF",
        "ip-address": "172.18.10.101",
        "hostname": "mon-client"
       }
      ]
     }
    ],

    "loggers": [
     {
      "name": "kea-dhcp4",
      "output-options": [ { "output": "syslog", "pattern": "%-5p %m\n" } ],
      "severity": "INFO",
      "debuglevel": 0
     }
    ]
   }
}
```

DHCP2
Utiliser la même configuration en remplaçant uniquement : "this-server-name": "dhcp2"

5.2.3 Configuration DHCP1 - Mode Hot Standby

Éditer le fichier /etc/kea/kea-dhcp4.conf et remplacer son contenu par :

```
nano /etc/kea/kea-dhcp4.conf
```

```
{
  "Dhcp4": {
    "interfaces-config": {
      "interfaces": [ "ens18" ],
      "dhcp-socket-type": "udp"
    },

    "control-socket": {
      "socket-type": "unix",
      "socket-name": "/run/kea/kea4-ctrl-socket"
    },

    "multi-threading": {
      "enable-multi-threading": true,
      "thread-pool-size": 4,
      "packet-queue-size": 64
    },

    "hooks-libraries": [
      {
        "library": "/usr/lib/x86_64-linux-gnu/kea/hooks/libdhcp_lease_cmds.so"
      },
      {
        "library": "/usr/lib/x86_64-linux-gnu/kea/hooks/libdhcp_ha.so",
        "parameters": {
          "high-availability": [
            {
              "this-server-name": "dhcp1",
              "mode": "hot-standby",

              "multi-threading": {
                "enable-multi-threading": true,
                "http-dedicated-listener": true,
                "http-listener-threads": 0,
                "http-client-threads": 0
              },

              "heartbeat-delay": 10000,
              "max-response-delay": 60000,
              "max-ack-delay": 5000,
              "max-unacked-clients": 10,

              "peers": [
                {
```

```
            "name": "dhcp1",
            "url": "http://172.18.20.20:8001/",
            "role": "primary",
            "auto-failover": true
           },
           {
            "name": "dhcp2",
            "url": "http://172.18.20.21:8001/",
            "role": "standby",
            "auto-failover": true
           }
          ]
         }
        ]
      }
    }
],

"lease-database": {
  "type": "memfile",
  "name": "/var/lib/kea/kea-leases4.csv",
  "persist": true,
  "lfc-interval": 3600
},

"expired-leases-processing": {
  "reclaim-timer-wait-time": 10,
  "flush-reclaimed-timer-wait-time": 25,
  "hold-reclaimed-time": 3600,
  "max-reclaim-leases": 100,
  "max-reclaim-time": 250
},

"renew-timer": 1800,
"rebind-timer": 3150,
"valid-lifetime": 3600,

"option-data": [
  { "name": "domain-name",        "data": "oasis.local" },
  { "name": "domain-name-servers", "data": "172.18.20.1" },
  { "name": "domain-search",       "data": "oasis.local" }
],

"subnet4": [
  {
    "id": 10,
    "subnet": "172.18.10.0/24",
    "pools": [ { "pool": "172.18.10.100-172.18.10.200" } ],
    "option-data": [ { "name": "routers", "data": "172.18.10.254" } ],
    "relay": { "ip-addresses": [ "172.18.10.254" ] },
```

```
      "reservations": [
       {
        "hw-address": "AA:BB:CC:DD:EE:FF",
        "ip-address": "172.18.10.101",
        "hostname": "mon-client"
       }
      ]
     }
    ],

    "loggers": [
     {
      "name": "kea-dhcp4",
      "output-options": [ { "output": "syslog", "pattern": "%-5p %m\n" } ],
      "severity": "INFO",
      "debuglevel": 0
     }
    ]
   }
}
```

DHCP2
Utiliser la même configuration en remplaçant uniquement : "this-server-name": "dhcp2"

5.2.4 Réservation statique

La configuration inclut une réservation statique pour un client connu :

Adresse MAC	IP réservée	Hostname	VLAN
AA:BB:CC:DD:EE:FF	172.18.10.101	mon-client	VLAN 10 / USERS

5.3 Configuration du Control Agent

Éditer le fichier /etc/kea/kea-ctrl-agent.conf sur chaque serveur :

```
nano /etc/kea/kea-ctrl-agent.conf
```

```
{
  "Control-agent": {
    "http-host": "172.18.20.20",
    "http-port": 8000,

    "control-sockets": {
      "dhcp4": {
        "socket-type": "unix",
        "socket-name": "/run/kea/kea4-ctrl-socket"
      }
    },

    "loggers": [
      {
        "name": "kea-ctrl-agent",
        "output-options": [
          {
            "output": "syslog",
            "pattern": "%-5p %m\n"
          }
        ],
        "severity": "INFO",
        "debuglevel": 0
      }
    ]
  }
}
```

> **Note**
> Sur DHCP2, modifier la valeur http-host en "172.18.20.21".

5.4 Démarrage et activation des services

```
# Activer les services au démarrage
systemctl enable kea-dhcp4-server kea-ctrl-agent

# Démarrer les services
systemctl start kea-dhcp4-server kea-ctrl-agent

# Vérifier le statut
systemctl status kea-dhcp4-server kea-ctrl-agent
```

5.5 Alias de commandes Kea (optionnel)

Pour simplifier l'administration via l'API, il est recommandé d'ajouter la fonction suivante dans /root/.bashrc :

```
nano /root/.bashrc

# Fonction kea - wrapper API REST
kea() {
    local cmd=$1; shift
    if [ $# -gt 0 ]; then
        echo "$@" | kea-shell --host 172.18.20.20 --port 8000 --service dhcp4
"$cmd" | python3 -m json.tool
    else
        kea-shell --host 172.18.20.20 --port 8000 --service dhcp4 "$cmd" <
/dev/null | python3 -m json.tool
    fi
}

# Recharger le bashrc
source ~/.bashrc
```

Exemples d'utilisation (cf. Annexes) :

```
kea status-get          # Statut du service + état HA
kea version-get         # Version Kea chargée
kea config-get          # Configuration active
kea config-reload       # Rechargement sans redémarrage
kea lease4-get-all      # Liste tous les baux actifs
kea ha-heartbeat        # Test de communication HA
kea ha-sync             # Synchronisation manuelle des baux
```

5.6 Migration du stockage des baux vers MySQL

Par défaut, Kea stocke les baux dans un fichier CSV (memfile), ce qui est largement suffisant pour une infrastructure de taille moyenne. Il est cependant possible de migrer vers une base de données MySQL/MariaDB, notamment pour bénéficier d'une consultation SQL native des baux ou d'une base partagée entre plusieurs serveurs Kea.

5.6.1 Installation des dépendances

```
apt install -y kea-admin mariadb-server
```

5.6.2 Création de la base de données

```
# Se connecter à MariaDB en root
mysql -u root -p

CREATE DATABASE kea;
CREATE USER 'kea'@'localhost' IDENTIFIED BY 'motdepasse';
GRANT ALL PRIVILEGES ON kea.* TO 'kea'@'localhost';
FLUSH PRIVILEGES;
```

5.6.3 Initialisation du schéma Kea

La commande kea-admin crée automatiquement toutes les tables nécessaires dans la base:

```
kea-admin db-init mysql -u kea -p motdepasse -n kea
```

5.6.4 Modification de la configuration Kea

Dans /etc/kea/kea-dhcp4.conf, remplacer le bloc lease-database existant par :

```
"lease-database": {
  "type":     "mysql",
  "host":     "localhost",
  "name":     "kea",
  "user":     "kea",
  "password": "motdepasse"
}
```

5.6.5 Redémarrage et vérification

```
systemctl restart kea-dhcp4-server
systemctl status kea-dhcp4-server

# Vérifier que les baux sont bien dans MySQL
kea lease4-get-all
```

6. Configuration du DHCP Relay sur OPNsense

Le DHCP Relay permet au pare-feu OPNsense de relayer les requêtes DHCP provenant du VLAN client (VLAN 10 USERS) vers les serveurs Kea situés dans le VLAN 20. Sans ce mécanisme, les clients du VLAN isolé ne pourraient pas obtenir d'adresse IP.

> **Principe du DHCP Relay**
> Les requêtes DHCP (broadcast) émises par les clients sont interceptées par OPNsense sur chaque interface VLAN client. OPNsense les convertit en requêtes unicast et les transmet aux serveurs Kea (172.18.20.20 et 172.18.20.21). Les réponses DHCP sont renvoyées aux clients via le même mécanisme.

6.1 Accès à la configuration DHCRelay

1. Se connecter à l'interface web d'OPNsense
2. Naviguer dans le menu : Services → DHCRelay → Configuration

6.2 Création du serveur de destination

3. Dans la section Destinations, cliquer sur le bouton + pour ajouter un nouveau serveur de destination
4. Renseigner les paramètres suivants dans la fenêtre « Edit DHCP destination » :

Champ	Valeur
Name	SRV-N-DHCP
Server	172.18.20.20 et 172.18.20.21

5. Cliquer sur Save pour enregistrer le serveur de destination

6.3 Création des règles de relay

Pour chaque VLAN client devant obtenir des adresses DHCP, créer une règle de relay :

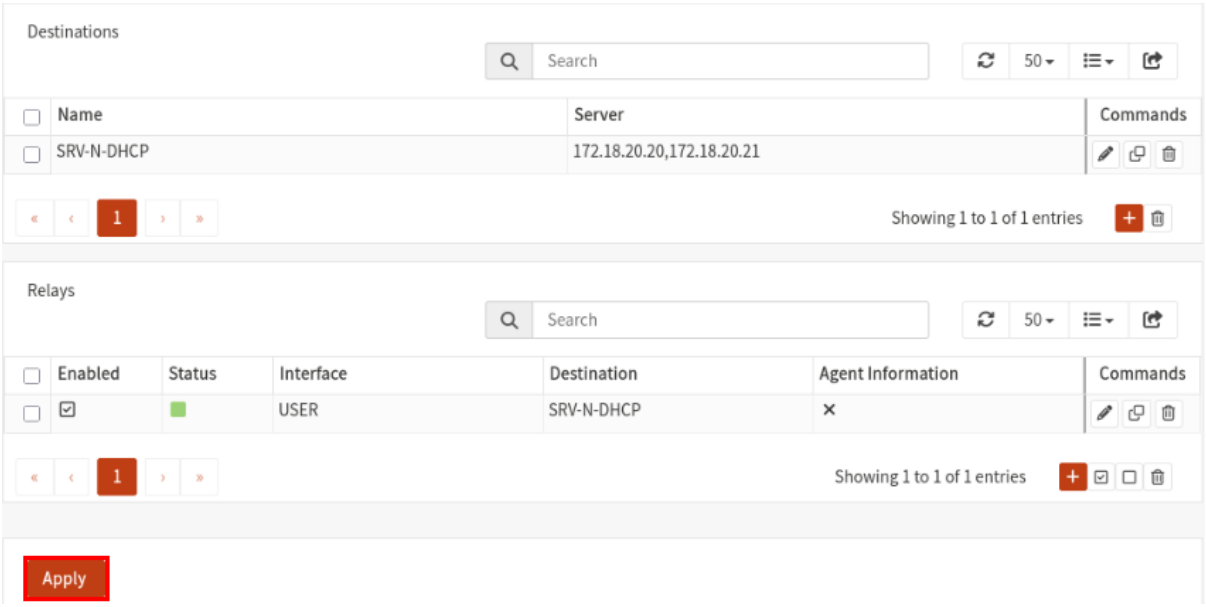
6. Dans la section Relays, cliquer sur + pour ajouter une nouvelle règle
7. Renseigner les paramètres suivants :

Champ	VLAN 10 - USERS
Enabled	Coché
Interface	USER (VLAN 10)
Destination	SRV-N-DHCP
Agent Info	Décoché
Depend CARP	None

8. Cliquer sur Save pour chaque règle
9. Cliquer sur Apply pour appliquer toutes les modifications

6.4 Vérification du relay

Après application, le tableau de relays doit afficher un statut vert (actif) pour chaque interface configurée : Interface USER → Destination SRV-N-DHCP → Statut : (vert)

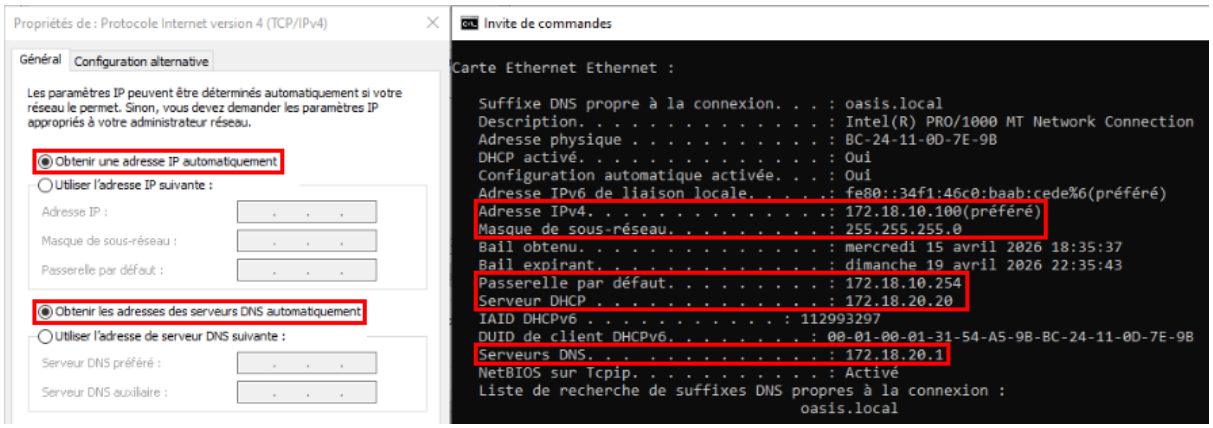


7. Vérification de l'attribution des baux

7.1 Vérification sur un client Windows

1. Ouvrir la boîte Exécuter (WIN + R) et saisir ncpa.cpl
2. Clic droit sur l'interface réseau → Propriétés → Protocole Internet version 4 → Propriétés
3. Vérifier que « Obtenir une adresse IP automatiquement » est coché
4. Ouvrir l'invite de commande et exécuter : ipconfig /all

Vérifier que l'adresse IP est dans la plage attendue et que le serveur DHCP indiqué est 172.18.20.20 ou .21.



7.2 Vérification sur un client Linux

```
# Capturer le trafic DHCP sur l'interface
tcpdump -i ens18 -nn -vv port 67 or port 68

# Dans un second terminal : recycler l'interface
ip link set ens18 down && ip link set ens18 up
```

```
root@CLI-N-001:~# tcpdump -i ens18 port 67 or port 68 -vv
tcpdump: listening on ens18, link-type EN10MB (Ethernet), snapshot length 262144 bytes
19:03:28.965407 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto UDP (17), length 321)
    0.0.0.0.bootpc > 255.255.255.255.bootps: [udp sum ok] BOOTP/DHCP, Request from bc:24:11:92:e2:f1 (oui Unknown), length 293, xid 0x7e46e
e74, secs 1, Flags [none] (0x0000)
          Client-Ethernet-Address bc:24:11:92:e2:f1 (oui Unknown)
          Vendor-rfc1048 Extensions
            Magic Cookie 0x63825363
            DHCP-Message (53), length 1: Request
            Client-ID (61), length 7: ether bc:24:11:92:e2:f1
            Parameter-Request (55), length 17:
              Subnet-Mask (1), Time-Zone (2), Domain-Name-Server (6), Hostname (12)
              Domain-Name (15), MTU (26), BR (28), Classless-Static-Route (121)
              Default-Gateway (3), Static-Route (33), YD (40), YS (41)
              NTP (42), Unknown (119), Classless-Static-Route-Microsoft (249), Unknown (252)
              RP (17)
            MSZ (57), length 2: 576
            Requested-IP (50), length 4: 172.18.10.102
            Hostname (12), length 9: "CLI-N-001"
19:03:29.968596 IP (tos 0x10, ttl 16, id 0, offset 0, flags [none], proto UDP (17), length 362)
    172.18.10.254.bootps > 172.18.10.102.bootpc: [udp sum ok] BOOTP/DHCP, Reply, length 334, hops 1, xid 0x7e46ee74, Flags [none] (0x0000)
          Your-IP 172.18.10.102
          Client-Ethernet-Address bc:24:11:92:e2:f1 (oui Unknown)
          Vendor-rfc1048 Extensions
            Magic Cookie 0x63825363
            DHCP-Message (53), length 1: ACK
            Subnet-Mask (1), length 4: 255.255.255.0
            Default-Gateway (3), length 4: 172.18.10.254
            Domain-Name-Server (6), length 4: 172.18.20.1
            Hostname (12), length 9: "cli-n-001"
            Domain-Name (15), length 11: "oasis.local"
            Lease-Time (51), length 4: 3600
            Server-ID (54), length 4: 172.18.20.20
            RN (58), length 4: 900
            RB (59), length 4: 1800
            Client-ID (61), length 7: ether bc:24:11:92:e2:f1
```

8. Améliorations

Voici quelques améliorations possibles pour ce projet :

- Mettre en place des alertes en cas d'épuisement d'un pool d'adresses.
- Coupler Kea avec BIND9 ou PowerDNS pour mettre à jour automatiquement les enregistrements DNS lors de l'attribution d'une IP (DDNS)
- Audit et traçabilité des attributions

9. Conclusion

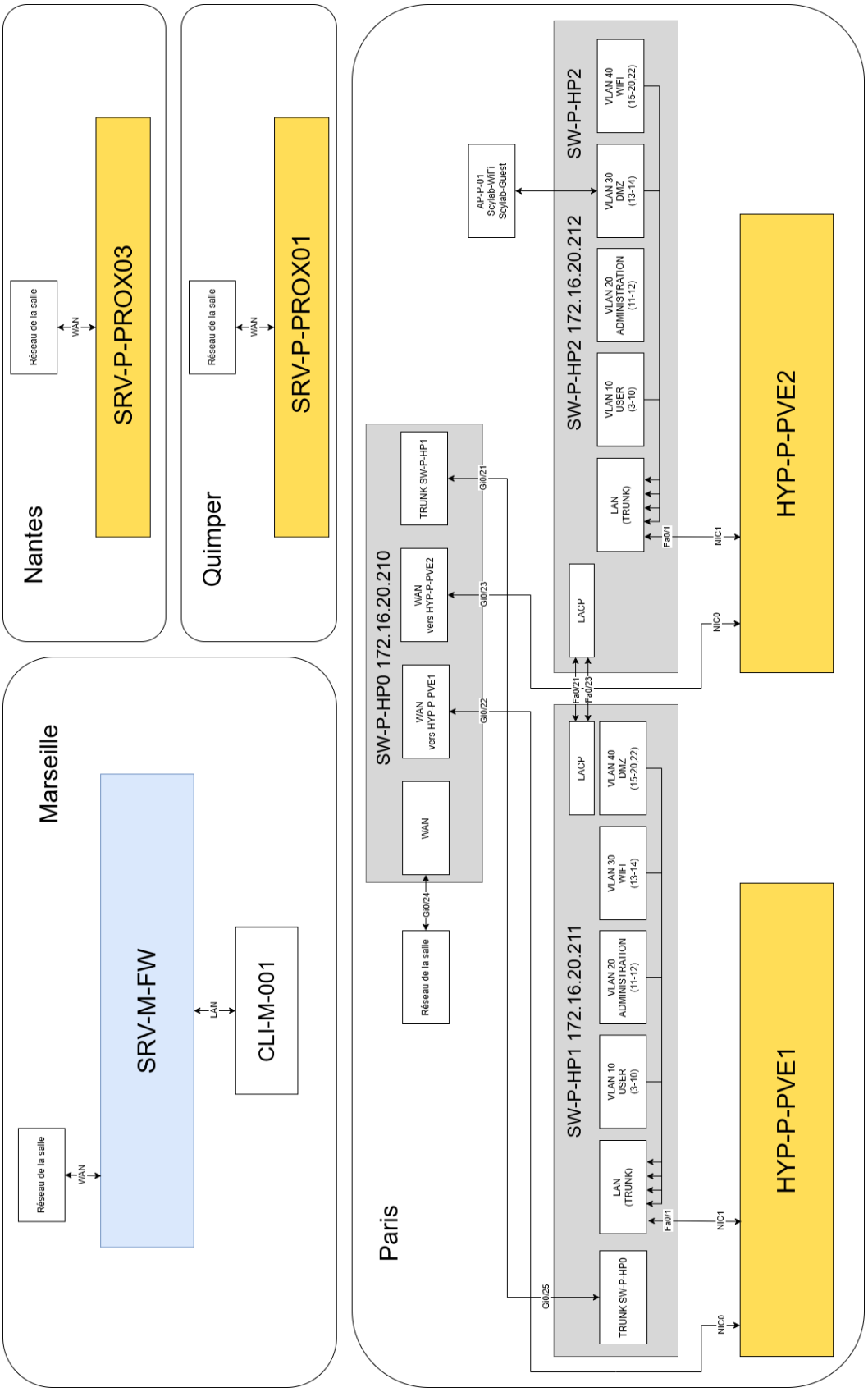
Ce projet a permis de déployer Kea DHCP comme solution centralisée, fiable et évolutive pour la gestion de l'attribution des adresses IP au sein de l'infrastructure réseau d'Oasis.

Grâce à sa conception modulaire et à son API REST native, Kea offre une grande flexibilité dans la gestion des pools d'adresses, des réservations statiques et des options réseau. Plusieurs améliorations restent néanmoins envisageables, notamment l'intégration d'alertes sur l'épuisement des pools.

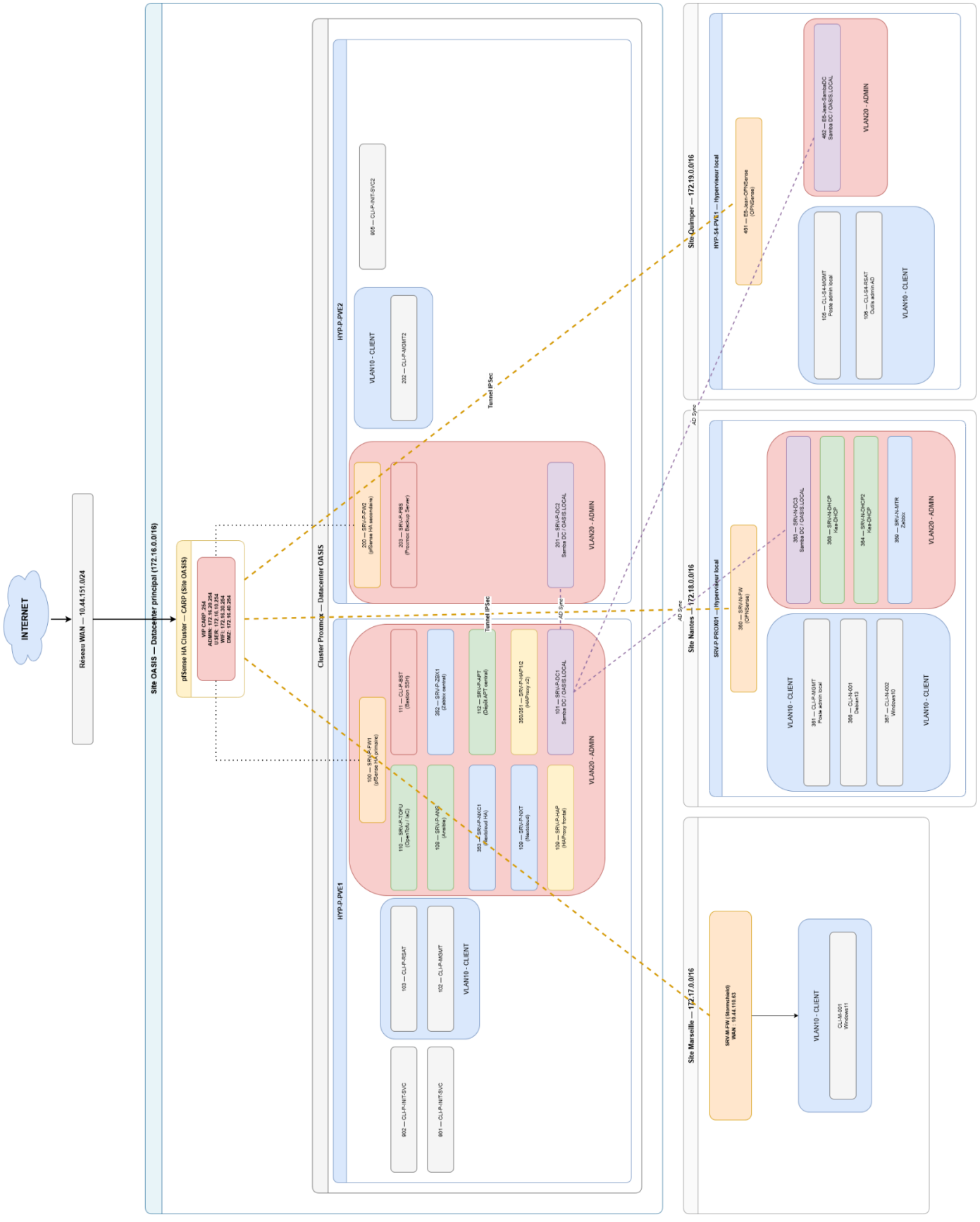
Au-delà de la technique, ce projet m'a permis de mieux comprendre le fonctionnement des protocoles réseau fondamentaux, de gagner en autonomie sur l'administration d'un service Linux critique, et de prendre conscience de l'importance d'un service DHCP bien configuré et maintenu pour assurer la stabilité d'un système d'information.

10. Annexes

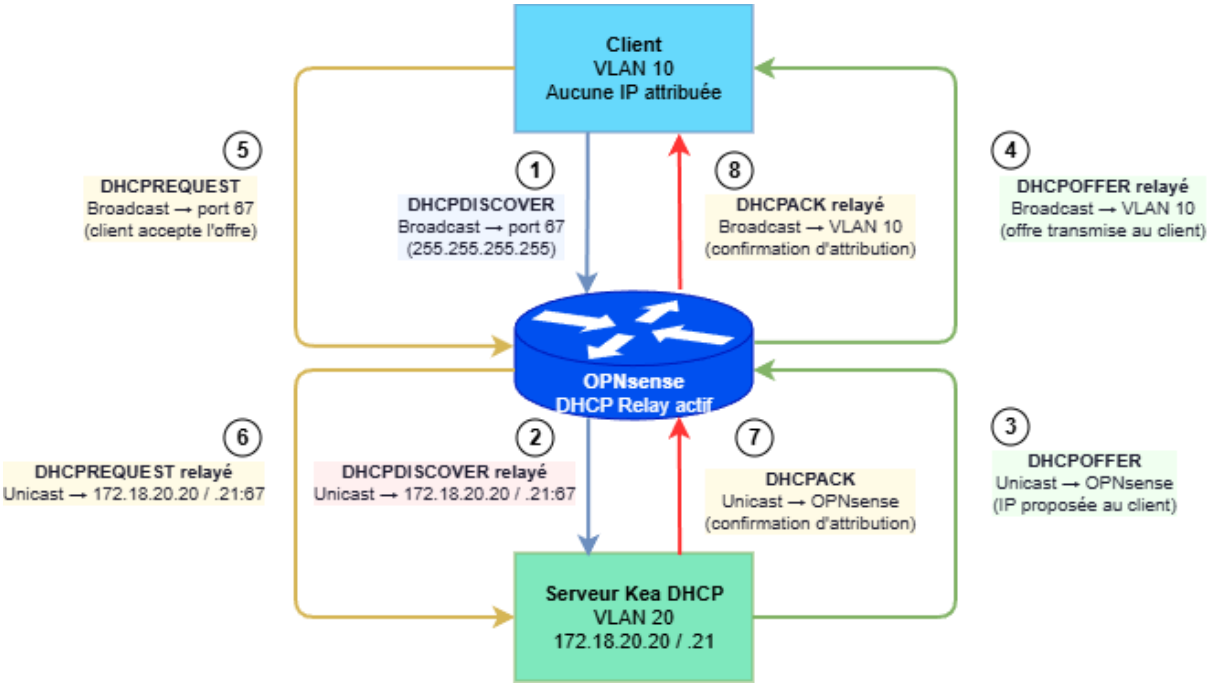
10.1 Schéma physique



10.2 Schéma logique



10.3 Schéma de flux DHCP avec relay



10.4 Référence des commandes API Kea

Liste complète des commandes disponibles via l'API REST Kea DHCP4 :

```
# Commandes de gestion générale
kea build-report           # Infos de build
kea version-get            # Version Kea
kea status-get             # Statut service + HA
kea list-commands          # Liste toutes les commandes
kea config-get             # Configuration active
kea config-reload          # Rechargement config
kea config-test            # Validation config
kea config-write           # Écriture config sur disque
kea shutdown               # Arrêt du service

# Gestion des baux IPv4
kea lease4-get-all         # Tous les baux
kea lease4-get             # Bail par IP
kea lease4-add             # Ajouter un bail manuel
kea lease4-del             # Supprimer un bail
kea lease4-update          # Modifier un bail
kea lease4-wipe            # Effacer tous les baux (subnet)

# Haute disponibilité
kea ha-heartbeat           # Test communication HA
kea ha-sync                # Synchronisation manuelle
kea ha-scopes              # Périmètre de service HA
kea ha-continue            # Reprendre après maintenance
kea ha-maintenance-start   # Démarrer maintenance
kea ha-maintenance-cancel  # Annuler maintenance
kea ha-reset               # Réinitialiser état HA
```

10.5 Référence des commandes API Kea

```
# Statut du service et état HA
curl -s -X POST http://172.18.20.20:8000/ \
  -H 'Content-Type: application/json' \
  -d '{"command":"status-get","service":["dhcp4"]}' | python3 -m json.tool

# Liste des baux actifs
curl -s -X POST http://172.18.20.20:8000/ \
  -H 'Content-Type: application/json' \
  -d '{"command":"lease4-get-all","service":["dhcp4"]}' | python3 -m json.tool

# Version du serveur
curl -s -X POST http://172.18.20.20:8000/ \
  -H 'Content-Type: application/json' \
  -d '{"command":"version-get","service":["dhcp4"]}' | python3 -m json.tool

# Rechargement de la configuration sans redémarrage
curl -s -X POST http://172.18.20.20:8000/ \
  -H 'Content-Type: application/json' \
  -d '{"command":"config-reload","service":["dhcp4"]}' | python3 -m json.tool
```

10.6 Consultation des journaux

```
# Logs en temps réel
journalctl -u kea-dhcp4-server -f

# 50 dernières lignes
journalctl -u kea-dhcp4-server -n 50 --no-pager
```

10.7 Lecture des baux depuis le fichier

```
cat /var/lib/kea/kea-leases4.csv
```