**Rapport Audit infrastructure Brass Elves**

1. **Infrastructure de notre client**

Deux hyperviseur ESXI

ESXI LILLE ADMIN et ESXI LILLE PROD

**Machine virtuelle** :

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

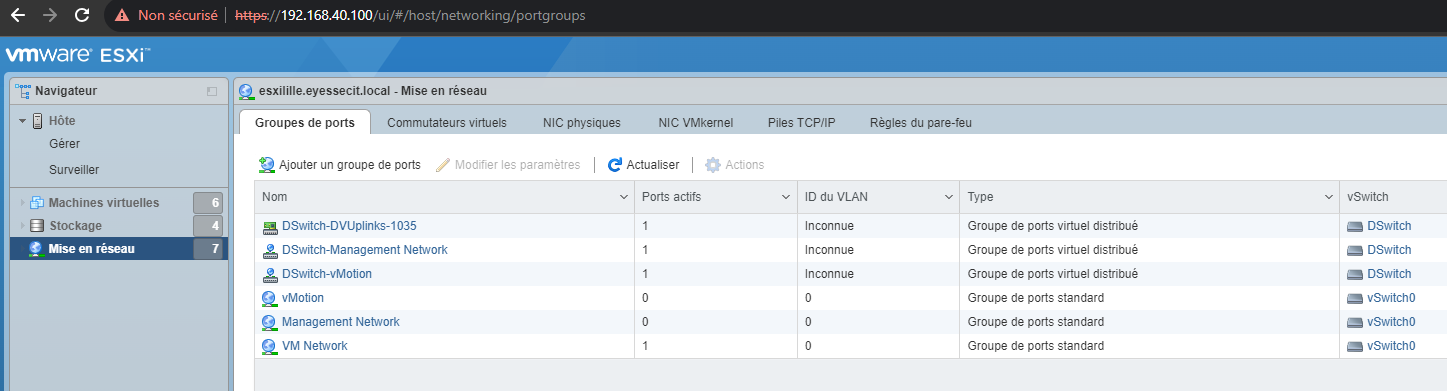
Description générée automatiquement

**Stockage** :

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement

**Réseau** :



**Machines virtuelles** :

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement

**Stockage** :

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement

**Réseau** :

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement

1. **Redondance**

Réplication AD > inexistent > créer un serveur qui s’occupera que de la réplication, et dans l’idée sur un réseau différent voir dans le cloud

1. **Ressource & droits**

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

Description générée automatiquement Ressource de la vm AD non suffisante

Aucune licence sur le serveur

Une image contenant texte, capture d’écran, Bleu électrique, bleu

Description générée automatiquement

Espace disque restant : 10,5 giga

* Incohérence de droits
* Tous les utilisateurs sont membre du groupe utilisateur du domaine sauf Fabian HOERNER pourquoi ?
* Pas de groupe créer dans l’unité d’organisation

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

Description générée automatiquementUne image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

1. **RDP** :

Aucun utilisateur autorisé à se connecté > donc le rdp est actif pour quelle raison ?

Port 3389 laissé par défaut

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

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

Description générée automatiquement

Recommandation RDP :

* Autorisé uniquement les utilisateurs ayant le besoin de se connecter
* Modifier le port par défaut
* Mettre en place une solution de sécurité lié au rdp (crowdSec)

1. **Serveur DNS**

Zones de recherche direct eyesecit.local :

Une image contenant texte, capture d’écran, nombre

Description générée automatiquement

Tous les services installés ont bien un enregistrement de type A

Zone de recherche inversée : bien configuré également

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

1. **Partage réseau**

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

Description générée automatiquementLecteurs partagés : C:\Commun

* Mauvaise pratique de l’utilisation d’un lecteur réseau mit en C :
* Non recommandé d’après la méthode AGDLP
* Droit incohérent sur le dossier partagé commun
* L’utilisateur Fabian a le contrôle total sur le répertoire

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

Description générée automatiquementUne image contenant texte, capture d’écran, affichage, nombre

Description générée automatiquement

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

Description générée automatiquement

1. **Firewall & SSH**

* Règle entrante sur le pare feu : 55 sans description
* Test de connexion en ssh avec l’utilisateur david sur le port 55
* Connexion refusé avec l’utilisateur David ainsi que son mot de passe



1. **Recommandations générales**

* Mettre en place une autorité de certificat
* Déployer des certificat SSL pour chaque service
* Réalloué les ressources de votre vm Active Directory (latence rencontré lors de l’utilisation)
* Mettre en place la réplication de l’active directory
* Désactiver le remote desktop protocol si cela n’ai pas utilisé & ou mettre en place une solution de sécurité
* Créer un groupe dans votre foret
* Sauvegarde : mettre en place une solution de sauvegarde pérenne ( shadow copy pour les fichier et répertoire des utilisateurs, Veeam backup ou autre pour sauvegarde votre machine virtuelle)
* Externalisé les sauvegardes