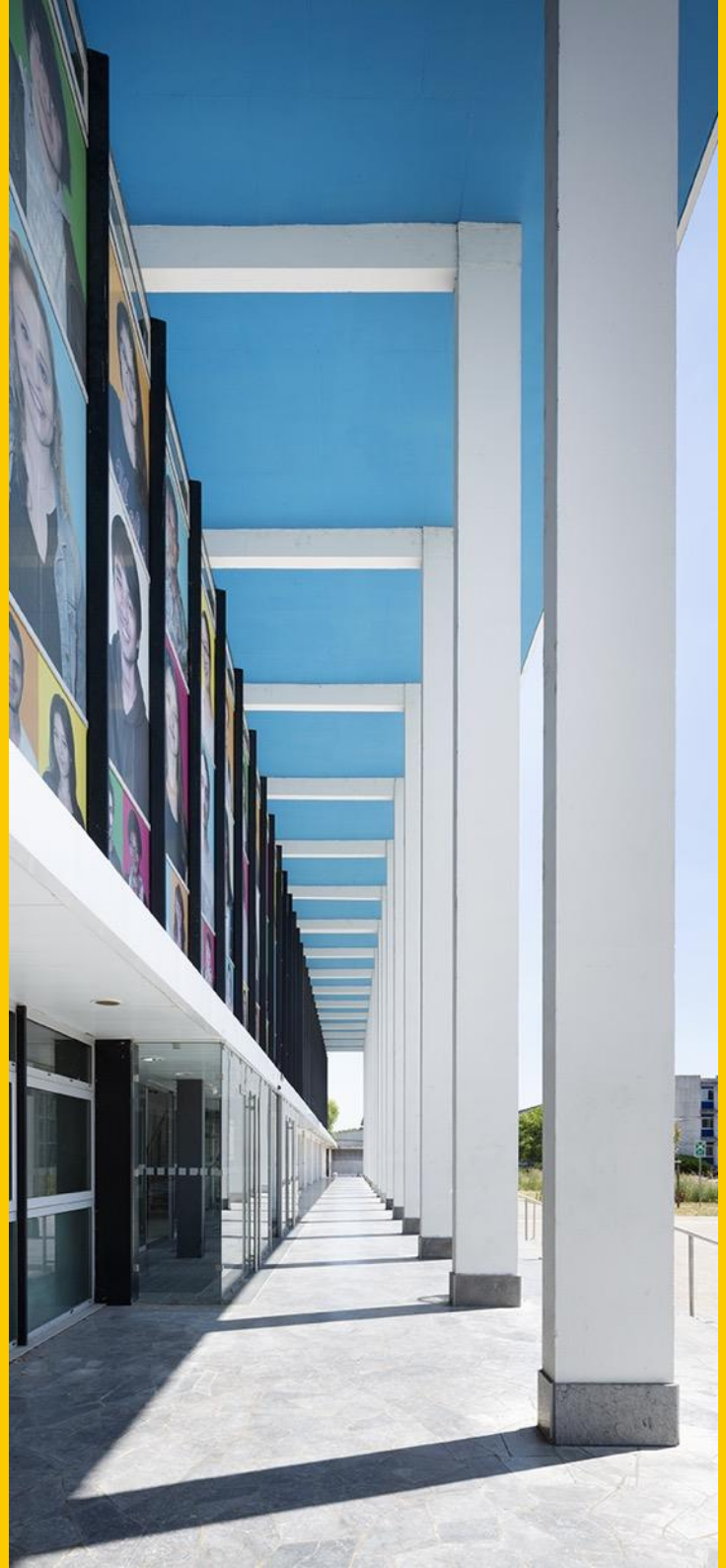
Capitoul
Projet DDI – UT3
22/06/2023

UNIVERSITÉ TOULOUSE III PAUL SABATIER

Université Fédérale Toulouse Midi-Pyrénées



Sommaire

- Définition DDI et objectifs du projet
- Architecture DNS actuelle à l’UT3
- Etude de solutions
- Choix final de la solution
- Calendrier et phases de mise en production

Intro

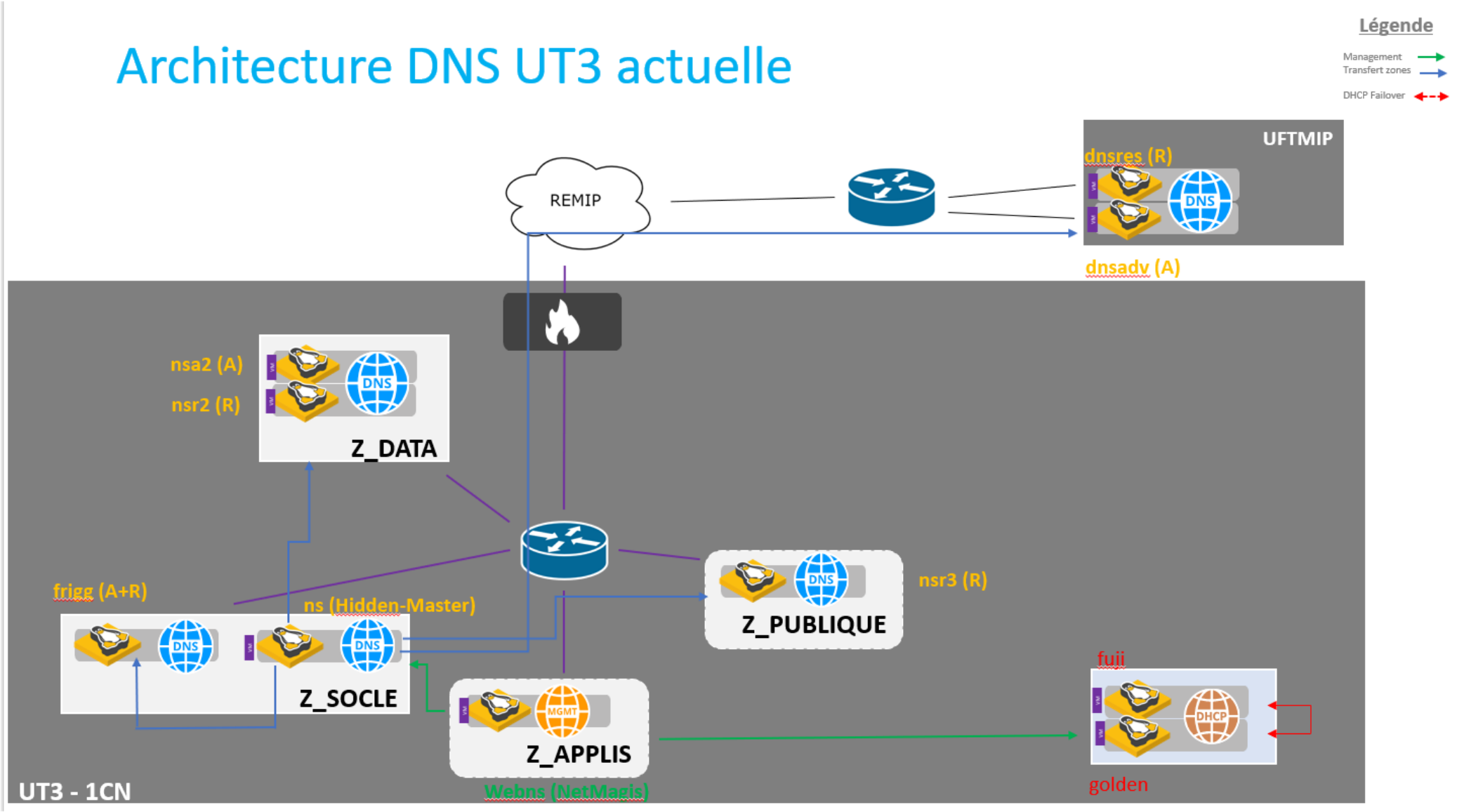
- Définition DDI
- Objectifs
- Archi actuelle

DDI : Définition et objectifs

- Définition DDI
  - DDI = DNS, DHCP et IPAM

- DDI actuel : **NetMagis**
  - Limites actuelles et besoins futurs
    - Solution plus maintenue
    - Gestion du **cycle de vie des IP** non optimal (IPAM)
      - Besoin d'un référentiel IP/VLAN
      - Besoins d'automatisation – Ansible ou REST API
        - Service Système (ELK, VM, …)
        - Service Parc (DHCP, déploiement nouvelles salles, …)
    - Pas d'**offre de service** DDI complète aux composantes
      - Délégations sur la partie IPAM/DNS via NetMagis seulement
        - Pas d'offre de service DHCP pour les composantes
        - Authentif via des comptes locaux => Outil lié à l'AD serait plus efficace !
    - La VM est hébergée au 1CN à l'UT3
      - Pas de site secondaire
      - Pas de PRA/PCA

Architecture actuelle



Etude de solutions

- Listing des outils etudiés
- Description de chaque outil

Listing des outils étudiés

- Solutions majeures
  - Efficient IP - Français
  - Infoblox - Américain

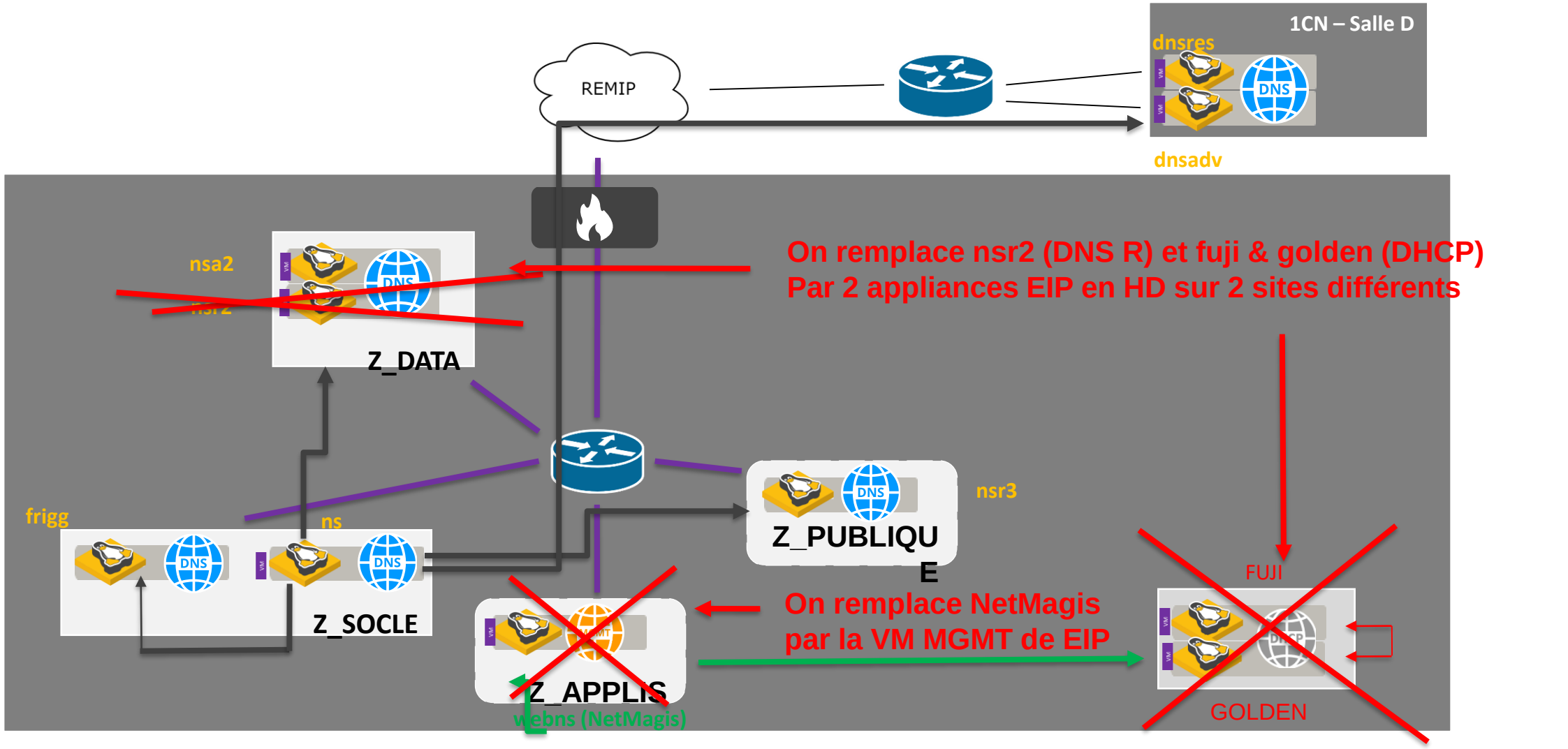
- Solution alternative
  - Micetro - Islandais

- Solution open source
  - TeemIP

- *Les autres solutions présentes sur le marché n'offrent pas les 3 services DDI ou ne respectent pas les prérequis en s'intégrant dans l'architecture existante*

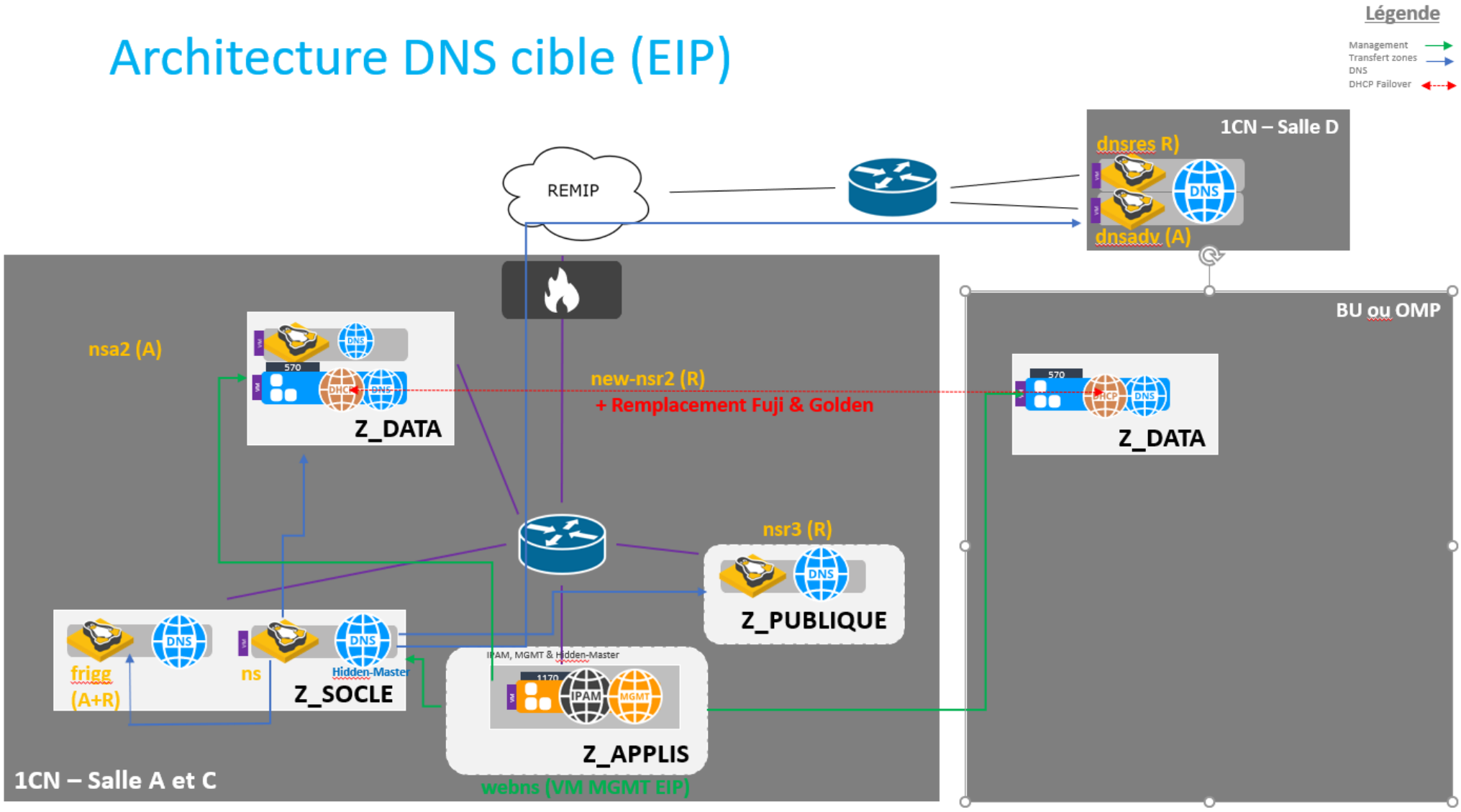
Architecture Efficient IP proposée

Architecture DNS UT3 actuelle => cible



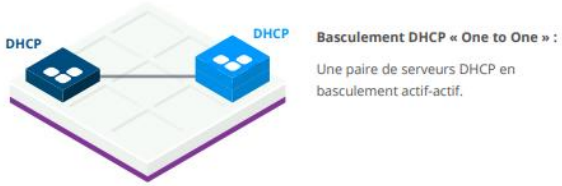
Architecture Efficient IP proposée

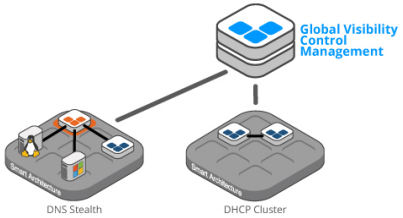
Architecture DNS cible (EIP)

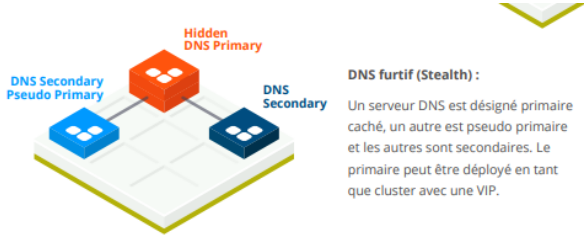


Solution 1 - Efficient IP

- **Architecture EIP à prévoir**
  - Suppression de **webdns** par la VM de MGMT => Appliance 1170 à prévoir
  - **Fuji** & **Golden** (DHCP) et **nsr2** (DNS R) à remplacer par 2 Appliances 570 (VMs) sur 2 sites différents (1CN et OMP)
  - **NS** (hidden-master) : On le garde et on le pilote via EIP (licence MVSM)







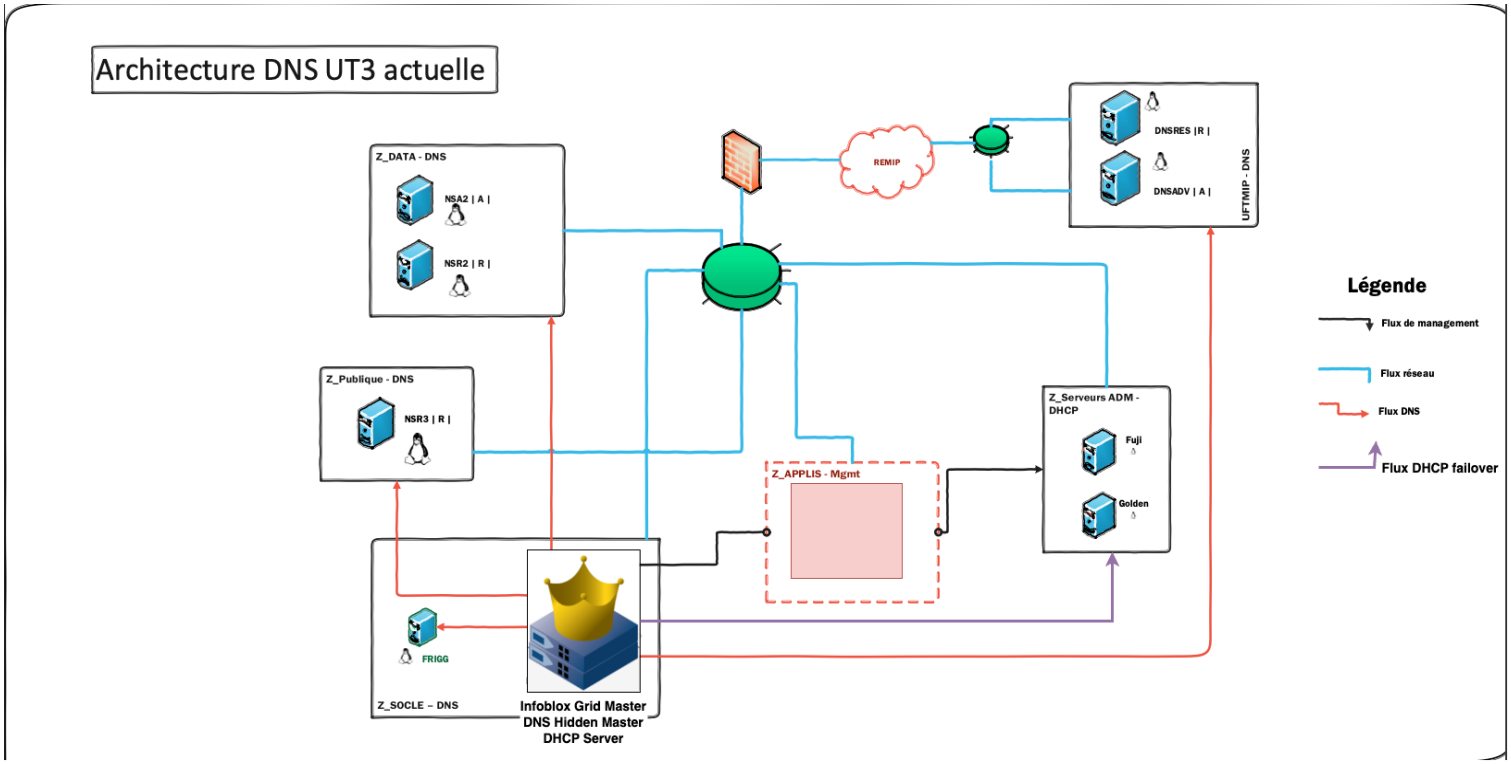
  - *Frigg, nsa2, nsr3, dnsres et dnsadv inchangés (transferts de zones DNS)*

- **Licences EIP à prévoir pour 3ans (même coût renouvelable) :**
  - *1 VM MGMT 1170*
  - *2 Appliances SDS-570 (en VMs)*
  - *1 licence MVSM pour le serveur hidden-master NS*

- **Achat via l'UGAP possible => pas de nouveau marché !**

Solution 2 - INFOBLOX

- Architecture INFOBLOX à prévoir



- Suppression de **NetMagis** par un cluster **GridMaster**
  - **Fuji** & **Golden** (DHCP) remplacés par ce cluster de 2 VMs sur 2 sites différents (1CN et OMP)
  - **nsr2** (DNS R) pourrait être piloté par la GridMaster
- **NS** (hidden-master) : on veut le garder et le piloter
  - **IMPOSSIBLE DE LE PILOTER via GridMaster**
    - **Le master doit être sur les 2 Appliances du GridMaster**

- *Frigg, nsa2, nsr3, dnsres et dnsadv inchangés (transferts de zones DNS)*

Solution 3 - MICETRO

- **Architecture Micetro à prévoir :**
  - **Micetro est un orchestrateur, il ne porte pas les services (sauf IPAM) !**
  - Suppression de **webdns et installation d'une VM avec une base MySQL/PostgreSQL dédiée**
  - **Fuji** & **Golden** (DHCP) et **nsr2** (DNS R) à piloter par 2 Virtual Appliances sur 2 sites différents (1CN/OMP)
  - **NS** (hidden-master) : On le garde et on le pilote via les appliances

  - *Frigg, nsa2, nsr3, dnsres et dnsadv inchangés (transferts de zones DNS)*

- **Inconvénients :**
  - **Installer la Micetro Console sur un serveur Windows si on veut lier à l'AD !**
  - Micetro n'est pas référencé à l'UGAP et aucun prestataire toulousain ne propose pas MICETRO => 1 seul prestataire le propose mais ne l'a encore jamais déployé (basé sur Paris)
  - Pas de support en France, solution islandaise

- **Budget Micetro à prévoir (pas de marge de manœuvre pour négocier) :**
  - **20000€ / an minimum pour notre archi**

Solution 4 - TeemIP

- **Architecture TeemIP à prévoir :**

Services DDI éclatés :

  - Service IPAM en standalone ou extension de « iTop »
  - Impossible de piloter des serveurs existants (ni DNS, ni DHCP)
    - Regroupe seulement les options DHCPs à mutualiser sur nos serveurs
    - Génère les zones mais il faut scripter ensuite pour les pousser sur nos serveurs bind

- **Budget TeemIP à prévoir :**
  - Logiciel libre gratuit (version standalone et iTop Community)
  - Payant avec la licence iTop Pro/Enterprise

⇒ **Ne respecte pas les prérequis techniques car beaucoup de limites techniques**

⇒ **Il faut monter une toute nouvelle architecture car ne s'implante pas dans l'existante !**

Solution choisie

- **Solution 4 : TeemIP**
  - Ne respecte pas les prérequis du projet
- **Solution 3 : MICETRO**
  - Prix trop excessif (3xEIP), pas re ReteX, pas de support français
- **Solution 2 : INFOBLOX**
  - Impossible de garder le serveur NS isolé des 2 VMs
  - Impossibilité de piloter un ou plrs serveurs DHCP externes
  - Obligation de passer par un marché :
    - Rédiger un CCTP, attendre les délais de publication, solliciter le DAP, …

Solution 1 : EIP

- Respecte les prérequis techniques en s'implantant ds l'architecture DNS actuelle :
  - Service DDI offerts avec délégations via l'AD pour nos labos/composantes
  - Possibilité de piloter plrs serveurs DNS/DHCP différents
    - Ici, le serveur NS sera piloté par la VM de Management
  - La VM de Management est évolutive et isolée par rapport aux 2 appliances et au serveur NS
  - Architecture évolutive avec les serveurs *frigg, nsa2, nsr3, dnsres et dnsadv inchangés (transferts de zones DNS)*

- Achat de la solution + prestation dispo via l'UGAP => Pas de marché !
  - Presta directe EIP possible sans passer par SFR

Mise en Prod

- Calendrier
- Détail des Phases

Planning de mise en prod

ACTION	DATE
Etude des solutions	Novembre 2022 à Mars 2023
Achat de la solution et prestation EIP via l'UGAP	27/03/2023
Réunion de lancement	24/04/2023
Phase 1 : Définition de l'architecture technique	24/04 au 16/05/2023
Phase 2 : Configuration et Validation	17/05/2023 au 22/06/2023
Phase 3 : Mise en Production	26/06/2023
Phase 4 : Suivi/Surveillance et Recette définitive	26/06 au 19/07/2023

Phases du projet

- **Phase 1 : Définition de l'architecture technique**
  - Schémas réseaux et ouvertures de flux
  - Préparation de l'infra VMware VMs (CARP pour la VIP DNS)
  - Préparation des exports IPAM
    - Réflexion sur les blocks, subnets et organisation IPAM en interne
    - Import successifs pour éliminer les *« orphans addresses »*
  - Préparation des scopes DHCP pour les importer
  - Réflexion sur les délégations pour reporter les accès NetMagis (comptes locaux)

- **Phase 2 : Configuration et Validation**
  - Installation des Appliances avec les services de base (licences, NTP, Syslog, …)
  - Installation de la VM Debian hidden-master DNS avec le package EIP
  - Configuration des services DHCP (actif-actif) et DNS (VIP actif-passif)
  - Validation de la structure et imports IPAM et transferts DNS
  - Liaison à l'AD UT3 et délégation aux composantes sur leur périmètre via les groupes AD
  - Supervision SNMP à intégrer à notre outil : check_mk

- **Phase 3 : Mise en production**
  - Cahier de test à valider avec le prestataire
  - Checks configuration et état des services avant migration
  - Elaboration d'un plan de migration
  - Communication auprès des correspondants UT3 une semaine avant la migration
  - **Migration le 26/06**

Phases du projet

- **Phase 4 : post-migration**
  - Suivi/Surveillance et Recette définitive
    - Documentations et formations pour les composantes UT3
    - Retours des correspondants
  - Evolutions
    - Référentiel IPAM/VLAN sur lequel on va pouvoir s'appuyer
    - Export des logs sur la pile SIEM de la DSI (ELK avec dashboards DHCP, DNS, …)
    - Automatisation avec accès à l'API REST
    - Architecture DNS générale à faire évoluer encore (dnsadv, dnsres ?)
    - Nouveaux besoins des labos/composantes (DHCP par ex)