****

*Mérignac, le vendredi 20 juin 2025*

Dossier technique

(Architecture et organisation)



|  |  |  |  |
| --- | --- | --- | --- |
| **Libellé** | Dossier technique | | |
| **Client** | *EVA Estuaire* | | |
| **Projet** | Architecture et organisation | | |
| **Auteur** | Service Technique | **Référence du document** |  |
| **Version** | 1 | **Date de modification** | 20/06/2025 |
| **Etat** | A valider  Validé | **Diffusion** | Interne    Contrôlée    Libre |

Sommaire

[1. Introduction 3](#_Toc144398803)

[2. Présentation de l'architecture 4](#_Toc144398804)

[2.1. Schéma d'architecture 4](#_Toc144398805)

[2.2. Serveurs 7](#_Toc144398806)

[2.3. Eléments actifs et protection électrique 8](#_Toc144398807)

[2.4. Plan d'adressage 12](#_Toc144398808)

[2.5. Gestion des noms 12](#_Toc144398809)

[3. Présentation du SI par service 13](#_Toc144398810)

[3.1. Service authentification réseau 13](#_Toc144398811)

[3.2. Service RDS (TSE) 14](#_Toc144398812)

[3.3. Service de fichiers 15](#_Toc144398813)

[3.4. Service DHCP 17](#_Toc144398814)

[3.5. Service Antivirus 18](#_Toc144398815)

[3.6. Service Impression 19](#_Toc144398816)

[3.7. Service WAN et Internet 20](#_Toc144398817)

[3.8. Service Pare-feu , VPN et Wifi 20](#_Toc144398818)

[3.9. Service de Messagerie 24](#_Toc144398819)

[3.10. Service de sauvegarde 25](#_Toc144398820)

[4. Postes utilisateurs 26](#_Toc144398821)

[5. Applications métiers 27](#_Toc144398822)

[6. Télécoms 29](#_Toc144398823)

[7. Conclusion 29](#_Toc144398824)

**- o O o -**

# Introduction

Ce document présente l'architecture générale du réseau utilisée par **EVA Estuaire**.

Ainsi que nos conseils et recommandations pour l’optimisation et la rationalisation du SI.

**Adresse :** 42 Avenue de la République 33820 BRAUD ET SAINT-LOUIS

**Interlocuteurs :**

M. Marie THOURAUD

Directrice adjointe

Tél : 05 57 94 80 60

M. Cédric DAVID-PASQUIER

Responsable maintenance

Tél : 05 57 94 80 60 - 06 46 84 22 93 - sg@eva.asso.fr

**Échelle d’évaluation des recommandations**

Les recommandations sont catégorisées sur trois niveaux :

Recommandation (risque critique)

Recommandation liée à un risque critique. Une action de priorité haute est à entreprendre dès que possible

Recommandation (risque important)

Recommandation liée à un risque important. Une action de priorité moyenne est à entreprendre à moyen terme

Recommandation (optimisation)

Une action est à entreprendre pour optimiser et/ou sécuriser l’environnement (sans être lié à un risque majeur)

# Présentation de l'architecture

## Schéma d'architecture

L'**architecture informatique** est représentée par le schéma page suivante.

Le réseau est centralisé autour d’un **serveur physique** sous l’environnement **VMWARE** et de 2 serveurs virtuels sous **Windows Serveur 2019 Standard**

Le réseau est de type Ethernet architecturé autour de **plusieurs switches** répartis sur l’ensemble des bâtiment

## Serveurs

L’environnement est architecturé autour d’un **serveur** sous l’environnement VMWARE :

*Celui-ci est installé avec le système de virtualisation* ***VMWARE ESXI 8.0****.*

|  |  |
| --- | --- |
| **Dell PowerEdge T450** |  |
| Nom du serveur : | **ESXI EVA** |
| Adresse IP (masque S/R) : | 192.168.0.20 |
| Passerelle : | 192.168.0.254 |
| DNS : | 192.168.0.14 |
|  |  |
| **Marque / Référence :** | **Dell PowerEdge T450**  iDARC = 192.168.0.19 |
| **Numéro série :**  Code de service express : | Numéro de série - SN = 812CNY3  17478675003 |
| Processeur : | 2 x Intel® Xeon® Silver 4314 |
| Mémoire RAM : | 64 Go RAM |
| Carte Raid : | PERC RAID |
| Disques Durs : | 4 x Disque dur 1,2 To ISE SAS 12 Gbit/s  3.3 To |
| Alimentation (redondante) : | Oui |
|  |  |
| Système d’exploitation : | Windows 2019 Standard – 2 VM |
| CAL Windows : | 20 CAL |
| CAL RDS/TSE : | 20 CAL RDS |
|  |  |
| Date d’achat : | 2023 |
| **Garantie :** | **04/10/2028**  Garantie DELL Pro Support J+1 |

Rôles du serveur VM EVADC :

* Contrôleur de domaine, Active Directory, DNS, DHCP
* Serveur de fichiers
* Sauvegardes Veeam

Rôles du serveur VM EVATSE (uniquement pour Epsilog qui va disparaitre à terme) :

* Contrôleur de domaine, Active Directory, DNS et DHCP
* Serveur RDS/TSE (Bureau à distance)

## Eléments actifs et protection électrique

Les **commutateurs (switches)** utilisés sont :

* **1 D-Link DES-1252 (48 ports)**
* **2 D-Link DGS-1210 (24 ports)**
* **5 D-Link DES-1228 (24 ports)**

**Répartition :**

* sw-cœur (DGS 1210-24) - Bâtiment principal salle de répartition
* sw-sr0 (DGS 1210-24) - Bâtiment principal salle de répartition
* sw-sr1 (DGS-1210-28p) - Unité 5
* sw-sr2 (DGS-1210-28p) - Unité 4
* sw-sr3 (DGS-1210-28p) - Unité 3
* sw-sr4 (DGS-1210-28p) - Unité 2
* sw-sr5 (DGS-1210-28p) - Unité 1
* sw-sr6 (DGS-1210-28p) - Bâtiment principal SR6 milieu du bâtiment

|  |  |  |
| --- | --- | --- |
| **2** | Marque : | **D-Link** |
| Modèle : | DES 1252 (10/100 /1000 mbps) |
| Nombre total de ports : | 52 |
| Nombre de ports disponibles : |  |

|  |  |  |
| --- | --- | --- |
|  | Marque : | **D-Link** |
| Modèle : | DGS-1210 (10/100 /1000 mbps) |
| Nombre total de ports : | 24 |
| Nombre de ports disponibles : |  |

|  |  |  |
| --- | --- | --- |
|  | Marque : | **D-Link** |
| Modèle : | DES-1210 (10/100 /1000 mbps) |
| Nombre total de ports : | 24 |
| Nombre de ports disponibles : |  |

|  |  |  |
| --- | --- | --- |
|  | Marque : | **D-Link** |
| Modèle : | DES-1228 (10/100 /1000 mbps) |
| Nombre total de ports : | 28 |
| Nombre de ports disponibles : |  |

|  |  |  |
| --- | --- | --- |
|  | Marque : | D-Link |
| Modèle : | DES-1228 (10/100 /1000 mbps) |
| Nombre total de ports : | 28 |
| Nombre de ports disponibles : |  |

|  |  |  |
| --- | --- | --- |
|  | Marque : | D-Link |
| Modèle : | DES-1228 (10/100 /1000 mbps) |
| Nombre total de ports : | 28 |
| Nombre de ports disponibles : |  |

|  |  |  |
| --- | --- | --- |
|  | Marque : | D-Link |
| Modèle : | DES-1228 (10/100 /1000 mbps) |
| Nombre total de ports : | 28 |
| Nombre de ports disponibles : |  |

|  |  |  |
| --- | --- | --- |
|  | Marque : | D-Link |
| Modèle : | DES-1228 (10/100 /1000 mbps) |
| Nombre total de ports : | 28 |
| Nombre de ports disponibles : | 23  **(04 octobre 2010)** |

Onduleur

Le serveur **Dell PowerEdge T430** est protégé électriquement par un onduleur **Riello IDG800.**

*Aucun logiciel de gestion installé.*

Recommandation (optimisation)

- Le serveur va être remplacé en septembre 2023 par un modèle Rack.

Il faudra utiliser l’onduleur Riello Rack VSD 2200 de la baie pour protéger le serveur

- Prévoir une prestation pour revoir et optimiser le câblage réseau et électrique des 2 baies (voir Cilan) & mise en rack onduleur VSD 2200

**Photos :**

*Emplacement : dans le local technique à côté de l’accueil*

|  |  |
| --- | --- |
| Baie principale : | Serveur **Dell PowerEdge T430**(ondulé) :    Modem routeur & Firewall Fortigate: |
|  | |

## Plan d'adressage

Le réseau dispose du plan d'adressage suivant :

**Classe Adresse IP : 192.168.0.0**

**Masque de sous Réseau : 255.255.255.0**

**Adresses IP fixes :**  Serveur : EVADC : 14

Serveur : EVARDS : 15

Routeur : Stormshield SN210 : 254

Imprimante : Canon iR C3330  : 100

Poste GTC : PC : 20

## Gestion des noms

**Convention de nommage des PC :**

**Une image contenant texte, capture d’écran, nombre

Description générée automatiquement**

EVA-PCX où X représente un nombre

Ex: **EVA-PC1**

**Convention de nommage des logins (nom d’ouverture de session) des utilisateurs :**

La règle d’attribution des logins utilisateurs a été définie comme suit :

Login = *fonction*

# Présentation du SI par service

Cette partie présente l’implication de chaque service au niveau du système de communication.

## Service authentification réseau

Le service d’authentification est assuré par le serveur **contrôleur de domaine** (DC) du serveur :

|  |  |
| --- | --- |
| **Nom du serveur :** | **EVADC** |
| Nom de domaine : | **Eva.lan** |
| Adresse IP (masque S/R) : | x.x.x.x/xx |
| Passerelle : | x.x.x.x |
| DNS : | x.x.x.x |

*L’authentification d'un utilisateur (login) est effectuée auprès du contrôleur de domaine Active Directory (comptes utilisateurs avec mot de passe sur le serveur AD).*

**Comptes utilisateurs AD (Active Directory) :**

Une image contenant texte, capture d’écran, Police

Description générée automatiquement Une image contenant texte, capture d’écran, Police

Description générée automatiquement

- Pas d’exigence de complexité sur les mots de passe sur les comptes utilisateurs

Recommandations (risque important)

- En termes de sécurité, il serait souhaitable d’évoquer une politique d’accès par mot de passe basée sur une longueur minimale et renouvelable périodiquement (mettre en place une stratégie de sécurité GPO associée).

La durée de **renouvellement d’un mot de passe** recommandée est de **90 jours**.

Recommandations (optimisation)

- Réorganiser les partages réseaux actuels afin de limiter les partages existants et faciliter leurs administrations.

## Service RDS (TSE)

Le serveur EVARDS est le **serveur RDS/TSE** (Bureau d’accès à distance).

**1 VM Windows 2019 Std– RDS/TSE, Fichiers, Applications (EIG)**

Nom = **EVARDS**

Domaine = **eva.lan**

Adresse IP = x.x.x.x

Masque S/R = x.x.x.x

Passerelle (routeur) = x.x.x.x

**1 VM Windows 2008 R2– ancient serveur EIG (non utilisé)**

Nom = **EVATSE**

Domaine = **eva.lan**

Adresse IP = x.x.x.x

Les utilisateurs s’y connectent via des clients légers Wyse.

Il faut être membre du groupe AD **GRP\_RDP** pour pouvoir ouvrir une session TSE sur le serveur :

L’accès au serveur est protégé par GPO (stratégie) afin de limiter les actions des utilisateurs qui s’y connectent.

## Service de fichiers

|  |
| --- |
| **EVARDS** [x.x.x.x] le 31/08/2023 |
| Partitionnement volume disque :  (C :) [SYSTEM]  (D:) [DATA] – Partition pour le serveur de fichiers |

**Partages :**

**Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement**

**D:\EVA\Commun**, nom de partage = EVA

-> dossier partagé à tout le monde

*Droits d’accès = utilisateurs du domaine*

**D:\Users\**, nom de partage = users$ (partage caché)

-> dossier personnel pour chaque utilisateur

*Droits d’accès = par utilisateur*

**D:\Messageries\**, nom de partage = messageries$ (partage caché)

-> dossier personnel pour fichier PST

*Droits d’accès = par utilisateur*

**Stratégie utilisateur – lecteurs réseaux :**

Une image contenant texte, table

Description générée automatiquement

**Convention des lecteurs réseaux :**

Z : \\EVARDS\EVA\Commun

Y : \\EVARDS\users$\%username%\

P : \\EVARDS\EVA

Z est le lecteur réseau Commun, tout le monde y a accès.

Y est le lecteur réseau Personnel, uniquement l’utilisateur a le droit d’y accéder.

P regroupe tous les répertoires.

## Service DHCP

**Service DHCP (Dynamic Host Configuration Protocole)**

Son rôle est d’assurer la configuration automatique des paramètres IP des équipements sur le réseau, notamment en lui affectant automatiquement une adresse IP et un masque de sous-réseau. DHCP peut aussi configurer l’adresse de la passerelle par défaut, des serveurs de noms DNS, etc.

Le **service DHCP** est assuré par le serveur **EVADC** [x.x.x.x]

Pool d’adresses IP distribuées par DHCP **EVADC** : **101 à 199**

Options DHCP :

Une image contenant texte

Description générée automatiquement

## Service Antivirus

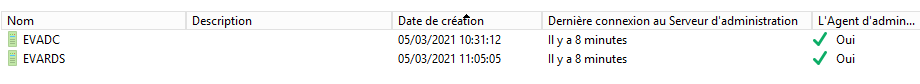
|  |  |
| --- | --- |
| Le **service Antivirus** est assuré par le logiciel : | **Une image contenant Police, Graphique, logo, texte  Description générée automatiquementMSP** |
|  |  |
| Mode : | **Kasperky MSP**  *Hébergé au DataCenter RECOM* |
| Nombre de licences : | **9 Licences MSP**  Protection de 2 serveurs  Protection de 7 postes |
| Date d’expiration : | **Abo mensuel** |

Migration en cours anti-virus Malwarebyte sur les postes.

Console administration Kaspersky MSP : le 31/08/2023

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement



Recommandations (risque important)

- Prévoir de compléter la protection antivirus par une solution EDR

*EDR (Détection et réponse des terminaux) est une solution de sécurité des terminaux qui inclut la surveillance en temps réel et la collecte des données de sécurité des terminaux avec un mécanisme de réponse automatisée aux menaces.*

*Certains EDR possède l’option de Rollback qui permet de restaurer l’état des fichiers après un cryptage.*

## Service Impression

Le service d’impression est assuré par un **copieur multifonction RICOH IM C3000**

Quelques imprimantes locales sont installées sur certains PC.

Pas de serveur d'impression installé

**COPIEURS RESEAUX :**

|  |  |  |
| --- | --- | --- |
| **Copieur** | **Emplacement** | **Adresse IP** |
| **RICOH IM C3000** | Accueil | x.x.x.x |

## Service WAN et Internet

L'accès **Internet** sur le site est assuré par **:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Débit (DL/UP)** | **Opérateur** | **IP Public fixe** | **Utilisation** |
| **Fibre SFR** | 440 Mbps  /420 Mpb | SFR | x.x.x.x | Data et Téléphonie |
| **4G RECOM** |  | SFR | x.x.x.x | Lien secondaire |

## Service Pare-feu , VPN et Wifi

Le site est protégé par un **pare-feu (firewall) :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Firewall** | **IP (LAN)** | **Firmware** | **Fonctions UTM** | **Expiration licence** |
| **FortiGate 60F** | 192.168.x.x | 7.4.7 | oui | 02/10/2028 |

*Les produits* ***UTM (Unified Threat Management, gestion unifiée des menaces)*** *permettent de dépister toute une série de menaces courantes. Ces appareils filtrent le trafic à destination ou en provenance d'Internet et recherchent essentiellement les virus, les chevaux de Troie, les logiciels espions et tout autre code malveillant.*

Une image contenant texte, conception

Description générée automatiquement

Interfaces firewall :

Une image contenant texte, capture d’écran, nombre, Police

Description générée automatiquement

Service VPN

Le produit **Fortigate 60F** est utilisé pour des connexions VPN (IPsec, SSL, PPTP).

Cette fonctionnalité permettrait de sécuriser les accès distants nomades (utilisateurs, prestataire, etc..) ou d’interconnecter des sites distants.

L’authentification des connexions se fait via les comptes utilisateurs de **l’Active Directory**.

Avec utilisation du logiciel **Stromshield VPN SSL** installé sur les postes concernés.

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

Service Wifi

Des **bornes** **wifi Ubiquiti** sont installées dans tous les bâtiments :



Deux SSID sont diffusés : un **réseau privé** et un **réseau public**

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Pour le wifi Public, un **système de voucher** est mis en place pour contrôler les accès wifi :

*(Système de création de tickets de connexion wifi unique)*

Une image contenant texte, nombre, Police, ligne

Description générée automatiquement Une image contenant texte, capture d’écran, nombre, Police

Description générée automatiquement

La procédure est mise à disposition de la Directrice Adjointe pour **génération de voucher** pour les réseaux :

[xxxxxxxxxxxxxxxxxxxxxxxxxx](https://wifi.recom.fr:8443/manage/hotspot/site/4x6bomik/vouchers/1/50)

**Recommandations (optimisation)**

Le firewall Stormshield va être remplacer prochainement par un firewall FORTINET (prévision septembre/octobre 2023)

## Service de Messagerie

Le service de messagerie est assuré par un serveur de **messagerie externe** :

|  |  |  |  |
| --- | --- | --- | --- |
| **Hébergeur** | **Nom de domaine** | **Nombre de BAL (mails)** | **Fonctionnalités** |
| **OVH** | @ eva.asso.fr |  | Messagerie simple  IMAP/POP |

Client de messagerie utilisé en session RDS/TSE : Outlook 2010 & Webmail

Les fichiers de **données des messageries (PST**) sont stockés sur le **serveur EVASRV.**

**Emplacement stockage PST : \\evatse\messageries$\**

**OVH**

Cod. Client : 78826061

Ref. Client : NR6061-OVH

**Paramètres de configuration des messageries (mails) :**

Serveur de courrier entrant (POP) : **pop3.eva.asso.fr POP ssl0.ovh.net  port xxx**

Serveur de courrier sortant (SMTP) : **smtp.eva.asso.fr SMTP ssl0.ovh.net port xxx**

0

**Recommandations (optimisation)**

Passer à Microsoft 365 pour optimiser votre messagerie et utiliser des outils collaboratifs :

**Les options de Microsoft 365 :**

- la messagerie Exchange Online (50 Go de stockage, calendriers et contacts partagés, messages d’absence, etc..)

- le pack Office (Word, Excel, Outlook..)

- un espace de stockage en ligne One Drive

- des outils collaboratifs Teams, Yammer et SharePoint.

En tant qu’association, vous pouvez bénéficier de tarifs préférentiels (via Solidatech ou autres programmes Microsoft)

## Service de sauvegarde

**Sauvegarde serveur :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Poste concerné** | **Logiciel utilisé** | **Données sauvegardés** | **Type de Sauvegardes** | **Support** |
| Serveurs | Veeam Backup Community Edition | VM complètes (serveurs)  **Sur ESXI** | Image complète VM + Incrémentiels | **NAS-EVA**  Synology DS220+  2 x 1To Raid1 |

**Veeam Backup pour Vmware (installé sur le serveur EVAVEE) :** solution de sauvegarde fiable et simple pour sauvegarder vos VM (serveurs) sous environnement VMware vSphere

**PRA (Plan de Reprise d’Activité) :**

**Veeam Backup permet un PRA.**

La sauvegarde consiste à réaliser une image complète de votre système (serveur) de façon à restaurer l’image en cas de sinistre.

Le **PRA** permet d'assurer, en cas de panne majeure de son serveur, sa reconstruction et la remise en route des applications supportant l'activité d'une organisation.

Le **P**lan de **R**eprise d'**A**ctivité (**PRA**) doit permettre, en cas de sinistre, de basculer sur un système de relève capable de prendre en charge les besoins informatiques nécessaires à la survie de l'entreprise. Il existe plusieurs niveaux de capacité de reprise, et le choix doit dépendre des besoins exprimés par l'entreprise.

**Sauvegarde des données utilisateurs :**

En environnement RDS/TSE, les données utilisateurs sont stockés sur les serveurs qui sont eux-mêmes sauvegardés.

# Postes utilisateurs

Le parc informatique est composé de PC et **18 clients légers** Wyse.

|  |  |
| --- | --- |
| **Nombre de postes PC :** | **9 (portable)** |
| **Nombre de postes MAC :** | **0** |
| **Nombre de clients légers :** | **18** |
|  |  |
| **Systèmes d’exploitation :** |  |
|  |  |
| **Bureautique (MS Office, libre Office) :** | **Office 2010 Standard** en RDS/TSE |
| Logiciel de messagerie (outlook..) : | Outlook 2010 |
|  |  |
| Applications métiers : | **Sur serveur RDS/TSE**  EIG  GTC, Previsoft, Sirius  **Applications Web (SAS) :**  Ageval  Mediteam  Octime |

**Recommandations (optimisation)**

Passer à **Microsoft365** pour optimiser l’utilisation des logiciels de bureautique.

qui permet de bénéficier de **version de pack Office récent** (Word, Excel, Outlook..)

En tant qu’association, vous pouvez bénéficier de tarifs préférentiels (via Solidatech ou autres programmes Microsoft)

# Applications métiers

EIG

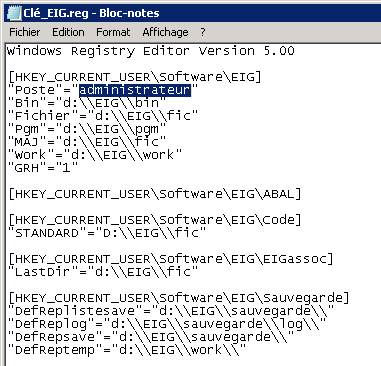
**Installé sur le serveur EVARDS**

Support technique : 05 56 75 59 15

**Procédure d’installation :**

**Depuis juillet 2021, GPO intègre directement l’utilisateur à EIG.**

1. Ajouter l’utilisateur membre du groupe AD **EIG-Acces-et-raccourci-Bureau-RDP**
2. Relancer la session TSE.
3. Il faut ensuite appeler EIG pour qu’il créé un compte sur l’application EIG (le compte doit correspondre au login Windows de la session TSE).
4. En administrateur, refuser la GPO Restrictions TSE pour l’utilisateur. Copier le fichier D:\EIG\ Clé\_EIG.reg sur le bureau de l’utilisateur. Modifier le fichier reg en remplaçant administrateur par le login Windows de l’utilisateur.



1. Ouvrir la session utilisateur et exécuter le fichier reg. Supprimer le fichier reg. Fermer la session.
2. En administrateur, supprimer le refus d’application de la GPO Restrictions TSE.

7- Relancer la session utilisateur.

**Sauvegarde :** via l’image serveur.

Octime

**Application Web (SAS)**

Support technique : 05 59 38 35 35

Mediteam

**Application Web (SAS)**

A terme : va remplacer EPSILOG

Ageval

**Application Web (SAS)**

Logiciel de pilotage de la qualité et de la gestion des risques

Poste GTC

1. Société Lamatherm
   1. Contact : Saad JEMAL - [s.jemal@lamatherm.fr](mailto:s.jemal@lamatherm.fr)
2. Société SOPCZ
   1. Contact : M.Crozat - [ccrozat@sopcz.com](mailto:ccrozat@sopcz.com)

PC en IP fixe : x.x.x.x

Sirius

**Installé sur un poste local (cuisine)**

Support technique :

**Fonctionnement :** PC installé en cuisine relié avec un modem USB pour contrôle des températures.

**Procédure d’installation :** aucune information.

**Sauvegarde :** pas de sauvegarde.

# Télécoms

Le service de téléphonie IP est géré par **RECOM** via le système de téléphonie sur IP 3CX.



# Conclusion

Suite visite préventive du 29/01/2025 – Clément Benard :

Travaux réalisés :

Maintenance sur le serveur RDS qui présente des lenteurs (installation en cours nouvelle version anti-virus)

Mise à jour DSM du Nas.

Mise à jour dossier technique (il y a beaucoup de changement notamment sur le réseau et la téléphonie géré par RECOM)

Il nous reste à mener les actions suivantes :

Redémarrage des serveurs en HNO (programmé au soir)

Faire des tests sur le serveur RDS.

Migration de mail bientôt à prévoir ainsi que le remplacement des postes (faire le point avec Marie)