IUT Réseaux et Télécommunication

Marseille – Luminy

CEOS Network

Projet TPR1 – IUT Aix-Marseille

MOUMDJIAN- PERDIGON – PECHEUX - MENGUY

Sommaire

Table des matières

CEOS Network

Qui sommes-nous ?

L'entreprise CEOS Network est une multinationale d'origine marseillaise créée en 2022 à la suite de la rencontre de 4 rêveurs souhaitant révolutionner le monde du numérique. De par l'apport de nouvelles technologies innovantes lors de réalisations de projets tout en restant adapté aux besoins du client. Les principaux membres de cette entreprise son monsieur PERDIGON actuel CEO accompagné de monsieur PECHEUX dans sa qualité de Chief information Officer mais aussi en représentant du personnel. Ils sont épaulés aussi par monsieur MOUMDJIAN ainsi que monsieur MENGUY respectivement responsable des finances et de la communication à l'international.

Notre activité principale

L'installation d'un parc informatique ne s'improvise pas, encore moins sa maintenance. Un spécialiste comme CEOS Network dispose des compétences nécessaires pour configurer efficacement vos matériels informatiques. Nous avoir à vos côtés c'est l'assurance d'avoir une continuité dans vos opérations qui se dérouleront dans les meilleures conditions.

Pour toute création de nouveaux locaux, rénovation, déménagement … CEOS Network vous propose des solutions systèmes et réseaux fiables, adaptées à vos besoins, sur mesure et bien sûr évolutives en fonction de votre organisation.

Le réseau est le point central du système d'information au sein de votre entreprise ; cet ensemble de câbles va relier les différents éléments informatiques tels que : les serveurs, les ordinateurs, les solutions WIFI …

Nous contacter

Il est possible de nous contacter via :

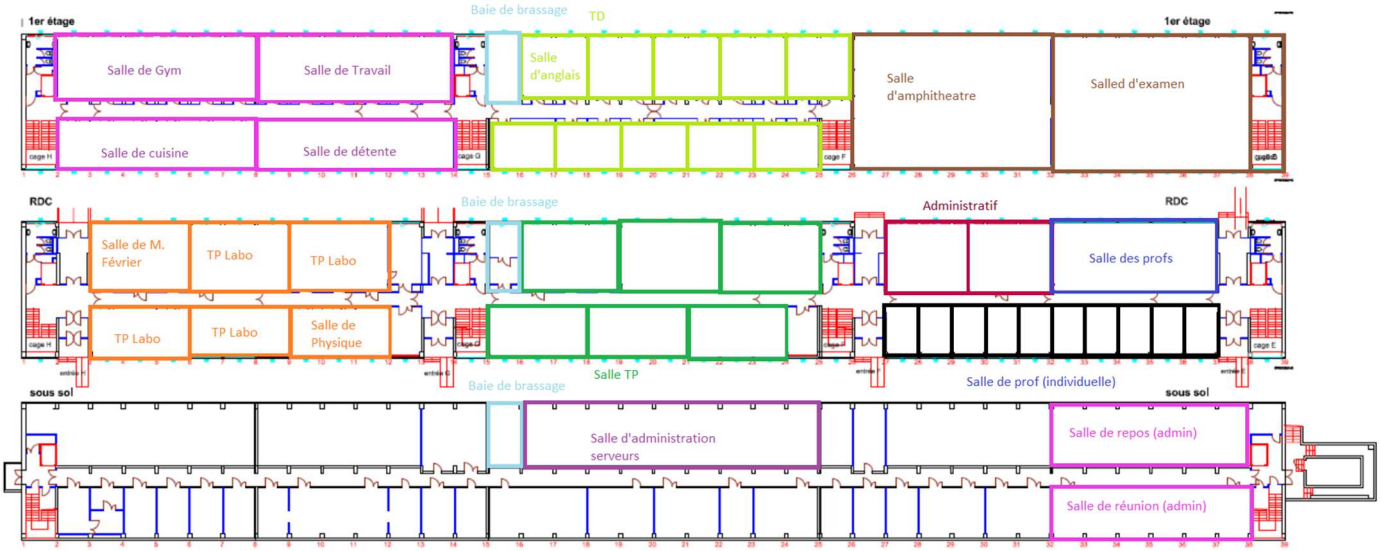
- Notre site internet https://ceosnet.fr
- Instagram : https://www.instagram.com/ceosnetwork/
- YouTube: https://www.youtube.com/@ceosnetwork

Projet TPR1

Introduction

CEOS Network a eu l'occasion de participer à la réalisation de ce projet via un appel d'offre posté sur internet par l'université Aix-Marseille. Celle-ci souhaitait rénover et déplacer l'institut Universitaire Technologique de Réseaux et Télécommunication qui serait amené à s'installer dans le nouveau bâtiment dénommé TPR1. Ce nouveau bâtiment possède la capacité d'accueil de 400 personnes en simultané. Les consignes étant les suivantes, CEOS Network devait faire en sorte que l'IUT puisse accueillir ses étudiants dans différents types de salles. On y compte 3 grands types de salles, dans un premier lieu les salles de TD devant accueillir 40 personnes, puis les salles de TP ayant la capacité d'accueil de 20 personnes et enfin de grandes salles dont la capacité sera de 100 personnes (amphithéâtre et salle d'examen). L'université nous a demandé la réalisation complète de son plan réseau ainsi que son infrastructure système.

Plan



Plan de l'organisation des salles du nouveau bâtiment

Ce plan a été réalisé de manière minutieuse pour optimiser l'espace à disposition. Au sous-sol le personnel de l'IUT pour d'ailleurs retrouver la salle d'administration des serveurs et du matériel réseau ainsi qu'une salle de repos pour les administrateurs systèmes et réseaux mais aussi une salle de réunion. Au premier étage, seront situés les salles de TP qui seront équipés des ordinateurs nécessaires à la réalisation de ces derniers. On y trouvera aussi le côté administratif ainsi que les bureaux des professeurs mais aussi la salle des professeurs équipé du matériel dont ils ont besoin dont ils auront besoin.

Au 1e étage nous trouverons une salle de gym juxtaposée d'une salle de travail équipée de livres, on pourra aussi y retrouver une salle de cuisine à disposition des étudiants ainsi que du personnel administratif et des professeurs tout en comptant une salle de détente. Cet étage comportera aussi des salles de TD, une salle d'examen et un amphithéâtre. Chaque étage disposera d'une baie de brassage.

Conception hiérarchique des réseaux

Architecture

L'architecture globale que CEOS Network propose se présente de la manière suivante, on y trouve un total de 2 arrivées extérieurs de 2 opérateurs différents ici RENATER et Orange pour accroître la résilience. Derrière ces arrivées se situeront 2 Firewall logiques, un pour la zone FRONT et un pour la zone BACK.

Zone FRONT

Dans la zone FRONT seront exposés les serveurs destinés à Internet notamment un reverse proxy pour le VDI ainsi qu'un autre reverse proxy concernant la messagerie mail. Chaque serveur possèdera une adresse IP publique allouée afin de supprimer le problème lié au NAT ainsi que de maximiser les performances tout en laissant croire à de potentiels assaillants que ces serveurs sont indépendants et décentralisés. Ils seront liés au Firewall BACK pour permettre un accès au serveur de mail et VDI.

Zone BACK

La zone BACK est destinée à la gestion de la zone FRONT mais aussi du LAN : étudiants ; professeurs ; Système d'Information ; personnel, ainsi que du datacenter et l'interconnexion avec les autres sites AMU.

Le modèle hiérarchique côté LAN

Nous avons opté pour un réseau à modèle hiérarchique dans le cadre de ce projet, car cette approche éprouvée présente de nombreux avantages. En plus de permettre une meilleure compréhension de l'infrastructure et une plus grande modularité du réseau, le modèle hiérarchique offre des temps de réponse plus rapides pour les équipements centraux et une optimisation accrue qui réduit les coûts.

Notre modèle comporte 3 couches, une couche cœur, une couche de distribution et enfin une couche d'accès.

Le cœur de réseau

La couche cœur est le niveau le plus central du modèle hiérarchique et son rôle principal est d'assurer une connectivité à haut débit entre les différents réseaux connectés au réseau central en commutant et en routant les paquets de données. Elle joue un rôle crucial dans la résilience du réseau en fournissant des mécanismes de redondance et de failover pour garantir une disponibilité maximale du réseau. En cas de panne d'un équipement ou d'une liaison, la couche cœur assure la continuité de la communication en routant les paquets de données vers des itinéraires alternatifs. Le site de Luminy possédera comme fournisseur d'accès internet à la fois RENATER et Orange pour profiter d'une couverture en cas de panne de l'un ou de l'autre. Cette couche cœur est représentée par les Firewall BACK.

La couche de distribution

La couche de distribution se situe entre la couche d'accès et la couche cœur du modèle hiérarchique et a pour rôle principal de fournir une agrégation du trafic provenant de la couche d'accès et de le distribuer efficacement vers la couche cœur.

Elle est donc chargée de regrouper le trafic en provenance de plusieurs équipements d'accès et de l'envoyer vers la couche cœur pour une commutation et un routage ultérieur. Elle filtrera et contrôlera le trafic pour bloquer ou autoriser certains types de trafic sur le réseau. La couche de distribution mettra également en place des politiques de QoS pour garantir un débit minimal ou une priorisation de certains types de trafic, tels que la voix ou la vidéo en temps réel, pour garantir une expérience utilisateur optimale. Enfin, elle assurera la sécurité du réseau en mettant en place des fonctions telles que la segmentation du réseau (VLAN voire plus loin) et la détection d'intrusion pour prévenir les attaques externes et internes sur le réseau.

La couche de distribution de la solution proposée et mise en place par CEOS sera composée, du cluster de firewall back, de switch QSFP+ connectés avec les switch de la couche d'accès ainsi que du contrôleur WiFi.

Le LAN et le WAN seront séparés, dans notre démarche d'utiliser dans le cadre du possible un maximum d'open-source, par un Firewall OPNsense. Ils se chargeront de l'interconnexion WAN ←→ LAN.

La couche d'accès

La couche d'accès est la couche la plus proche des utilisateurs et des périphériques finaux tels que les ordinateurs de bureau, les téléphones IP, les caméras de sécurité, etc. Son rôle principal est de fournir une connectivité locale aux utilisateurs et de connecter les périphériques finaux au reste du réseau.

Plus précisément, la couche d'accès sera responsable de l'acheminement des paquets de données à destination et en provenance des périphériques finaux, tels que les ordinateurs personnels et les téléphones IP. Elle utilisera le Wi-Fi pour permettre aux utilisateurs de pratiquer le BYOD, le câblage Ethernet ou les liaisons optiques pour fournir une connectivité locale aux utilisateurs finaux. La couche d'accès est également chargée de fournir des services de commutation de paquets pour permettre aux périphériques de communiquer entre eux et avec le reste du réseau.

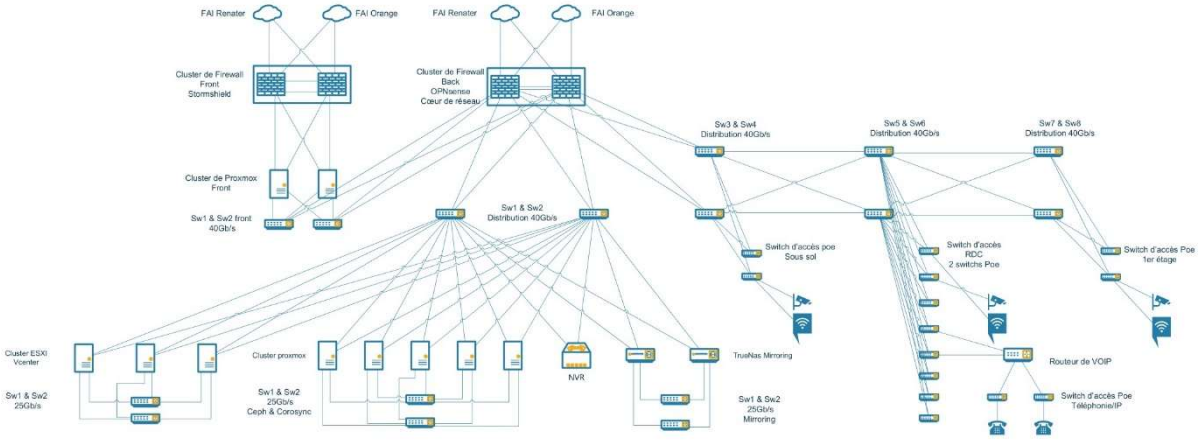


Schéma global de l'architecture

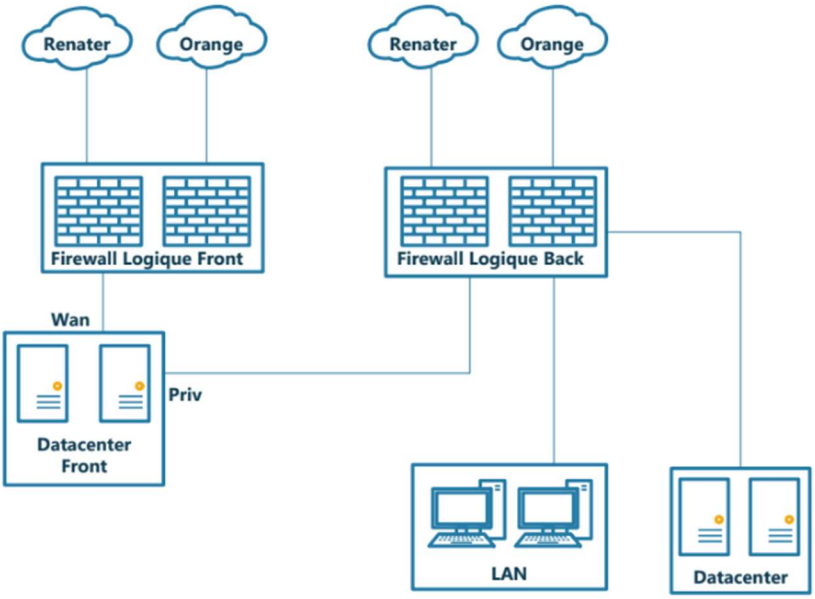


Schéma synthétique de l'architecture

Plan d'adressage

Plan d'adressage IPv4

IPv4 - 172.20.0.0/16			
VLAN ID	**Nom**	**Réseau**	**CIDR**
10	Vlan ETUDIANTS	172.20.10.0	24
20	Vlan PROFS	172.20.20.0	24
30	Vlan SI	172.20.30.0	24
40	Vlan ADMINISTRATIF	172.20.40.0	24
50	Vlan TOIP	172.20.50.0	24
60	Vlan CAMERAS	172.20.60.0	24
70	Vlan ACCESS	172.20.70.0	24
80	Vlan WIFI	172.20.80.0	24
90	Vlan INTERCO_FW	172.20.90.0	30
100	Vlan COROSYNC	172.20.100.0	29
101	Vlan CEPH	172.20.101.0	29
102	Vlan Mirroring	172.20.102.0	30
103	Vlan AUTH	172.20.103.0	30
104	Vlan SURVEILLANCE	172.20.104.0	24
105	Vlan WEB_FRONT	172.20.105.0	24
106	Vlan WEB_BACK	172.20.106.0	24
107	Vlan PASSAGE	172.20.107.0	24
108	Vlan PRINT	172.20.108.0	29
109	Vlan MAIL_PRIV	172.20.109.0	29
110	Vlan MAIL_FRONT	172.20.110.0	24
111	Vlan FRONT_VDI	172.20.111.0	24
112	Vlan VDI	172.20.112.0	24
113	Vlan Déploiement	172.20.113.0	30
114	Vlan Administration	172.20.114.0	24

Plan d'adressage IPv6

IPv6 - 2001:660:5402::/48			
VLAN ID	**Nom**	**Réseau**	**CIDR**
10	Vlan ETUDIANTS	2001:660:5402:1::	64
20	Vlan PROFS	2001:660:5402:2:::	64
30	Vlan SI	2001:660:5402:3::	64
40	Vlan ADMINISTRATIF	2001:660:5402:4::	64
50	Vlan TOIP	2001:660:5402:5::	64
60	Vlan CAMERAS	2001:660:5402:6::	64
70	Vlan ACCESS	2001:660:5402:7::	64
80	Vlan WIFI	2001:660:5402:8::	64
90	Vlan INTERCO_FW	2001:660:5402:9::	64
100	Vlan COROSYNC	2001:660:5402:A:0::	64
101	Vlan CEPH	2001:660:5402:B::	64
102	Vlan Mirroring	2001:660:5402:C::	64
103	Vlan AUTH	2001:660:5402:D::	64
104	Vlan SURVEILLANCE	2001:660:5402:E::	64
105	Vlan WEB_FRONT	2001:660:5402:F::	64
106	Vlan WEB_BACK	2001:660:5402:10::	64
107	Vlan PASSAGE	2001:660:5402:11::	64
108	Vlan PRINT	2001:660:5402:12::	64
109	Vlan MAIL_PRIV	2001:660:5402:13::	64
110	Vlan MAIL_FRONT	2001:660:5402:14::	64
111	Vlan FRONT_VDI	2001:660:5402:15::	64
112	Vlan VDI	2001:660:5402:16::	64
113	Vlan Déploiement	2001:660:5402:17::	64
114	Vlan Administration	2001 :660 :5402 :18 ::	64

CEOS Network a décidé pour le plan d'adressage du nouveau bâtiment mis à disposition de l'IUT, de séparer minutieusement les réseaux pour des besoins spécifiques comme exposé ci-dessus avec chaque tableau. L'adresse de réseau IPv4 sera 172.20.0.0/16, nous avons choisi une adresse de classe B afin d'avoir un maximum de VLAN à notre disposition dans l'optique d'une séparation du réseau. Quant à l'IPv6 CEOS Network a tenu à se tenir aux préfixes déjà fournis tout en ayant les VLANs.

Implémentation LAN

LAN Utilisateur

Le LAN est séparé en plusieurs VLANs, dont le routage inter VLAN pour une communication entre les différents systèmes et appareils du réseau, est assuré par les Firewall Back (OPNsense) faisant office de cœur de réseau. Ce sont eux qui vont permettre la sortie vers le WAN. Puis on trouve derrière eux des switch que l'on nomme de distribution. Nous avons choisi d'avoir des liens fibres QSFP+ (40 Gbps) entre chaque équipement réseau pour avoir la meilleure performance possible sur le réseau de l'IUT et éviter la congestion qui serait causée par d'un trop grand trafic entrant et sortant, jusqu'aux switch nommés « d'accès » qui sont directement reliés au plus proche de l'utilisateur ou alors à des bornes Wi-Fi qui permettent l'accès à des utilisateurs de type nomades.

Ce schéma est appliqué à n'importe quel étage du bâtiment avec les mêmes équipements listés ci-dessous :

1. Firewall « Back » : NCA-6520 hébergeant OPNsense accompagnés de module QSFP+
2. Switch de distribution : C9500-12Q-A comportant 12 ports QSFP 40 Gbps
3. Switch d'accès : C9300-48T-A \ Switch PoE : C9300-48P-E accompagnés de modules QSFP+

De plus, la partie administrative et le sous-sol seront équipés de téléphones, incluant donc un routeur Cisco destiné à la VoIP.

StackWise

Par souci de redondance et de simplicité de configuration, les switch Cisco de la gamme Catalyst 9300 ont paru être une solution efficace pour une production massive, grâce à la technologie StackWise propriétaire Cisco. L'utilisation de cette technologie lors de stacking de switch leur permet d'apparaître comme un seul ensemble et de partager une configuration et des ressources communes.

Un des avantages de StackWise est aussi sa simplicité de mise en place, il suffit d'utiliser le cable adéquat afin de relier les switchs entre eux puis de configurer StackWise en ligne de commandes.

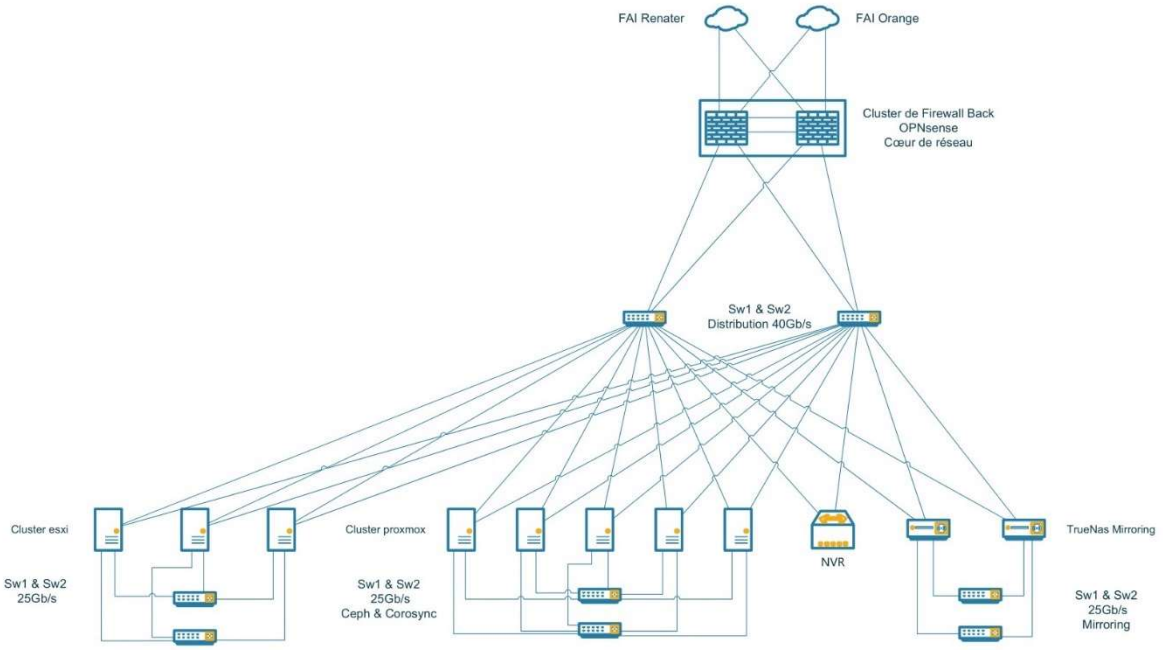
Quelques prérequis :

- Les deux switches du pair Cisco StackWise Virtual doivent être directement connectés l'un à l'autre.
- Les deux switches du pair Cisco StackWise Virtual doivent être du même modèle
- Les deux switches du pair Cisco StackWise Virtual doivent avoir la même licence
- Les deux switches du pair Cisco StackWise Virtual doivent avoir la même version
- Les deux switches du pair Cisco StackWise Virtual doivent utiliser le même modèle SDM (Switching Database Management).
- Tous les ports utilisés pour configurer un lien StackWise Virtual (SVL) doivent avoir la même vitesse. Par exemple, vous ne pouvez pas configurer simultanément un port 10G ou un port 40G pour former un SVL.

StackWise est également conçu pour améliorer les performances des équipements. En utilisant la technologie de mise en mémoire tampon distribuée, les switches empilés peuvent répartir les ressources de la mémoire tampon entre les ports, améliorant ainsi la vitesse et la fiabilité des transferts

de données. StackWise propose des avantages comme la gestion du Spanning Tree Protocol, l'élection d'un nouveau maître dans la pile grâce au Dual-Active-Detection en cas de non-réponse de ce dernier, il supporte aussi EtherChannel permettant plus de redondance et de débit.

LAN Datacenter



Topologie LAN Datacenter

Le LAN Datacenter est relié au pare-feu logique BACK ce dernier permet la communication entre le LAN utilisateur et celui-ci. On y retrouve deux switch de distribution qui assure l'acheminement des paquets jusqu'aux serveurs Proxmox avec un débit de 40Gbps grâce aux liens fibres QSFP+.

Les serveurs Proxmox sont reliés entre eux grâce à deux switch avec deux VLANs pour assurer une sécurité, séparer le réseau corosync de synchronisation du cluster, ceph pour le stockage distribué et par souci de redondance.

Quant aux TrueNAS, le mirroring est assuré par deux switch, également pour assurer la redondance.

Le datacenter hébergera un cluster ESXI pour le VDI et sera connectée de la même manière que les cluster Proxmox et le mirroring TrueNAS, c'est-à-dire, deux NIC reliées aux switch de distribution et deux NIC reliées à deux autres switch pour l'échange de données au sein du cluster.

Le NVR qui gère l'agrégation des flux vidéo des caméras sera également dans le datacenter.

Interconnexion WAN

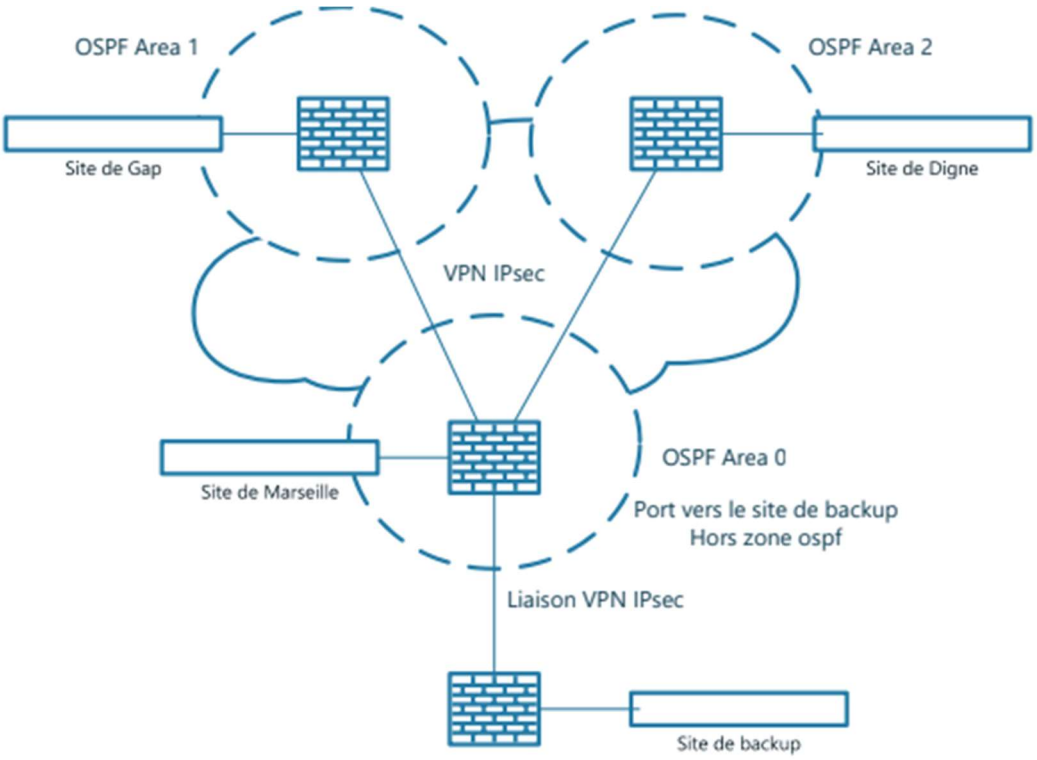


Schéma représentant l'interconnexion des sites d'Aix Marseille université avec l'IUT réseaux & télécommunications

Le datacenter du bâtiment de l'IUT sera le principal. Ce site sera donc interconnecté avec les autres IUT afin de permettre à n'importe quel élève de l'IUT d'accéder à ses données peu importe où il se trouve.

Il y aura un Active Directory en mode "listener" dans chaque campus, il recevra les mises à jour de l'AD principal situé dans le datacenter. Cela permettra de ne pas exposer l'AD principal et aussi d'avoir un annuaire répliqué sur chaque site en cas de déconnexion entre les sites, permettant une disponibilité le temps qu'une intervention soit menée.

Les contrôleurs wifi seront propres à chaque IUT, tous reliés à leur propre serveur radius, en lien avec l'AD en mode listener.

L'interconnexion des sites sera réalisée à l'aide d'un tunnel VPN IPsec entre les firewalls back de chaque site. Des règles propres au service VPN seront mises en place afin de laisser passer le trafic nécessaire. Ce VPN ne redirige pas tout le trafic, c'est-à-dire que chaque campus sera autonome quant à sa connexion avec internet.

Un VPN IPsec a été choisi plutôt qu'un VPN SSL pour garantir l'intégrité et la confidentialité des données à partir de la couche 3 du modèle OSI.

Un routage dynamique OSPF sera mis en place entre les sites afin de permettre la mise à jour automatique des routes en cas de changement, permettant ainsi de segmenter les sites par des zones OSPF. La zone 0 étant l'IUT.

Interconnexion Internet et routage extérieur

CEOS Network a fait le choix de conclure deux contrats avec Orange ainsi que RENATER pour fournir l'IUT de Luminy avec des accès extérieurs tout en permettant une résilience et un débit de 40 Gbps (limité par l'infrastructure).

Nous avons le choix d'Orange de par leur renommé dans le milieu des Fournisseurs d'Accès Internet mais aussi de par leur service client ainsi que de leur GTR (Garantie de temps de rétablissement) court.

Quant à RENATER, étant le FAI des centres de recherches ainsi que l'éducation, il nous a paru logique de les contracter dans le but de permettre aux enseignants chercheurs de bénéficier des privilèges proposés par ce FAI.

Sécurité des réseaux

Infrastructure

La totalité de l'infrastructure sera basée sur une architecture PKI, permettant à chaque actif de disposer de certificats afin de pouvoir communiquer sur le réseau. Les serveurs RA et CA seront distincts et dans un réseau différent. Seulement la RA sera accessible par les autres réseaux.

Concernant le réseau Wifi, seul le contrôleur aura besoin d'accéder à la RA.

Toutes les communications entre serveurs, clients (fixes)/serveurs seront chiffrées via certificat. Aucun équipement ne peut communiquer sur le serveur sans un certificat valide. Chaque ordinateur utilisateurs disposera de l'autorité de certification préinstallée dans son système/navigateur afin de reconnaître les sites internes et de pouvoir y accéder. **ANNEXE SERVICES NEXTCLOUD**

Serveurs

Chaque serveur sera géré par le serveur Ansible, l'accès aux serveurs se fera seulement via un utilisateur mappé + une clé publique pré partagée sur le serveur.

Les utilisateurs seront des comptes administrateur nominatifs et propres au LDAP qui ne seront pas des comptes sudo.

Les clés à courbe elliptique (ED25519) seront générées côtés clients et seront mappés dans la configuration des serveurs (~/.ssh/authorized_keys). **ANNEXE SECURITE DES SERVEURS SSH**

Le compte root restera activé et ne sera accessible que de l'intérieur via les comptes administrateurs. Le mot de passe sera donc totalement différent et partagé via un coffre-fort de mots de passe internes.

Fail2Ban sera installé sur tous les serveurs afin d'éviter les attaques en force brute. Plus de 5 tentatives sur SSH aura pour conséquence un bannissement de 1 heure.

Enfin, chaque service sera exécuté par un utilisateur non root pour garantir la sécurité en cas de compromission en évitant la latéralisation d'une attaque. Cet utilisateur sera "**gest**" et sera seulement accessible depuis l'utilisateur root. Les administrateurs devront donc se connecter avec leurs identifiants, passer en root puis basculer sur l'utilisateur **gest**.

Utilisateurs

Wifi

Tous les élèves/professeurs/personnel, auront accès au wifi du bâtiment avec leurs identifiants LDAP. Le gestionnaire de borne wifi aura accès au serveur Radius pour l'authentification. Le serveur Radius, lui, aura un accès direct et sécurisé (LDAPs) au serveur AD *listener* afin de récupérer la liste des utilisateurs. Les utilisateurs seront contraints de passer par un portail captif avant de pouvoir naviguer sur internet. L'authentification sera de type EAP-TTLS.

Lien câblé

Tous les ordinateurs seront déverrouillables avec les identifiants LDAP. Chaque ordinateur disposera d'un certificat avec le profil "PC" pour communiquer avec le réseau. Les images étant déployées dynamiquement sur le parc informatique, l'installation des certificats sera une procédure appart après l'installation du poste, qui sera géré par l'utilisateur gest.

Portail d'applications

Afin de se connecter à travers les différentes applications misent à disposition pour les élèves et les professeurs (Gitlab, Nextcloud, test…). Les utilisateurs devront se diriger vers un portail authentifiant (différent du portail captif pour la connexion sans fil). Afin de renseigner leurs identifiants LDAP. Ainsi ils auront accès à leurs applications à l'aide d'une authentification SSO via le protocole SAML, leur permettant de se logguer qu'une seule fois.

Le portail a pour rôle de reverse proxy vers les applications, de contrôle d'accès permettant de limiter l'accès à certaines applications en fonction du groupe d'un utilisateur, et le rôle de IDP (Identity Provider) pour la synchronisation des identités.

Comptes Utilisateurs

Chaque étudiant, personnel, professeur possèdera son propre compte utilisateur qui sera géré par l'Active Directory. Chaque action sera datée et stockée de manière à avoir un suivi.

Surveillance physique

Le datacenter, ces entrées et sorties seront surveillés 24h/24 par le biais de caméras de surveillance, elles même installées sur un réseau totalement appart. Le NVR devra passer par le cluster de firewalls BACK pour l'externalisation des sauvegardes vidéo.

Surveillance

La surveillance de tous nos actifs, notamment sur la détection et la réponse, sera effectuée par le serveur Wazuh. Des agents seront déployés sur chaque pc et serveurs afin de pouvoir remonter des logs et alertes au centre de sécurité opérationnel. Chaque agent devra utiliser son certificat machine pour pouvoir s'authentifier auprès du serveur.

Afin de garantir la sécurité de tous les actifs du SI. La solution Wazuh a été retenue. Un centre d'opération basé sur Ubuntu 22.04 LTS garantissant la sécurité des terminaux, de la "Threat Intelligence" le tout réuni dans un centre de sécurité facile à mettre en œuvre et à maintenir.

Un agent sera installé sur chaque poste et chaque serveur, les agents devront utiliser leurs certificats pour pouvoir s'authentifier auprès du serveur Wazuh. **ANNEXE CENTRE DE SECURITE (WAZUH)**

De plus, une sonde Sherlock aura accès à l'intégralité de nos actifs. Le principe est de pouvoir scanner les appareils connectés au réseau et de remonter les vulnérabilités. Une liste des remédiations est mise à disposition pour pouvoir prévenir de nombreuses attaques par exploitations de failles. Seul le réseau wifi ne sera pas scanner, les utilisateurs mobiles ne sont pas sous notre responsabilité. **ANNEXE SOLUTION SHERLOCK**

Interconnexion des sites

Chaque campus est interconnecté au site principal de Marseille par le biais d'un tunnel VPN IPsec sur le Firewall BACK. Chaque campus extérieur aura un serveur AD en mode "listener" et donc en lecture seule pour ne pas exposer l'AD principal.

Un VPN IPsec a été choisi plutôt qu'un VPN SSL pour garantir l'intégrité et la confidentialité des données à partir de la couche 3 du modèle OSI.

Filtrage

Zone FRONT

Les firewall FRONT filtreront et excluront tout trafic ne concernant ni la messagerie ni les serveurs WEB. Autrement dit, ils autoriseront uniquement HTTP/HTTPS, POP3, SMTPS, IMAPS. Tout autre requête n'aboutira pas. Néanmoins il sera toujours possible aux administrateurs situés dans la Zone BACK d'y accéder via SSH car les requêtes ne suivent pas le même chemin.

Zone BACK

Les Firewall BACK filtreront de manière à laisser uniquement ce qui est nécessaire au bon fonctionnement du réseau LAN et Datacenter mais aussi en fonction des besoins des utilisateurs. Le mode stateful du firewall permet de gérer automatiquement les réponses depuis l'extertieur.

Proxy

Le trafic HTTP/HTTPS vers le WAN de l'IUT sera filtré par un serveur proxy transparent utilisant Squid. Ce service est open source hébergée sur un système d'exploitation debian 11 et agit comme proxy et un cache HTTP (stocker les sites web souvent consultés afin de les renvoyer directement vers l'utilisateur au lieu d'aller chercher la ressource). Squid permettra aux administrateurs du SI de l'IUT Réseaux et Télécommunications de Luminy d'avoir un contrôle sur le trafic HTTP/S sur le réseau mais aussi de filtrer les URLs et les contenus de telle sorte à sécuriser les clients et empêcher l'accès à des liens suspects ou non autorisés sur un réseau universitaire. Quant au contrôle sur le trafic, le service donne la possibilité aux administrateurs de configurer des règles spécifiques en fonction de plusieurs paramètres tels que, le nom d'utilisateur, l'adresse IP du client, l'heure de la journée…

Le trafic sera enregistré par le service de log mis en place par Squid et sera récupéré par le puit de log Wazuh compris dans le projet de déplacement de l'IUT vers le nouveau bâtiment TPR1.

Les optimisations apportées par Squid à une infrastructure en termes d'efficacité et de performances incluent une réduction de la latence via la mise en cache citée ci-dessus, les ressources téléchargées par un client seront téléchargées sur le proxy puis redirigées vers les autres clients qui demanderont la ressource dans le futur.

En complément de Squid, sera utilisé SquidGuard, de même que Squid, ce service est open source et fonctionne comme un complément qui ajoute des fonctionnalités à Squid. SquidGuard sera utilisé dans le cadre du filtrage des URLs, en effet SquidGuard utilise des bases de données (nous utiliserons la base de filtres de l'université de Toulouse qui correspond au contexte de l'installation de ce proxy) de sites web mis à jour régulièrement pour catégoriser les sites pour les bloquer en amont. Ces blocages seront rapportés à l'utilisateur via l'envoi de pages personnalisées lorsque l'utilisateur tente d'accéder à ces ressources. Pour résumer, SquidGuard sera utilisé principalement dans l'optique de rajouter une surcouche de sécurité sur le trafic HTTP.

Reverse Proxy VDI/messagerie

Dans le cadre du projet de mise en service du bâtiment TPR1, nous mettrons à disposition un service de VDI via le service Horizon installé sur un Windows Server ainsi qu'un service de mail via Zimbra installé sur Ubuntu. De ce fait, il est nécessaire de protéger ce serveur et ne pas l'exposer directement sur internet. Un reverse proxy est donc nécessaire. Pour ce faire, Ceos Networks mettra en place NGINX comme serveur de reverse proxy.

NGINX est reconnu dans le monde de l'entreprise comme un des meilleurs reverse proxys disponibles sur le marché.

NGINX propose de nombreux services mais l'IUT sera doté du module anti-Ddos mais aussi de l'équilibrage de charge et la mise en cache du trafic.De plus, le trafic qui transite à travers le NGINX sera enregistré et transféré sur Wazuh pour le puit de logs.

Les optimisations apportées par Nginx à une infrastructure en termes d'efficacité et de performances incluent l'équilibrage de charge, la répartition intelligente du trafic entre les serveurs backend, la mise en cache des contenus statiques et la gestion optimisée des connexions SSL/TLS. En utilisant Nginx comme reverse proxy, les administrateurs peuvent assurer une haute disponibilité et une bonne résilience pour les services et applications hébergés au sein de l'IUT.
Nous avons décidé d'utiliser un service Nginx au lieu d'Apache car Nginx a été désigné principalement pour être un serveur proxy tandis qu'Apache que pour être un serveur web. Nginx est aussi capable de gérer de nombreuses requêtes clients avec une quantité de ressources à sa disposition limitée.

NGINX est donc bien plus rapide pour traiter la surcharge. En revanche Apache a une plus grande flexibilité de configuration et un plus grand nombre de modules. Pour résumer nous avons choisi NGINX car nous priorisons la performance contre la flexibilité et personnalisations qu'offre Apache2.

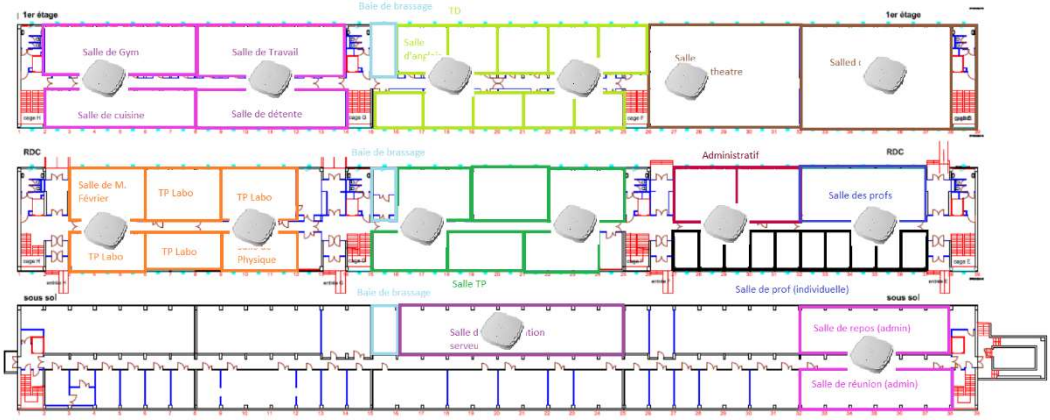
Réseaux sans fil, et mobilité

Borne Wi-Fi

Nous avons décidé d'utiliser une borne Wi-Fi Cisco Catalyst 9105 de fabrication Cisco de par sa compatibilité avec le contrôleur Wi-Fi Cisco (voir plus bas) mais aussi pour une cohérence au niveau des équipements réseaux Cisco. De plus, cette borne couvre de nombreuses technologies Wi-Fi, IEEE 802.11b, IEEE 802.11a, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, 802.11ax. Elle apporte donc la nouvelle technologie émergeante Wi-Fi 6 qui permet une meilleure gestion des applications ainsi que des flux vidéo de haute qualité.

Cette borne Wi-Fi est aussi équipée de la technologie propriétaire nommée Cisco Trust Anchor qui permet de fournir une vérification des équipements et leur authenticité dans la chaine d'approvisionnement ce qui permet d'éviter des attaques de type man-in-the-middle qui viseraient les bornes directement.

CEOS Network compte déployer un nombre de 14 bornes réparties dans le bâtiment, voire schéma ci-dessous.



Plan d'installation des bornes Wi-Fi au sein de l'IUT

Borne Wi-Fi Cisco Catalyst C9105

Contrôleur Wi-Fi

Quant au contrôleur Wi-Fi CEOS Network a décidé de fournir l'IUT avec un Cisco Catalyst 9800-L Wireless Controller pour la bande passante que l'appareil est capable de gérer qui peut aller jusqu'à 10 Gbps via Ethernet. Le contrôleur est aussi capable de supporter l'authentification EAP qui est désormais une nécessité en termes d'authentification Wi-Fi et un gage de sécurité si configuré convenablement. Bien évidemment ce contrôleur est capable de gérer les bornes Wi-Fi susmentionnées, il sera d'ailleurs présent dans le réseau Wi-Fi comme les autres bornes et sera en relation directe avec le serveur RADIUS pour l'authentification du personnel et étudiants.

Contrôleur Cisco Catalyst C9800-L

Systèmes et Equipements : Postes clients, serveurs et Datacenter

Les postes étudiants vont être des HP pro mini 260 G9 avec i5, 16Go de Ram et 512Go ssd. Ce choix a été fait pour répondre aux besoins de puissance pour faire tourner les vms que les étudiants en iut peuvent avoir besoin dans le cadre des tps.

Les postes pour l'administration vont être des HP pro mini 400 G9 avec i3, 8Go de Ram et 256Go ssd. Ce choix a été fait pour répondre au besoin du personnel administratif qui va principalement faire de la bureautique donc n'a pas besoin de la même puissance que les postes étudiants ou du SI (2 par bureau + 1 salle examen).

Les PC portables fourni aux enseignants et au SI seront des HP ZBook Firely G9 16 pouces avec un i7, 16Go de Ram et 512Go ssd. Les profs comme le SI dans le cadre d'un bâtiment dédié à de l'informatique ce doivent d'être assez puissant et de pouvoir répondre à leurs besoins pour garantir la qualité d'enseignement.

Les postes pour le SI vont être des HP elite Mini 800 G9, avec i7, 16Go de Ram et 512Go ssd. Ce choix a été fait pour avoir des tours vraiment puissantes et qui permettent aux différents administrateurs réseau, système, … de travailler dans les meilleures conditions. Des postes portables leurs seront également fournit au même titre que les enseignants.

Les serveurs d'Hypervision seront des HPe Proliant DL360 gen10 5220 avec 2x intel xeon 18 cores 2.2Ghz, 64Go de Ram et 3x500Go nvme. Ce choix a été fait en fonction de la puissance nécessaire pour faire tourner les services tout en prenant en compte les perspectives d'évolution de l'infrastructure.

Les serveurs de stockage seront eux des supermicro ssg-121e-nes24r avec un intel xeon 6416s glod de 32 cores, 128Go de Ram et 80To NVMe. Le choix des supermicro a été motivé par l'absence de raid hardware ce qui facilite la mise en place d'un système comme truenas qui gère le raid de façon logiciel de plus, d'expérience l'utilisation de cette marque pour gérer des grosses volumétries de données donne de très bons résultats.

Virtualisation

Une infrastructure de postes de travail virtuels (VDI) fait référence à l'utilisation de machines virtuelles pour fournir et gérer des postes de travail virtuels. La VDI héberge des environnements de postes de travail sur un serveur centralisé et les déploie à la demande à l'intention d'utilisateurs.

La VDI offre un certain nombre d'avantages, tels que la mobilité des utilisateurs, la facilité d'accès, la flexibilité et une plus grande sécurité. Une infrastructure de la sorte permet de faciliter le travail à distance.

Plusieurs solutions ont été comparées, en particulier :

- VMware Horizon
- Proxmox VDI

Étant dans une approche Open Source nous nous sommes d'abord penchés sur la solution de proxmox, celle-ci permet un accès à des machines virtuelles pré-installées en utilisant des identifiants PAM ou bien en lien avec un annuaire LDAP.

Cette solution nécessite donc le développement d'un script pour auto-provisionner les machines virtuelles à chaque création d'utilisateurs, en créant potentiellement des effets de bord. **ANNEXE DATACENTER VDI**

C'est pourquoi nous nous sommes orientés vers la solution de VMWare, appelée Horizon. La mise en place de cette infrastructure demande une architecture ESXI/vCenter/Windows Server. En contrepartie, Horizon fournit un service très complet et intuitif, permettant une configuration poussée. Notamment sur le clonage automatique de machine virtuelle à chaque nouvel utilisateur dans l'annuaire LDAP (AD).

Concernant les serveurs requis, il y aura :

- Un reverse proxy (pour l'accès depuis l'extérieur)
- Windows Server : Horizon Connexion Server
- Cluster ESXI (vCenter)
- Interaction avec l'AD listener

Nous avons décidé de séparer les ressources de calcul VDI de celle des serveurs Proxmox afin d'éviter des effets de bords et de ne pas avoir des machines étudiantes venant interférer avec les serveurs en production. Ainsi un cluster ESXI contrôlé par un vCenter sera installé dans le datacenter, il contiendra le serveur Horizon ainsi que les VMs étudiants.

Le comportement des VMs étudiants/professeurs via Horizon sera similaire à celui des machines physiques dans le bâtiment. Le même montage NFS sera accessible par les utilisateurs. Ils accéderont donc au serveur de connexion avec leurs identifiants LDAP.

Le reverse proxy sera donc placé dans la zone FRONT avec un accès en HTTPs au serveur de connexion Horizon. Le réseau VDI_FRONT sera utilisé pour le reverse proxy. Le réseau VDI sera utilisé par Horizon et le cluster ESXI contenant les machines virtuelles.

Les utilisateurs accéderont au service via l'adresse **https://vdi.iutrt.fr** autant depuis l'extérieur que de l'intérieur du bâtiment. En effet une surcharge DNS sera poussée sur le serveur pour les utilisateurs au sein du réseau afin d'utiliser qu'une seule adresse.

La licence utilisée pour les serveurs sera la *VMware vSphere Essentials Plus Kit 6 processeurs*. Permettant de couvrir 3 serveurs et de nombreuses fonctionnalités comme la haute disponibilité. De plus, une option de support de production (24h/24h 7j/7j) a été retenue en cas de problèmes sur les serveurs.

Hypervision

L'hypervision sera géré par un cluster de serveurs Proxmox. Créé en 2008 sur un noyau debian optimisé pour la virtualisation c'est un hyperviseur libre qui a évolué vers une infrastructure hyperconvergée et intègre plusieurs logiciels open-source type : kvm, lxc, corosync et d'autres. Les raisons de notre choix sont multiples, en effet Proxmox possède une interface graphique intuitive, respecte la démarche de CEOS Network priorisant l'open-source. Proxmox permet une Haute-Disponibilité, prend en charge Corosync et Ceph pour une synchronisation et migration des VMs. Avec un cluster de 5 serveurs dans l'optique de répartir les VMs, la haute disponibilité nous permet de perdre jusqu'à 2 serveurs tout en ayant une infrastructure fonctionnelle.

Le stockage des datas de nos services ne seront pas assurés par les TrueNAS réservés au données des personnes physiques et au VDI mais par une solution de stockage distribué intégré : Ceph

Avec 3x500Go NVMe par node, le stockage ceph sera donc de 7.5To.

La stockage distribué Ceph a été préféré au montage NFS qui pouvait être offert par les TrueNAS pour des raisons de performances, en effet la migration à chaud et la haute disponibilité va être assurés sans perte de service pour les utilisateurs. De plus les possibilités d'évolution en termes de stockage sont quasiment infinies. Une présentation de ceph et de la HA en annexe. **ANNEXE PROXMOX**

Le stockage Ceph entre les nœuds sera utilisé avec un réseau 25Gb/s dédié pour faciliter la migration à chaud et la haute dispo des Vms avec aucun temps d'interruption de services. (Plus rapide qu'un montage NFS)

Services

Serveur d'impression

Ceos Network se chargera de l'installation du serveur d'impression dans le but d'avoir une gestion efficace des imprimantes au sein du bâtiment.

Le serveur sera configuré pour répondre aux attentes des utilisateurs en termes de simplicité d'utilisation, de sécurité, une gestion des ressources disponibles et un déploiement d'imprimantes plus efficace que d'installer chaque imprimante sur chaque poste utilisateur.

Le package que nous utiliserons sera task-print-server qui installera CUPS (Common UNIX Printing System), ce dernier sera l'élément principal qui nous permettra notamment la liaison avec RADIUS dans le but de la mise en place d'une authentification. CUPS sera configuré de manière à chiffrer les flux d'impression via TLS (et certificats distribués par l'infrastructure PKI) pour garantir un chiffrement de l'impression.

CUPS contribuera au partage des imprimantes sur le réseau administratif afin d'aider les utilisateurs et administrateurs à installer les imprimantes dont ils ont besoin via le serveur d'impression.
Il contribue aussi à la gestion des ressources, le suivi de leurs états (tâches en cours) et leurs paramétrages ainsi qu'à la centralisation de la gestion de celles-ci.

CUPS est livré avec des pilotes déjà implémentés et qui correspondent aux imprimantes de la marque Brother qui seront livrées à la fin du projet dans les bureaux des professeurs, salle des professeurs ainsi qu'aux secrétariats. Quant aux secrétariats qui auront Windows comme système d'exploitation, nous installerons le paquet samba qui permettra une récupération automatique des drivers sur le serveur CUPS

Une fiche concernant les imprimantes déployées sera à retrouver en annexe de ce rapport. **ANNEXE IMPRIMANTES**

RADIUS

RADIUS (Remote Authentication Dial-In User Service) est un protocole de réseau utilisé pour la gestion de l'authentification, de l'autorisation et de la comptabilité des utilisateurs se connectant à un réseau.

Le protocole RADIUS permet à un utilisateur de s'authentifier en utilisant un nom d'utilisateur et un mot de passe auprès d'un serveur RADIUS centralisé. Le serveur RADIUS vérifie ensuite l'authentification et autorise ou non l'accès à l'utilisateur en fonction des informations d'identification fournies. L'installation de RADIUS s'effectuera sur une VM sous Linux présente dans nos serveurs DATA.

RADIUS sera utilisé dans le cadre des bornes Wifi et du serveur d'impression. Lors de la connexion à ces bornes/imprimante, le boîtier de contrôle wifi/le serveur d'impression questionnera le serveur RADIUS pour vérifier si les logins sont bien acceptés par le serveur AD. Concernant les règles de firewall, le boîtier de contrôle wifi aura accès au serveur RADIUS et celui-ci aura accès au serveur AD.

DHCP via OPNsense

Nous utiliserons la plateforme de pare-feu pour mettre en place un service DHCP (Dynamic Host Configuration Protocol). Le DHCP est un protocole réseau qui permet à un serveur DHCP de fournir des adresses IP et d'autres informations de configuration réseau à des clients DHCP, tels que des ordinateurs, des téléphones IP et d'autres périphériques réseau.

Seulement les SI auront accès à l'interface de paramétrage du pare-feu tandis que le service DHCP devrait avoir accès à tous les systèmes dans le back pour assigner les différentes adresses IP.

Les adresses des serveurs dans le datacenter seront réservés tandis que le réseau wifi et les ordinateurs en LAN auront des plages d'adresses spécifiques attribuées dans les VLAN (voir les plages d'adresses mentionnées précédemment).

Annuaire LDAP

Le serveur LDAP sera mis en place sur un Windows Server 2022. Le prix de la licence est de 6 702,28 €.

Active Directory (AD) est un service d'annuaire développé par Microsoft pour gérer l'authentification et l'autorisation des utilisateurs, des ordinateurs et d'autres ressources au sein d'un réseau informatique.

AD stocke les informations sur les utilisateurs, les groupes et les ordinateurs dans une base de données centralisée appelée annuaire. L'annuaire peut être réparti sur plusieurs serveurs pour améliorer les performances et garantir la disponibilité en cas de panne.

Grâce à AD, les administrateurs système peuvent définir des politiques de sécurité pour contrôler l'accès des utilisateurs aux ressources et surveiller les activités sur le réseau. Les utilisateurs peuvent également gérer leur propre compte, y compris leur mot de passe et leurs informations personnelles.

AD est souvent utilisé dans les environnements d'entreprise pour gérer les comptes d'utilisateurs, les ordinateurs, les serveurs, les applications et les services. Il est étroitement intégré avec d'autres produits Microsoft tels que Windows Server, Exchange Server, SharePoint et Microsoft Teams.

Nous allons également mettre en place un second serveur AD qui serait seulement en mode listener. Tous les composants du réseau utilisant le service LDAP se connectent à cette AD listener.

Ce serveur en listener copierait sa configuration AD sur le serveur AD principal qui ne serait accessible que par le serveur en listener ainsi que par les administrateurs du système.
Chaque IUT interconnecté au datacenter de Luminy disposera d'un AD en mode listener.

DNS

BIND9 sera utilisé comme service de DNS, sera hébergé sous debian 11, afin de gérer efficacement la résolution des noms de domaines pour les différents services proposés par l'IUT.

BIND9 est une solution open source fiable et robuste qui convient parfaitement à nos besoins. Comparé à d'autres solutions payantes, BIND9 offre une grande flexibilité de configuration et permet une gestion optimale des zones DNS. En choisissant une solution open source, nous respectons également notre politique de maximisation de l'utilisation de logiciels libres.
Grâce à BIND9, nous pourrons configurer des zones DNS pour l'IUT et assurer la résolution des noms de domaines pour les différents serveurs web, mails, ainsi que pour les applications utilisées par les étudiants et les enseignants.

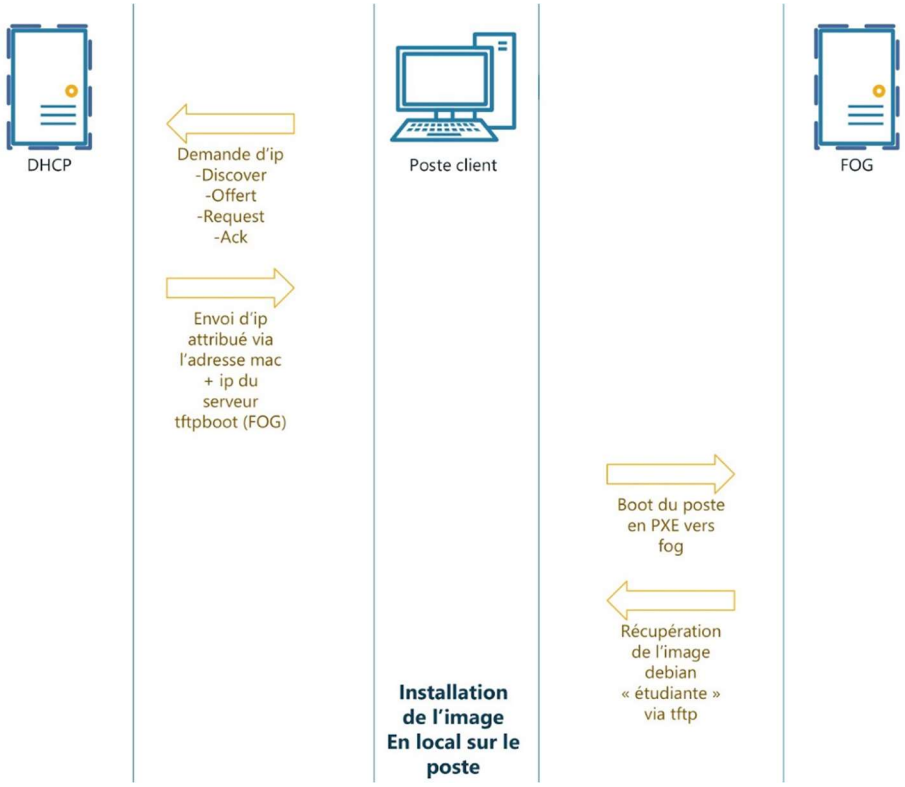
Enfin, BIND9 nous permettra également de configurer des enregistrements DNS pour les serveurs de messagerie, facilitant ainsi la gestion des adresses de messagerie pour les étudiants et le personnel administratif de l'IUT.

En somme, en choisissant BIND9 comme serveur DNS, nous optons pour une solution open source fiable et flexible qui répond parfaitement à nos besoins tout en respectant notre politique d'utilisation maximale de logiciels libres.
Les serveurs et stations auront accès à ce serveur via le port 53 pour la résolution DNS. Le serveur gérera la zone **iut.rt.fr** (seulement pour la surcharge interne) et **iut.rt.lan.**

FOG

FOG (Free Open-Source Ghost) est un serveur de déploiement open-source pour les systèmes d'exploitation Windows, Linux et macOS. FOG servira au déploiement des images des postes étudiants, prof et administratif afin de gagner en temps et permettre une facilitation de gestion.

Il utilise une architecture client-serveur pour déployer des images système sur des ordinateurs distants. Les images système sont stockées sur le serveur FOG et sont déployées sur les ordinateurs clients via le réseau. Les ordinateurs clients doivent être configurés pour démarrer à partir du réseau (boot PXE) afin de pouvoir accéder au serveur FOG et recevoir l'image système comme illustré pour les étudiants par le schéma suivant :



Via une requête DHCP classique le poste récupérera l'adresse IP associée à son adresse MAC. Une configuration au niveau du DHCP sera à effectuer lors de la réception d'un nouveau poste, il suffira d'associer l'adresse MAC à son IP et son rôle (ex : poste étudiant ici) en revanche un pc portable du personnel enseignant qui sera susceptible de sortir du bâtiment et à contenir des données subira une préparation différente avec association de son propriétaire en plus et chiffrement du disque ainsi que l'IP du serveur TFTPboot (FOG).

Différents cas de figure d'un boot :

- Tout premier boot, la machine téléchargera l'image associée au poste et l'installer en local sur son ssd/nvme
- Dans le cas où un système d'exploitation est déjà installé et stocké sur la machine en local, avant de boot sur cette image, l'ordinateur va requêter FOG pour savoir si une mise à jour de son image et disponible, si cela est le cas, la machine installera la nouvelle image puis bootera dessus. Dans le cas contraire, le PC boot directement sur l'image installée.

Fog est donc totalement approprié pour gérer des déploiements à l'échelle d'un bâtiment éducatif avec son interface web instinctive, le déploiement sur plusieurs postes en même temps via la configuration de groupe sur FOG, de plus ce service est un outil open source gratuit.
L'installation ainsi que l'utilisation de FOG est assez simple et facile à configurer permettant un bon nombre de possibilités.

Infrastructure et Services Voix et Vidéo

Le routeur utilisé pour la VoIP sera le Cisco ISR 1100-4G qui est équipé de fonctionnalités de qualité de service (QoS) avancées qui permettent de prioriser le trafic VoIP pour une qualité d'appel optimale.

Le routeur sera connecté à un switch qui sera à connecter directement aux différents téléphones.

Nous mettrons un routeur Cisco dans la baie de brassage du sous-sol qui sera connecté à un switch uniquement utilisé pour la téléphonie des étages 0 et 1.

Cisco VoIP (Voice over IP) est une solution de communication vocale basée sur le protocole IP de Cisco Systems. Cette solution utilise la technologie de VoIP pour permettre aux utilisateurs de passer des appels téléphoniques via Internet en utilisant le protocole IP. Cisco VoIP fournit des fonctionnalités avancées telles que la visioconférence, la messagerie instantanée, la présence, la collaboration en temps réel, etc.

Ce routeur installé dans la salle de serveur sera connecté à un switch à la baie de brassage du 1er étage qui connectera les différents téléphones VoIP dans les bureaux administratifs et les bureaux des professeurs.

Les téléphones seront des Cisco IP Phone 8841 choisi pour un son de haute qualité avec des fonctionnalités avancées de suppression de bruit et de réduction d'écho pour des conversations claires et précises ainsi que pour sa fonction de messagerie vocale, un répertoire et une liste d'appels pour une utilisation pratique.

Solutions logicielles, Applications réparties, outils collaboratifs

CEOS Network a décidé de mettre à disposition des étudiants et professeurs plusieurs outils de collaboration pour leur permettre de réaliser au mieux leurs différents projets. On peut compter du Cloud grâce à la solution NextCloud, un Pack Office Azure AD ou encore de la gestion de projet de développement et du running grâce à GitLab et GitRunner. Toutes ces solutions de travail collaboratif seront accessibles depuis un portail d'application dont la solution est LemonLDAP ::NG. **ANNEXE PORTAIL D'APPLICATIONS**

Le portail permettra :

- D'authentifier les utilisateurs à l'aide de leurs identifiants LDAP
- De reverse proxy toutes les applications, permettant un gain de sécurité
- D'autoriser certaines applications en fonction des groupes utilisateurs
- De fournir une solution SSO (Single-Sign-On) avec le protocole SAML

NextCloud

Nextcloud est une plateforme de stockage et de collaboration en ligne qui permet aux utilisateurs de stocker et de partager des fichiers, des calendriers, des contacts, des notes, des tâches, des flux RSS, etc. Nextcloud est une alternative open source à des services cloud tels que Google Drive, Dropbox, etc.

Nextcloud est une plateforme de collaboration et de stockage en ligne très polyvalente qui offre de nombreuses fonctionnalités. Il est également open source, ce qui signifie que les utilisateurs peuvent le personnaliser et le modifier en fonction de leurs besoins spécifiques. Nextcloud peut être installé sur un serveur privé ou utilisé comme service hébergé par un fournisseur de cloud.

Le serveur Nextcloud sera mis en place dans le réseau DATA et devra être accessible par les élèves, les profs ainsi que l'administrateur réseaux au moyen de leurs identifiants LDAP. **ANNEXE SERVICES NEXTCLOUD**

Pack Office Azure AD

Azure Active Directory est un service de gestion d'identité et d'accès basé sur le cloud, proposé par Microsoft. Il permet aux organisations de gérer les identités des utilisateurs et l'accès à des ressources telles que des applications, des fichiers et des réseaux.

Le serveur Azure AD est basé sur le cloud de Microsoft est copiera la configuration de notre serveur Windows AD en listener grâce à l'outil Azure Connect un outil fourni par Microsoft permettant la synchronisation de la configuration d'un Windows AD vers Azure AD.

Grâce à cela tous les élèves, professeurs et personnels auront accès à ce pack office grâce à un compte créé via leurs adresses mails, en lien avec leurs identifiants LDAP

Energie et refroidissement

Refroidissement

Liquide

Le refroidissement liquide est une méthode de refroidissement de l'équipement informatique qui utilise de l'eau ou d'autres liquides pour dissiper la chaleur. Cette méthode peut être plus efficace que les méthodes de refroidissement par air, car les liquides ont une capacité de refroidissement plus élevée que l'air et peuvent transporter plus rapidement la chaleur loin des composants électroniques.

Le refroidissement liquide peut être utilisé pour refroidir les processeurs, les alimentations électriques et les disques durs. Les liquides de refroidissement utilisé sera l'eau grâce à son

abondance et est capable d'absorber de grandes quantités de chaleur par sa capacité de chaleur. Elle est aussi un bon conducteur de chaleur, capable d'éloigner la chaleur rapidement.

Le refroidissement liquide peut offrir plusieurs avantages, notamment une meilleure efficacité énergétique, une plus grande capacité de refroidissement, une réduction du bruit et une meilleure fiabilité des composants électroniques. Cependant, il peut également être plus coûteux à mettre en place et nécessiter une maintenance régulière pour éviter les fuites ou les problèmes de corrosion.

En résumé, le refroidissement liquide est une méthode efficace de refroidissement de l'équipement informatique qui peut offrir des avantages importants en termes de performance et de fiabilité.

Air

Le refroidissement à air est une méthode qui utilise l'air ambiant pour dissiper la chaleur générée par les composants électroniques. L'air sera aspiré à travers des ventilateurs et des conduits, puis sera soufflé à travers les composants électroniques pour dissiper la chaleur. Les composants électroniques sont refroidis par convection, c'est-à-dire que la chaleur est transférée à l'air qui circule autour des composants.

Les avantages du refroidissement à air sont nombreux. Tout d'abord, le refroidissement à air est économique et facile à installer, car il utilise l'air ambiant disponible, sans nécessiter de liquide de refroidissement ou d'équipement supplémentaire. De plus, le refroidissement à air est généralement plus silencieux que les systèmes de refroidissement liquide, car il utilise des ventilateurs plutôt que des pompes pour déplacer l'air.

Cependant, le refroidissement à air a également des inconvénients. Le refroidissement à air est moins efficace que le refroidissement liquide dans les environnements de haute densité ou de haute performance, car il peut être difficile d'extraire suffisamment de chaleur de l'air pour maintenir les composants électroniques à des températures sûres. De plus, le refroidissement à air peut causer des problèmes de bruit, de poussière et d'humidité, qui peuvent tous affecter la performance des composants électroniques. C'est pour cela qu'il est ajouté avec le réchauffement par liquide.

Alimentation électrique

Chaque serveur possèdera deux lignes d'alimentation, la première ligne sera celle amené par EDF. Dans le cas où l'arrivée EDF se retrouve coupée, un onduleur Minerva 30kW prendra le relais de la ligne EDF. Si la coupure dure plus longtemps que la durée supportée par le premier onduleur, un deuxième onduleur APSM3330-60-9 de capacité 30 kW. En solution d'extrême urgence, un groupe électrogène suivra le deuxième onduleur.

Sécurité incendie

Le datacenter possèdera une alarme incendie qui dans un premier lieu permettra la libération de 3 gaz contenus dans des cylindres prévus à cet effet dans la salle serveur. Les gaz contenus dans ces cylindres sont le CO2 (Dioxyde de Carbone), l'Azote (N2) et l'Argon (Ar). En effet un incendie a besoin d'oxygène pour se propager et continuer à s'enflammer, un manque d'O2 par la libération de ces 3 gaz permettra d'étouffer le feu et ainsi éviter les pertes. Néanmoins ces gaz ont des inconvénients, le CO2 peut causer de l'asphyxie car il deviendra plus présent suite à l'incendie et à la libération de ce gaz dans l'air ambiant abaissant le niveau d'oxygène nécessaire au bon fonctionnement du corps en dessous du seuil mais permettant l'extinction du feu. L'Azote et l'argon comme le CO2 sont des gaz ininflammables, l'azote va venir diluer l'oxygène présent dans l'air sous le seuil permettant la combustion et favorisant l'étouffement du feu. L'argon possède les mêmes propriétés, tous deux ne déposent pas de résidus après utilisation permettant ainsi de protéger les équipements. De plus les deux derniers gaz ne participent pas du tout à la combustion comme le CO2 serait potentiellement capable de le faire. L'azote, l'argon et le CO2 combinés sont donc des bons choix économiques et efficaces pour l'extinction d'incendie dans le datacenter de l'IUT.

Stockage et Sauvegarde

Stockage TrueNAS

TrueNAS est un système d'exploitation de stockage réseau open-source qui est conçu pour fournir une solution de stockage performante, fiable et sécurisée. Il est basé sur le système de fichiers ZFS, qui offre une grande capacité de stockage et une grande fiabilité grâce à sa capacité à détecter et à corriger les erreurs de stockage.

Avantages

- Le système de fichier ZFS paraissait approprié pour du stockage de données à destination des professeurs, personnels administratifs et étudiants du bâtiment notamment grâce aux snapshots afin de réparer de potentiels erreurs utilisateurs.
- La prise en charge des protocoles NFS ou SMB fut un critère important dans la décision, là où les étudiants pourront bénéficier de montages NFS avec une image de leur poste en Debian un personnel administratif est amené à utiliser Windows et bénéficier d'un montage SMB pour leurs données.
- Le fait de disposer du raidz2 pour le stockage qui est l'équivalent logiciel du RAID6 qui permet sur nos 10 disques d'en perdre jusqu'à 2 avant de perdre de la data. Contrairement à RAID6, raidz2 va gagner en évolutivité, point important pour un bâtiment universitaire en termes de scalabilité.
- L'interface peut être qualifiée de "user friendly", elle en est donc très agréable et simple à gérer au niveau de l'administration des TrueNas.
- TrueNAS étant Open Source, et CEOS se projetant dans une démarche de priorisation de l'open source, il nous a paru logique de concevoir ce système comme une solution répondant aux besoin utilisateurs aussi par sa gratuité.
- De plus, la capabilité de TrueNAS à gérer une grande quantité de donnée est un des avantages qui nous a orienté sur cette solution.

Allocation du stockage

- Les élèves auront à disposition un lecteur réseau pour stocker VMs et documents.
- Stockage par élève : **40** Go
- 355 élèves donc 355x40 = **14,2** To
- Les professeurs auront eux aussi un lecteur réseau attitré, mais un pc portable pour leurs cours, leur stockage sera le même que ceux des élèves.
- Stockage par professeur : **40** Go
- 35 professeurs donc 35x40 = **1,4** To
- Le personnel administratif dispose d'un lecteur aussi.
- 5 personnes donc 5x80 = **400** Go
- Le SI, aura pour ses 5 admins également un lecteur
- 5 admins donc 5x200Go = **1** To
- Le VDI à un lecteur de **16** To pour le stockage des VMs

Dans un premier temps, à la livraison, l'espace de stockage sera de **33**To. Cependant il pourra évoluer en fonction des besoins utilisateurs.

Les serveurs destinés à héberger TrueNAS seront de marque Supermicro et de modèle SSG-121E-NES24R, ces derniers ont l'avantage de ne pas avoir de raid hardware implémenté qui peut entrer en conflit avec Truenas.

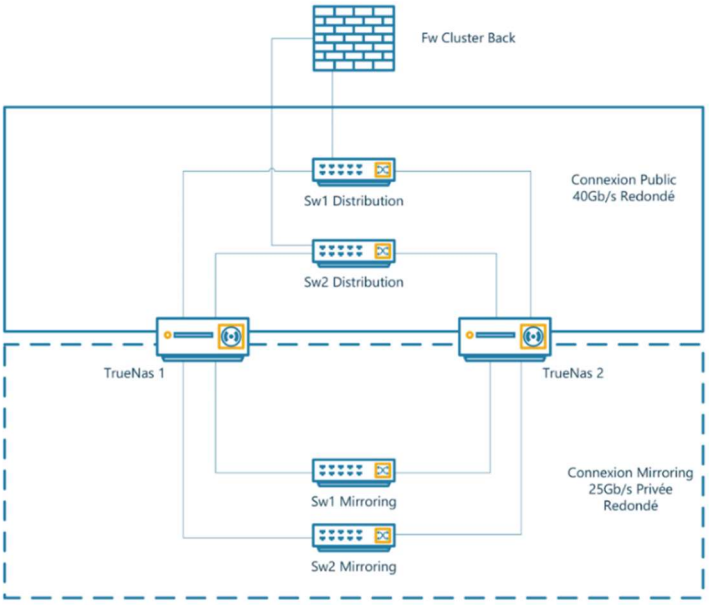
Avec 10 disques NVMe de 8To ce qui avec le raidz2 donne en stockage réel utilisable :

53.51 TiB soit 58.83TB donc 73.55% d'espace utilisable sur la prévision de **33**To alloué pour le personnel et étudiants, avec la possibilité d'aller jusqu'à 24 slots NVMe et avec une simplicité d'évolution grâce à raidz2. Nous avons donc une marge de 25,83TB de stockage sur truenas en plus des slots encore disponibles.

Au niveau de la RAM le serveur va avoir 4x32Go en DDR4 et au niveau du réseau en plus de son interface ipmi* native pour l'administration il va avoir 1 carte AOC-A25G-b2s de 2 ports de 25Gb/s ce qui est suffisant pour le mirroring et 1 carte 40Gb/s fibre pour l'accès aux données

RAID type:	RAID-Z2 (Double parity with variable stripe width)		
Number of RAID groups:	1		
Number of drives per RAID group:	10		
Total number of drives:	**10**		
Drive capacity (GB):	8000		
Drive capacity (TiB):	7.275958		
	(TiB)	**(TB)**	**(%)**
Total raw storage capacity:	72.759576	80.000000	**100**
Zpool storage capacity:	**72.500000**	**79.714593**	**99.64**
Reservation for parity and padding:	17.261905	18.979665	23.72
Zpool usable storage capacity:	55.238095	60.734928	75.92
Slop space allocation:	1.726190	1.897967	2.37
ZFS usable storage capacity:	**53.511905**	**58.836962**	**73.55**
Minimum free space:			
Practical usable storage capacity:	**53.511905**	**58.836962**	**73.55**

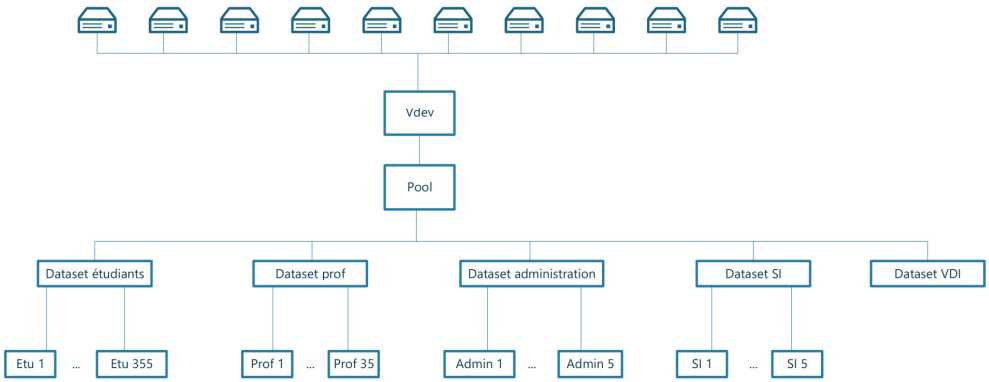
Implémentation datacenter



Définitions

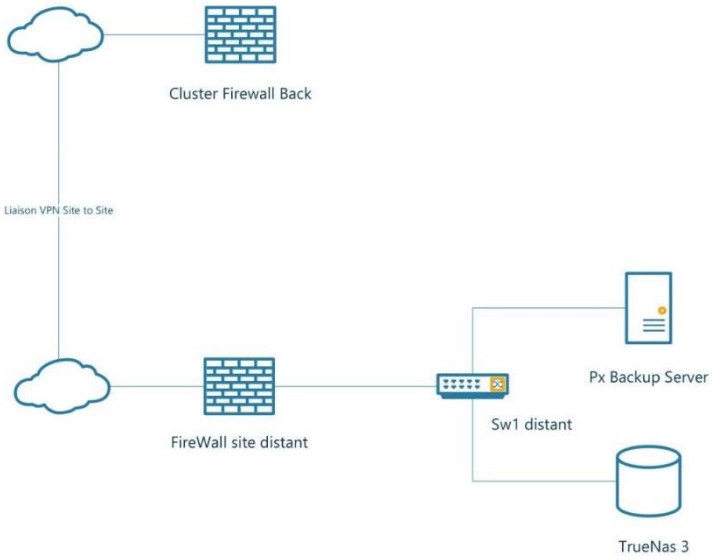
IMPI : L'IPMI (Intelligent Platform Management Interface) est un protocole de gestion à distance des serveurs qui permet d'effectuer des tâches de surveillance, de contrôle et de récupération sur des équipements informatiques sans avoir besoin d'un accès physique à ces derniers. Celui-ci passe par le réseau et offre une console de management à l'administrateur.

ZFS : ZFS est le système de fichiers utilisé par TrueNAS qui utilise ZFS pour offrir une solution de stockage de données avancée et fiable. ZFS est conçu pour offrir une grande capacité de stockage, une grande fiabilité et une protection contre les erreurs de données grâce à ses fonctionnalités de vérification de la cohérence des données, de réplication et de snapshot. TrueNAS utilise ces fonctionnalités pour garantir que les données stockées sont sécurisées, disponibles et protégées contre les erreurs.



Sauvegarde

Les sauvegardes des données étudiantes ainsi que les VMs sur lesquelles tournent les services sur le proxmox seront en plus externalisé sur un site de sauvegarde distant relié par une liaison VPN IPsec avec derrière un autre TrueNAS en mirroring pour les datas et une solution proxmox backup pour les services



Gestion et supervision

GLPI

GLPI dans le contexte de son utilisation au sein du projet de déplacement de l'IUT Réseaux et Télécommunications de Luminy vers le nouveau bâtiment TPR1 aura pour but d'avoir un suivi des incidents du parc informatique de l'IUT.

Pour ce faire, GLPI effectuera un inventaire des PCs, licences ainsi que les serveurs et imprimantes que nous installerons lors de ce projet.
GLPI a pour but premier de donner la possibilité aux utilisateurs de l'IUT, professeurs, personnel administratif ou étudiants de créer des tickets lors de la rencontre de problèmes utilisateurs.
La création de ticket est assez fournie, les utilisateurs voulant faire part d'un incident rencontré peuvent trier le type de problème, le décrire, et fournir des fichiers comme des captures d'écrans. Ces tickets peuvent être mis à jour, commentés mais aussi la durée d'activité du ticket en cours.

Nous pourrons coupler GLPI et le suivi des tickets au serveur de mail mis à disposition afin de donner la possibilité d'avoir un vrai suivi en temps réel via la messagerie pour plus de confort pour l'utilisateur concerné.

GLPI donne accès à des statistiques et rapports détaillés pour les responsables du service support afin de voir l'efficacité de ce dernier dans le but de trouver les points bloquants au sein du support avec pour optique d'améliorer la qualité du service.

Zabbix

Zabbix est un logiciel de monitoring open-source qui permettra une surveillance de serveurs, postes, équipements réseaux, application, cloud ou encore des services. Il fournit des fonctionnalités avancées de surveillance, d'alerte et de reporting pour aider les futurs administrateurs système et les opérateurs de réseaux de l'IUT à optimiser les performances des systèmes informatiques et des réseaux. Ses fonctionnalités comprennent la collecte de données, la surveillance en temps réel, les alertes personnalisables, la corrélation d'événements, la visualisation de données, la création de rapports et la gestion de la configuration. Avec une architecture flexible, Zabbix peut être utilisé pour surveiller des infrastructures informatiques de toutes tailles et de toutes complexités.

Le choix s'est porté vers cet outil en raison de son grand nombre d'intégration qui correspond à notre système : proxmox, truenas, stormshield ,opensence et autres. Mais aussi grâce à sa souplesse d'intégration avec possibilité de personnalisation suivant les besoins des administrateurs systèmes à l'aide de script.

Via la récupération des métriques par ses agents tels que ceux concernant les protocoles SNMP, HTTP, SSH, IPMI, etc il s'adapte aux besoins du client et les options supplémentaires de rapports ou d'alerte par mail, webhook et sms sont très utiles pour les administrateurs du SI.
Zabbix sera hébergé sur le cluster proxmox via un container de type LXC avec :

Nom de la techno	Template	Type	Métrics importantes
Proxmox	Proxmox VE via HTTP Ceph by zabbix agent 2 active	Http et zabbix agent 2	- -état datacenter - -état cluster ceph - -débit Proxmox et VM - -RAM et CPU utilisation Proxmox et VM - -VM Running ou off
TrueNas	TrueNas by SNMP	SNMP	- -Débit TrueNas - -RAM et CPU utilisation - -stockage des datasets
Postes étudiants/ Administratifs	Zabbix agent active	agent active	- -débit réseau - -état des systèmes - -RAM et CPU utilisation
Stormshield	Stormshield by SNMP	SNMP	- -débit réseau
OPNsense	Template OS FreeBSD	agent	- -débit réseau/VPN - -état dhcp - -Nombre de règles matchées + erreurs - -RAM et CPU

Tableau des intégrations et des métrics importantes récupérées via zabbix suite en annexe.

ANNEXE INTEGRATION ZABBIX

Grafana

Grafana est une plateforme open-source de visualisation et d'analyse de données en temps réel.
Elle permet de connecter et de collecter des données à partir de différents systèmes, tels que des bases de données, des outils de monitoring, des services cloud, etc., pour les afficher sous forme de graphiques, de tableaux et de tableaux de bord.
Grafana est également connue pour sa grande communauté d'utilisateurs et de contributeurs qui fournissent des mises à jour régulières, des corrections de bugs et des fonctionnalités améliorées pour la plateforme.
L'installation de Grafana se fera sur une VM sous Linux présente dans nos serveurs DATA. Grafana sera lié au Zabbix via une connexion à l'API de zabbix en https permettant un échange de données sécurisées. Grafana étant une plateforme Open-Source aucun achat n'est nécessaire.

Ansible

Créé en 2012, repris en 2015 par red hat et basé sur du python ansible est utilisé pour du déploiement de configuration et de gestion de parc informatique.

Avantage d'ansible : configuration des tâches et des playbooks (mappage des adresses IP avec les tâches attribuées à ces dernières) en YAML donc une simplicité de configuration, connexion SSH, pas besoin d'agent juste de python installé sur le client (peut même installer python sur un client distant via une exécution d'un script bash)

Niveau sécurité les connexions SSH depuis un bastion d'administration vers les clients et avec une gestion des secrets via vault les failles proviennent plus de problèmes de configuration par l'administrateur que de l'outil lui-même. Ansible va donc servir à la gestion des postes pour des petites upgrades, il va être un complément de FOG pour la gestion des postes étudiants et administratif avec en plus une réelle utilité dans la maintenance des serveurs, le déploiement de nouveau service et toutes les tâches qui peuvent être répétitives. La communication entre les clients et le serveur Ansible sera chiffrée et authentifiée via les certificats.

Technologie d’avant-garde

Entrées sécurisées

La sécurité du bâtiment sera assurée par un prestataire (société ARD) et par CEOS Network. En effet nous avons décidé de faire appel à eux pour le contrôle d’accès aux entrées du bâtiment et des salles de ce dernier. Le déverrouillage des portes et le verrouillage se basera sur un badge autorisé. Le contrôleur de badge au niveau de la porte sera en communication avec le contrôleur situé dans la salle du SI et ce dernier communiquera avec l’AD pour permettre une identification et l’accès aux salles au personnel enseignant ou encore étudiants. Le SI demandera une accréditation supérieure. En annexe sera disponible plus de détails concernant le système. **SECURITE PHYSIQUE**

Casier connecté

Refrigerated Locker de Parcel Pending est une solution de casier réfrigéré. Le système utilise des casiers équipés de réfrigération pour stocker les produits alimentaires périssables en toute sécurité jusqu'à ce que l'utilisateur soit prêt à les récupérer. Les casiers sont accessibles via le badge fourni à l'étudiant en début d’année. Les casiers sont à l’état fermé et peuvent être déverrouillé via le badge d’un étudiant.

L'étudiant pourrait ici stocker sa nourriture et refermer le casier. Celui-ci sera maintenant fermé et ne pourrait être ouvert que par l’étudiant qui l’a précédemment verrouillé.

Le casier est lié à notre AD et permet la vérification de l'identité du badge présenté au casier. Ce casier permettra aux étudiants de gérer leur propre alimentation en toute sécurité.

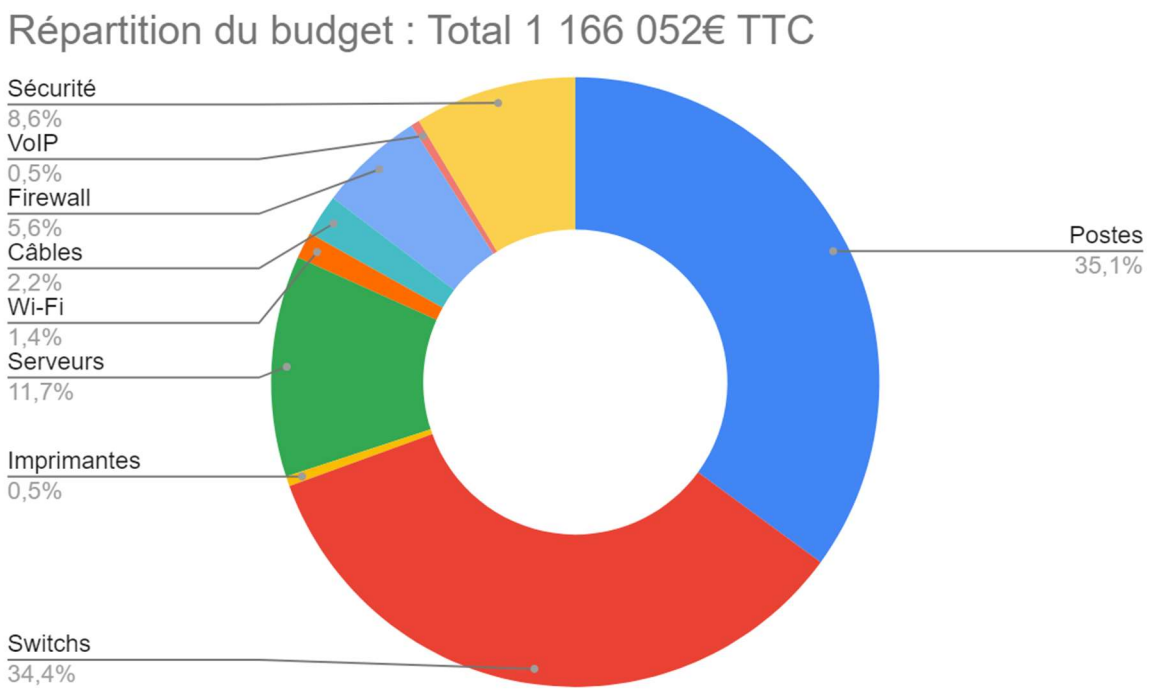
Les casiers seront vidés tous les soirs et toute nourriture trouvée sera mise dans un frigo public ou l’étudiant devra se rendre pour récupérer la nourriture.

Réservation de salle

Plusieurs salles de réunion ainsi qu’une salle de sport seront disponibles et les étudiants pourront réserver ces salles à l'avance. Grâce à Windows Active Directory les étudiants pourront observer en temps réel si une salle est réservée ou non.

La salle de sport aura une capacité maximum de 8 personnes et les réservations se feront sur des créneaux d’une heure.

Comptabilité



Graphique représentant la répartition du budget du projet en % et en €

Ce graphique permet de faire un état des lieux de l'utilisation du budget donné à CEOS Network par l'IUT d'Aix-Marseille concernant la réalisation de ce projet. Il est possible de constater que le budget a été principalement utilisé dans l'équipement réseau et peu dans les licences grâce à notre principe de priorisation de l'Open-source.

Conclusion

CEOS Network est fier d'avoir eu l'occasion de travailler sur ce projet et tiens à remercier le personnel de l'IUT Aix-Marseille pour leur confiance en notre compagnie et son savoir-faire.

ANNEXE

Charte Informatique

Objet du document

L'objet de ce document est de définir les règles d'utilisation des ressources informatiques de l'Institut Universitaire Technologique Réseaux et Télécommunications (IUT RT) afin de garantir la sécurité et la confidentialité des données et de préserver le bon fonctionnement du système d'information. Cette charte s'adresse à l'ensemble des utilisateurs des équipements informatiques de l'IUT RT, y compris les étudiants, les enseignants, le personnel administratif et technique. Elle a pour but de définir les règles d'utilisation des ressources informatiques de manière claire et précise, et de sensibiliser les utilisateurs aux risques liés à une mauvaise utilisation des équipements informatiques.

Définitions

On désignera sous le terme de réseau, un ensemble d'équipements reliés entre eux pour échanger des informations.

On désignera sous le terme ressources informatiques, les moyens informatiques de traitement de l'information ainsi que ceux auxquels il est possible d'accéder à distance à partir du réseau de l'entreprise.

On désignera par services Internet, la mise à disposition par des serveurs locaux ou distants de moyens d'échanges et d'informations diverses : Web, messagerie, forum,

On désignera sous le terme utilisateur, les personnes ayant accès ou utilisant les ressources informatiques et les services Internet.

Accès aux ressources informatiques

L'accès aux ressources informatiques de l'IUT RT est réservé aux personnes autorisées, à savoir les étudiants, enseignants, personnels administratifs et techniques de l'IUT RT. Tout accès non autorisé est interdit et constitue une violation de la présente charte.

Utilisation d'internet

L'utilisation d'internet est autorisée dans le cadre des activités pédagogiques et professionnelles de l'IUT RT. Toutefois, l'accès à certains sites web peut être restreint si leur contenu est jugé inapproprié ou illégal. Il est interdit de télécharger, d'installer ou d'utiliser des logiciels ou des applications qui ne sont pas autorisés par l'IUT RT.

Utilisation des machines virtuelles

L'IUT RT met à disposition des machines virtuelles pour les activités pédagogiques et professionnelles. Il est interdit de modifier la configuration des machines virtuelles, d'installer des logiciels non autorisés ou de supprimer des données sur les machines virtuelles sans autorisation préalable.

Service de messagerie mail

L'IUT RT met à disposition un service de messagerie mail pour les activités pédagogiques et professionnelles. L'utilisation de ce service est réservée aux personnes autorisées et doit respecter les règles de bonnes pratiques de sécurité informatique. Il est interdit d'envoyer des messages électroniques qui contiennent des informations confidentielles sans autorisation préalable.

Confidentialité de l'information utilisateur

L'IUT RT s'engage à respecter la confidentialité des informations utilisateur et à mettre en place les mesures de sécurité nécessaires pour assurer leur protection. Il est interdit de divulguer des informations personnelles ou confidentielles sur les membres de la communauté de l'IUT RT sans autorisation préalable.

Bonnes pratiques de sécurité informatique

L'IUT RT recommande aux utilisateurs de mettre en place des mesures de sécurité informatique pour protéger leurs équipements et leurs données, notamment :

- Utiliser des mots de passe forts et les changer régulièrement ;
- Ne pas partager ses identifiants de connexion avec d'autres personnes ;
- Ne pas télécharger ou installer des logiciels ou des applications non autorisés ;
- Sauvegarder régulièrement ses données ;
- Mettre à jour régulièrement les logiciels et les applications ;
- Ne pas ouvrir d'emails ou des pièces jointes provenant de sources inconnues ou suspectes.

Surveillance du système d'information

Le système d'information de l'IUT RT est surveillé en permanence pour garantir sa sécurité et son bon fonctionnement. Des mesures de traçabilité, de contrôle et d'alerte sont mises en place pour détecter toute activité suspecte ou non autorisée.

Préservation du système d'information

La préservation du système d'information de l'IUT RT est primordiale pour garantir le bon fonctionnement des équipements informatiques et la sécurité des données. Les utilisateurs doivent prendre toutes les mesures nécessaires pour protéger les équipements informatiques et les données qu'ils contiennent. À cet effet, les mesures suivantes doivent être respectées :

Protection des équipements physiques

Les utilisateurs sont responsables de la protection physique des équipements informatiques mis à leur disposition. Ils doivent éviter de les endommager et s'assurer que les équipements sont sécurisés et ne présentent pas de risques pour la sécurité des personnes et des biens

Sauvegarde des données :

Les utilisateurs doivent sauvegarder régulièrement leurs données, notamment sur des supports de stockage externes, pour éviter toute perte de données en cas de dysfonctionnement des équipements informatiques.

Gestion des accès :

Les accès aux équipements informatiques de l'IUT RT sont gérés de manière à garantir la sécurité et la confidentialité des données. Les utilisateurs doivent respecter les règles d'accès et ne pas divulguer leurs identifiants de connexion à des tiers.

Protection contre les virus et les logiciels malveillants :

Les utilisateurs doivent prendre toutes les mesures nécessaires pour protéger les équipements informatiques contre les virus et les logiciels malveillants. Ils doivent notamment installer et maintenir à jour un logiciel antivirus.

Respect des règles de sécurité :

Les utilisateurs doivent respecter les règles de sécurité mises en place par l'IUT RT. Ils doivent notamment éviter de télécharger des logiciels ou des fichiers provenant de sources inconnues ou suspectes et ne pas utiliser de matériel ou de logiciels non autorisés.

Signalement des incidents de sécurité :

Les utilisateurs doivent signaler immédiatement tout incident de sécurité ou toute tentative d'intrusion au responsable de la sécurité informatique de l'IUT RT.

Responsabilité juridique :

Les utilisateurs sont tenus responsables de tout dommage causé aux équipements informatiques de l'IUT RT et des infractions commises en utilisant ces équipements. Tout manquement aux règles de préservation du système d'information peut entraîner des sanctions disciplinaires et/ou des poursuites judiciaires.

Surveillance du système d'informations

CONTRÔLE

Pour des nécessités de maintenance et de gestion, l'utilisation des ressources matérielles ou logicielles, les échanges via le réseau, ainsi que les rapports des télécommunications peuvent être analysés et contrôlés dans le respect de la législation applicable, et notamment de la loi Informatique et Libertés.

TRAÇABILITÉ

L'Institut Universitaire Technologique Réseaux et Télécommunications de Marseille assure une traçabilité sur l'ensemble des accès aux applications et aux ressources informatiques qu'elle met à disposition pour des raisons d'exigence réglementaire de traçabilité, de prévention contre les attaques et de contrôle du bon usage des applications et des ressources.

Par conséquent, les applications de l'établissement, ainsi que les réseaux, messagerie et accès Internet intègrent des dispositifs de traçabilité permettant d'enregistrer :

- L'identifiant de l'utilisateur ayant déclenché l'opération ;
- L'heure de la connexion ;
- Le système auquel il est accédé ;
- Le type d'opération réalisée
- Les informations ajoutées, modifiées ou supprimée des bases de données en réseau et/ou des applications de l'Institut ;
- La durée de la connexion (notamment pour l'accès Internet) ;
- Création / modification des fichiers sur le systèmes d'information

Le responsable sécurité du système d'information respecte la confidentialité des données et des traces auxquelles ils sont amenés à accéder dans l'exercice de leur fonction, mais peuvent être amené à les utiliser pour mettre en évidence certaines infractions commises par les utilisateurs.

ALERTES

Tout constat de vol de matériel ou de données, d'usurpation d'identité, de détournement de moyen, de réception de messages interdits, de fonctionnement anormal ou de façon plus générale toute suspicion d'atteinte à la sécurité ou manquement substantiel à cette charte doit être signalé au Responsable de la Sécurité du Système d'information.

La sécurité de l'information met en jeu des moyens techniques, organisationnels et humains. Chaque utilisateur de l'information se doit d'avoir une attitude vigilante et responsable afin que les étudiants et les personnels bénéficient d'une utilisation sécurisée et que leur vie privée ainsi que celle des personnels soient respectés.

Rappel des principales lois françaises

La loi "Informatique et Libertés" du 6 janvier 1978 modifiée en 2018, qui encadre la collecte, le traitement et la conservation des données personnelles. Cette loi garantit les droits des individus sur leurs données, tels que le droit d'accès, de rectification et de suppression de leurs données, ainsi que le droit d'opposition et le droit à la portabilité. Cette loi a été modifiée en 2018 par le Règlement Général sur la Protection des Données (RGPD) de l'Union Européenne. Les sources officielles de cette loi sont disponibles sur le site de la CNIL : https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978-modifiee

La loi du 7 octobre 2016 pour une République numérique, qui vise à encadrer les usages du numérique et à favoriser l'accès à l'information et aux données publiques. Cette loi renforce également les droits des internautes sur leurs données personnelles et leur vie privée. Les sources officielles de cette loi sont disponibles sur le site de Legifrance : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000033202746/

Le Code pénal, qui réprime notamment les atteintes aux systèmes informatiques, tels que le piratage ou le vol de données, ainsi que les atteintes à la vie privée, tels que la collecte illicite de données personnelles ou la surveillance illégale. Les sources officielles du Code pénal sont disponibles sur le site de Legifrance : https://www.legifrance.gouv.fr/codes/id/LEGIARTI000006418984/2020-10-16/

Il convient également de prendre en compte le Règlement Général sur la Protection des Données (RGPD) de l'Union Européenne, qui s'applique à toute organisation traitant des données personnelles de citoyens européens, ainsi que les recommandations de la CNIL en matière de sécurité informatique. Les sources officielles du RGPD sont disponibles sur le site de l'Union Européenne : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A32016R0679 et celles de la CNIL sont disponibles sur son site internet : https://www.cnil.fr/fr/securite-des-donnees-les-10-bonnes-pratiques-de-la-cnil.

Responsabilités

L'attention du personnel est attirée sur le fait qu'en cas d'atteinte à un de ces principes protégés par la loi, la responsabilité pénale et civile de la personne, ainsi que celle de l'entreprise est susceptible d'être recherchée.

L'utilisateur qui ne respectera pas les règles juridiques applicables, notamment celles rappelées ci-dessus, verra sa responsabilité juridique personnelle engagée non seulement par toute personne ayant subi un préjudice du fait du non-respect de ces règles, mais aussi de l'entreprise en sa qualité d'employeur.

Annexe Sécurité des serveurs SSH

Configuration SSH des serveurs permettant l'accès uniquement par clé ED25519

```
Port 22
ListenAddress 0.0.0.0

SyslogFacility AUTH
LogLevel INFO

LoginGraceTime 10m
PermitRootLogin no
StrictModes yes
MaxAuthTries 3
MaxSessions 10

PubkeyAuthentication yes
AuthorizedKeysFile .ssh/authorized_keys
HostbasedAuthentication no
PasswordAuthentication no
PermitEmptyPasswords no
ChallengeResponseAuthentication no

UsePAM yes
AllowTcpForwarding no
X11Forwarding no
PrintMotd no
VersionAddendum none
Banner none

AcceptEnv LANG LC_*

Ciphers aes128-ctr,aes192-ctr,aes256-ctr
HostKeyAlgorithms ssh-rsa,ssh-dss,rsa-sha2-256,rsa-sha2-512
KexAlgorithms diffie-hellman-group-exchange-sha256
MACs hmac-sha2-256,hmac-sha2-512
```

Annexe Architecture PKI

Les serveurs RA et CA seront basés sur debian 11 Bullseye. La suite "*µpki*" sera utilisée.

Gestion des paquets :

- Upki CA pour l'autorité de certification
- Upki RA + Upki Web pour l'autorité d'enregistrement + gestion des certifs
- Upki CLI sera installé sur tous les serveurs/actifs du réseau.

Profils :

- server : installé sur tous les serveurs du parc (communication entre serveurs)
- pc : installé sur chaque ordinateur (communication clients sur le réseau)
- public : installé sur les serveur exposant un service aux clients/public

Construction du certificat : <profil>.<FQDN>

Exemple : server.web.iutrt.lan et certificat publique : public.web.iutrt.fr

Le profil ne sera pas apparent dans l'URL directement, il est spécifié dans cet exemple à but explicatif.

Page Github : https://github.com/proh4cktive/upki

Schéma explicatif de l'architecture PKI

Annexe Centre de sécurité (Wazuh)

L'interface de Wazuh permet une bonne compréhension quant aux concepts de Détection & Réponse.

Le serveur Wazuh aura accès à tous les serveurs/stations du réseau afin de pouvoir remonter des alertes de sécurité via mail.

Plus de détails sur les avantages de la solution :

- Sécurité des terminaux
  - Détection et réponse avancée
  - Vérification de l'intégrité des fichiers
- Threat Intelligence
  - Threat Hunting
  - Règles d'hygiène cyber
  - Détection de vulnérabilité
  - Liens avec le Mitre Att&ck
- Centre de sécurité opérationnel
  - Analyse des logs
  - Détection de malwares
- Sécurité Cloud
  - Sécurité des containers

Annexe solution Sherlock

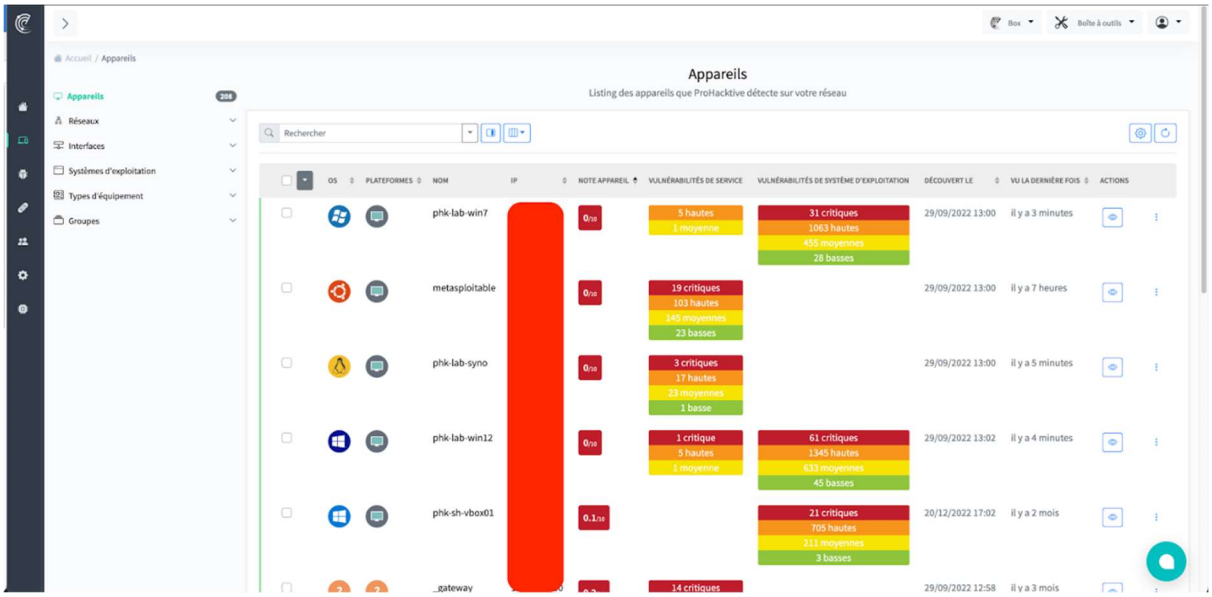
Le boîtier Sherlock est une solution d'audit permanent plug-and-play développée par la société ProHacKtive.

Afin de scanner nos actifs et de remonter les différentes vulnérabilités. La solution choisie sera une VM installée dans le datacenter. De plus, leur interface permet une bonne compréhension quant aux vulnérabilités de nos actifs et nous propose un « score » de cybersécurité. La possibilité d'exporter des rapports permet de pouvoir transmettre ceux-ci à la direction pour que tout le monde soit conscient des risques encouru en cas d'absence de correctifs. Ceos Network c'est donc orienté vers cette solution développer par des Français, ProHacKtive étant un partenaire de la société dans d'autres projets.

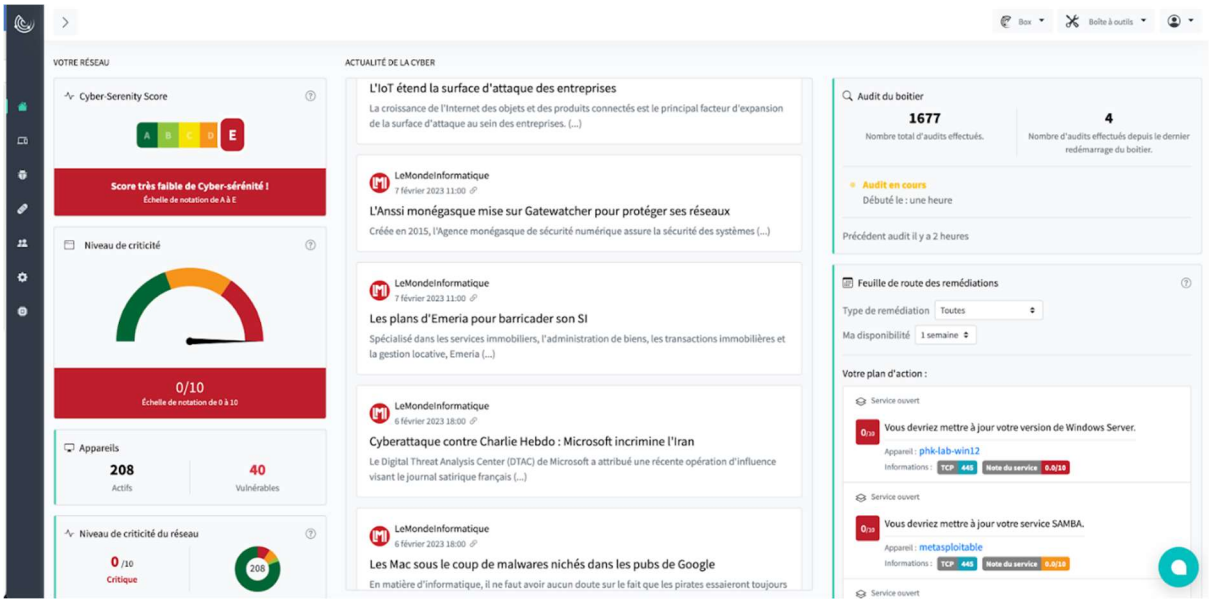
L'abonnement "Offre ETI - Grande Entreprise" a été choisi pour permettre de couvrir l'entièreté du parc.

Concernant les règles de firewall, le boîtier doit avoir un accès complet à l'ensemble du parc, seul le réseau AUTH ne sera pas accessible par le boîtier. Le boîtier fera partie du réseau "SURVEILLANCE".

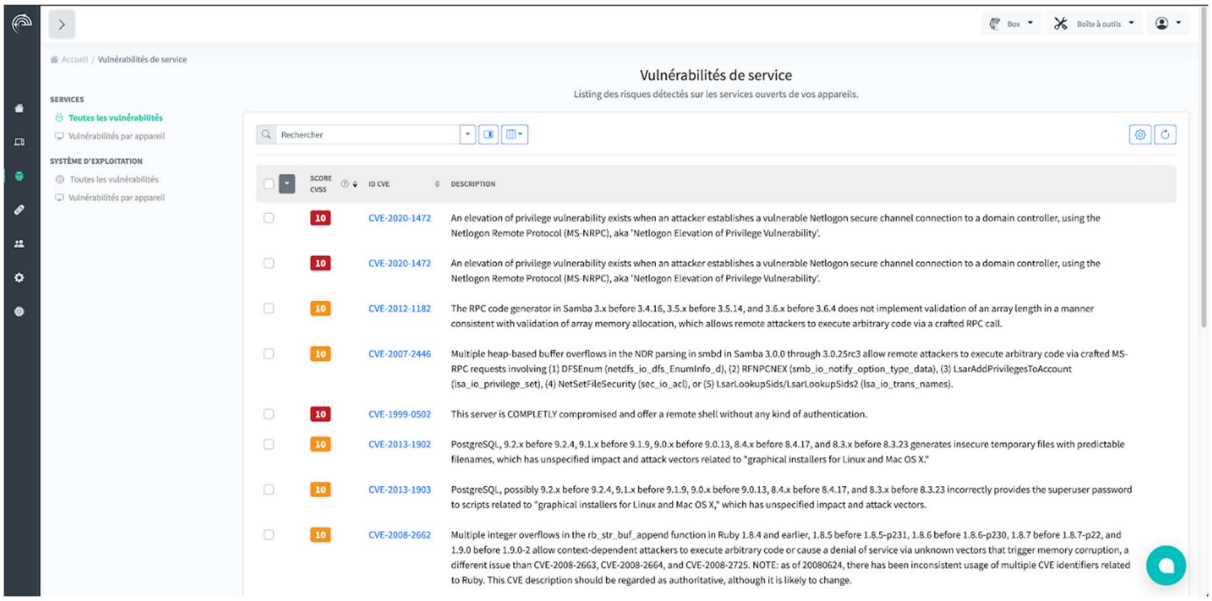
Quelques images de l'interface



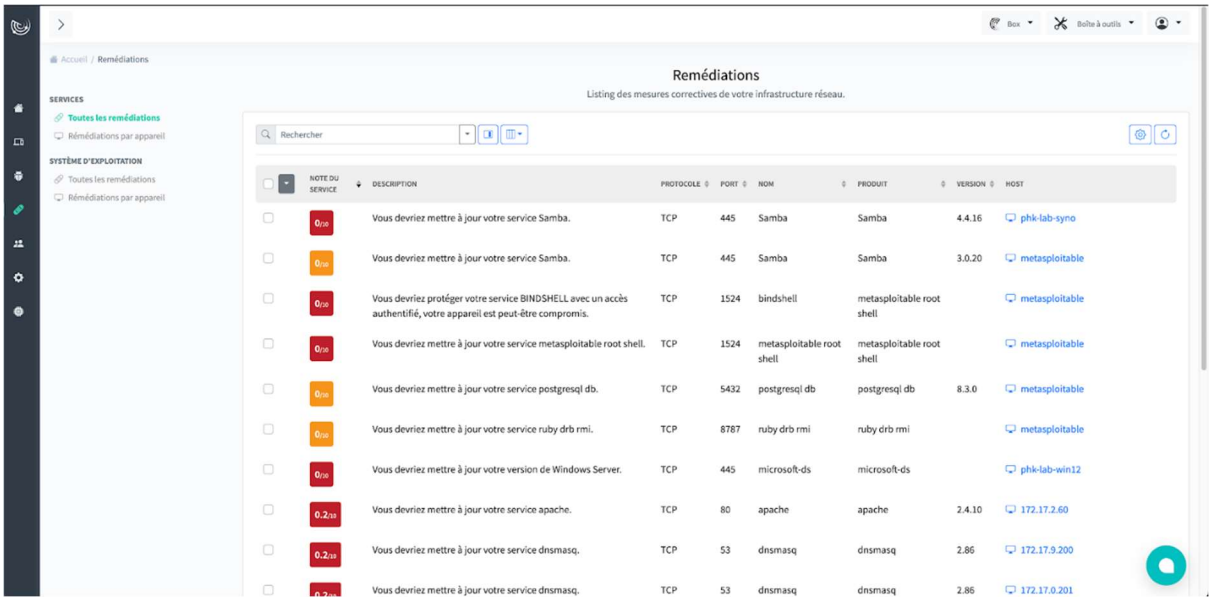
Interface Sherlock - Liste des appareils



Interface Sherlock - Tableau de bord, comprenant le cyber-score



Interface Sherlock - Liste des vulnérabilités par appareil



Interface Sherlock - Liste des remédiations par appareil

Annexe Datacenter VDI

Nous avons décidé de séparer les ressources de calcul VDI de celle des serveurs Proxmox afin d'éviter des effets de bords et de ne pas avoir des machines étudiants venant interférer avec les serveurs en production. Ainsi un cluster ESXI contrôlé par un vCenter sera installé dans le datacenter, il contiendra le serveur Horizon ainsi que les VMs étudiants.

Chaque VM disposera de 4 Go de RAM, 4 vCPU, 40Go de stockage (via montage NFS/SMB)

Ayant 355 élèves, 35 professeurs, soit un total de 390 personnes :

- 390*4 = 1560 Go de RAM
- 390*4 = 1560 vCPU

Un stockage de base de 20Go en ajoutant le montage NFS/SMB calculé avec les baies TrueNas

Étant donné que les utilisateurs ne peuvent exécuter qu'une seule VM à la fois, le calcul de ressources nécessaire est effectué pour qu'une seule VM.

Il y a donc un besoin conséquent concernant le datacenter ESXI.

Il se compose de 3 serveurs HPE ProLiant DL380 Gen11 6430 contenant :

- 2x Processeurs Intel® Xeon® Gold 6430 32 cœurs/64 threads
- 1024 Go de RAM
- Kit bloc d'alimentation enfichable à chaud HPE 1000 W Flex Slot Titanium[P03178-B21]

Ainsi, si un serveur ESXI tombe, les deux restants peuvent assurer le fonctionnement de l'infrastructure VDI dans le cas où toutes les VMs sont utilisées en même temps, avec leur capacité utilisée au maximum.

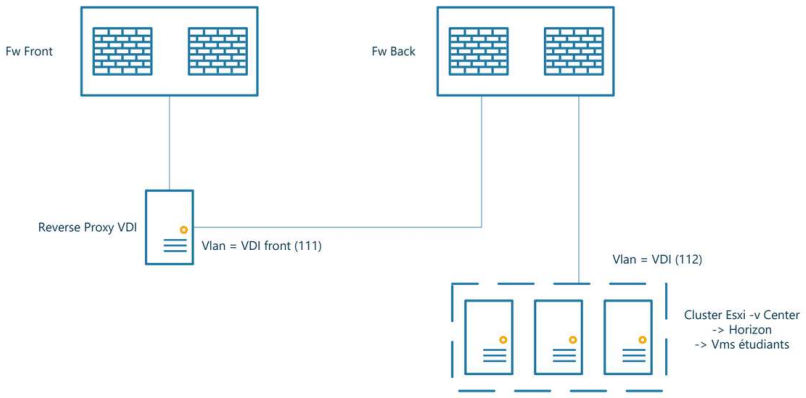
Pour avoir la capacité de vCPU disponible, il faut faire le calcul suivant : Nombre de cœurs x nombre de threads.

Le Intel® Xeon® Gold 6430 dispose de 32 cœurs et de 64 threads, soit 32*64 = 2048 vCPU disponible. Ce nombre est évidemment multiplié par le nombre de processeur soit 2048*2 = 4096 vCPU. Ainsi, un seul serveur ESXI est capable d'assurer la charge CPU nécessaire.

La capacité totale du cluster ESXI est la suivante :

- CPU : 32*6 = 192 cœurs, 64*6 = 384, et donc 192*384 = 73 728 vCPU
- RAM : 1024*3 = 3072 Go de RAM
- Stockage : Un montage NFS sera mis à disposition pour le cluster (390*20 = 7 800*2 = 15600 + le stockage nécessaire pour le serveur Horizon + vCenter, le chiffre sera arrondi à 16 T de stockage.)

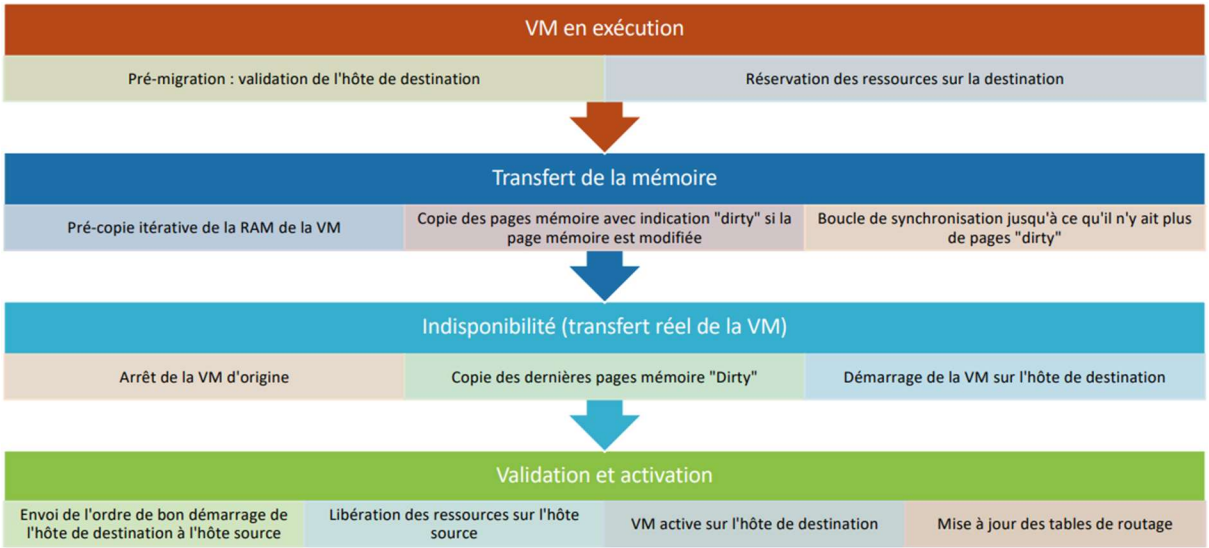
Schéma cluster ESXI VDI



Annexe Proxmox

Haute disponibilité Proxmox

La mise en place d'un cluster proxmox avec un stockage partagé de type ceph permet la mise en place de la haute disponibilité pour nos vm sur lesquels tournent nos services. Pour assurer une continuité de service la HA sera mise en place dans l'optique ou si un node tombe les VMs présente dessus seront automatiquement migré à chaud sur un autre node et cela via un transfert de la RAM comme présenté ci-dessous :



L'avantage de coupler ceph avec un lien direct 25Gb/s et une mémoire NVMe pour les services hébergé sur des QEMU qui ne nécessite pas de redémarrage contrairement au container, le temps d'indisponibilité réel de la machine malgré son transfert n'est pas perceptible.

Proxmox Backup Serveur

Au même titre que proxmox VE, proxmox backup est une solution open-source de backup pour les machines virtuels qemu comme lxc que l'on va envoyer sur ce serveur distant afin de pouvoir récupérer des machines en cas de perte ou de dommage des VMs sur le cluster principale. Son intégration avec proxmox, sa vitesse et sa sécurité avec un chiffrement des données via AES-256 et la vérification de l'intégrité de celle-ci pour éviter les erreurs en font pour notre système une vraie force dans le cadre d'un plan de reprise d'activité.

Ceph

Ceph est une solution de stockage distribué qui permet de stocker de grandes quantités de données de manière fiable et efficace. Les principaux avantages de Ceph sont son évolutivité, sa disponibilité élevée, sa tolérance aux pannes, sa flexibilité et son intégration facile avec d'autres outils et technologies. Ceph utilise une architecture de stockage en cluster qui permet de répartir les données sur plusieurs nœuds de stockage, ce qui permet de réduire les coûts et d'améliorer les performances globales.

Ceph en revanche est assez complexe à mettre en place sur des serveurs classique la ou, proxmox nous offre une mise en place simplifié avec son interface web qui propose la mise en place de ce type de stockage en 4 clics avec en plus la possibilité de rajouter plusieurs module comme RESTful pour le monitoring

Annexe Intégration Zabbix

Liste des autres intégrations possible avec zabbix :

Nom de la techno	Template	Type	Métrics importantes
Caméra dahua	dahua video camera	SNMP	- Etat de la caméra - uptime - version
Bases de données	postgresql	Zabbix agent 2	- stockage - nombre de connexion - débit d'ecriture
switch cisco	cisco by snmp	SNMP	- CPU - Débit - Temperature
router cisco	cisco by snmp	SNMP	- CPU - Débit - Temperature
git	Gitlab by http	http	- nombre de requête - processes - nombre de pipeline
squid	Squid proxy by SNMP	SNMP	- CPU usage - Ram usage - Nombre de requête http

Conf Zabbix

/etc/zabbix/zabbix_agentd.conf :

```
PidFile=/run/zabbix/zabbix_agentd.pid
LogFile=/var/log/zabbix/zabbix_agentd.log
LogFileSize=0
StartAgents=0
Hostname=<FQDN>
ServerActive=<AdresseSERVEUR:Port>
RefreshActiveChecks=120
BufferSend=5
BufferSize=100
TLSConnect=cert
TLSCAFile=<Chemin_CA>
TLSCertFile=<CheminCRT>
TLSKeyFile=<CheminKEY>
Include=/etc/zabbix/zabbix_agentd.d/*.conf
```

/etc/zabbix/zabbix_agentd.d/userparameter_upki-cli.conf :

```
UserParameter=upki-cli_lld-crt-files,/usr/bin/python3
/etc/zabbix/zabbix_agentd.d/upki-cli_lld-crt-files.py

UserParameter=upki-cli_lld-crl-files,/usr/bin/python3
/etc/zabbix/zabbix_agentd.d/upki-cli_lld-crl-files.py

UserParameter=upki-cli_expiry-crt-files[*],/usr/bin/python3
/etc/zabbix/zabbix_agentd.d/upki-cli_expiry-crt-files.py $1

UserParameter=upki-cli_expiry-crl-files[*],/usr/bin/python3
/etc/zabbix/zabbix_agentd.d/upki-cli_expiry-crl-files.py $1
```

/etc/zabbix/zabbix_agentd.d/upki-cli_expiry-crl-files.py :

```
#!/usr/bin/python3
import sys
import os
import OpenSSL
import datetime
crt_base = "/home/UTILISATEUR/.upki/"

def parse_crl(file):
    crl_text =
str(OpenSSL.crypto.dump_crl(OpenSSL.crypto.FILETYPE_TEXT,
OpenSSL.crypto.load_crl(OpenSSL.crypto.FILETYPE_PEM,
open(file).read())))
    for line in crl_text.split("\\n"):
        if "Next Update: " in line:
            key, value = line.split(":", 1)
            date = value.strip()
            dt = datetime.datetime.strptime(date, "%b %d %X
%Y %Z")
            break
    return str(dt)

if __name__ == '__main__':
    if len(sys.argv) < 2:
        sys.exit(-1)
    file = sys.argv[1]
    if len(file) == 0:
        sys.exit(-1)

    cert = os.path.join(crt_base, file)
    if not os.path.isfile(cert):
        sys.exit(-1)
```

```
    expire_timestamp = parse_crl(cert)
    year = int(expire_timestamp[:4])
    month = int(expire_timestamp[5:7])
    day = int(expire_timestamp[8:10])
    hour = int(expire_timestamp[11:13])
    minute = int(expire_timestamp[14:16])
    second = int(expire_timestamp[17:19])
    expire = datetime.datetime(year, month, day, hour,
minute, second)
    hours_to_expire = expire - datetime.datetime.now()

    if hours_to_expire.seconds >= 0:

print(hours_to_expire.days*24+hours_to_expire.seconds//3600)
    else:
        print(0)
```

/etc/zabbix/zabbix_agentd.d/upki-cli_expiry-crt-files.py :

```
#!/usr/bin/python3

import sys

import os

import OpenSSL

import datetime

crt_base = "/home/UTILISATEUR/.upki/"


if __name__ == '__main__':

    if len(sys.argv) < 2:

        sys.exit(-1)
```

```
    file = sys.argv[1]

    if len(file) == 0:

        sys.exit(-1)



    cert = os.path.join(crt_base, file)

    if not os.path.isfile(cert):

        sys.exit(-1)



    x509 =
OpenSSL.crypto.load_certificate(OpenSSL.crypto.FILETYPE_PEM,
open(cert).read())

    expire_timestamp = x509.get_notAfter().decode()

    year = int(expire_timestamp[:4])

    month = int(expire_timestamp[4:6])

    day = int(expire_timestamp[6:8])

    expire = datetime.datetime(year, month, day)

    days_to_expire = expire - datetime.datetime.now()



    if days_to_expire.days >= 0:

        print(days_to_expire.days)

    else:

        print(0)
```

/etc/zabbix/zabbix_agentd.d/upki-cli_lld-crl-files.py :

```
#!/usr/bin/python3

import sys

import os

import json
```

```
crl = "/home/UTILISATEUR/.upki/crl.pem"



def make_lld_json(file):

    dict_to_json = {'data': []}

    dict_to_json['data'].append({"{#CRLFILE}":
str(os.path.basename(file))})

    return json.dumps(dict_to_json)



if __name__ == '__main__':

    if not os.path.isfile(crl):

        print("{'data': []}")

    else:

        print(make_lld_json(crl))
```

/etc/zabbix/zabbix_agentd.d/upki-cli_lld-crt-files.py :

```
#!/usr/bin/python3
import os
import glob
import json
crt_base = "/home/UTILISATEUR/.upki/*.crt"

def crt_files_discovery(folder: str):
     files=glob.glob(folder)
     return files

def make_lld_json(files):
    dict_to_json = {'data': []}
    for file in files:
        dict_to_json['data'].append({"{#CRTFILE}":
str(os.path.basename(file))})
    return json.dumps(dict_to_json)

if __name__ == '__main__':
    print(make_lld_json(crt_files_discovery(crt_base)))
```

Annexe Portail d'applications

Un portail d'applications authentifiant sera mis à disposition des élèves et des professeurs afin d'accéder aux outils collaboratifs tels que Nextcloud, Gitlab, ou le webmail.

La solution choisie est LemonLDAP::NG pour sa diversité de configuration permettant de répondre à nos attentes, c'est aussi une solution Open Source.

Ce portail ne sera accessible que depuis l'intérieur du bâtiment/réseau pour des questions de sécurité. Les applications sont réservées à un usage interne.

Fonctionnement avec PKI

En vue de notre architecture PKI, l'implémentation du portail d'applications doit être cohérente avec notre stratégie de sécurité.

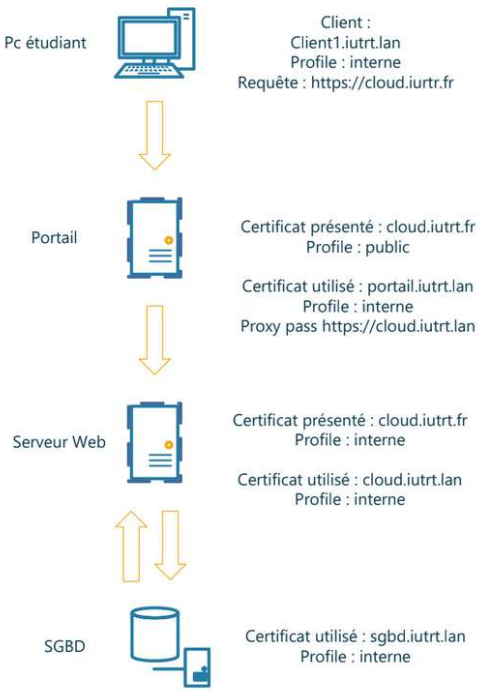
Le portail présentera des certificats avec un profil et une extension "public" (mais non exposés sur internet) aux utilisateurs.

Le serveur web quant à lui présentera lui aussi un certificat avec une extension "publique" mais un profil "interne".

Enfin, le serveur web communiquera avec les bases de données et autres serveurs avec un certificat de profil "interne" et avec extension interne.

Le fait d'utiliser deux fois l'extension "publique" permet d'éviter des erreurs de certificats dans de nombreux cas. Pour rappel, la sécurité est assurée quand le certificat dispose du même nom (CN) que le serveur/nom DNS.

Schématisation de la tentative d'accès au Nextcloud



Annexe services Nextcloud

Voici quelques-unes des fonctionnalités principales de Nextcloud :

Stockage de fichiers : Nextcloud permet aux utilisateurs de stocker des fichiers en ligne. Les utilisateurs peuvent télécharger des fichiers, créer des dossiers, partager des fichiers avec d'autres utilisateurs et gérer les autorisations d'accès.

Partage de fichiers : Nextcloud permet aux utilisateurs de partager des fichiers avec d'autres utilisateurs en utilisant des liens publics ou des liens privés avec des autorisations d'accès spécifiques. Les utilisateurs peuvent également collaborer sur des fichiers en temps réel.

Synchronisation de fichiers : Nextcloud permet aux utilisateurs de synchroniser des fichiers entre leur ordinateur de bureau, leur téléphone mobile et leur compte en ligne.

Calendrier et contacts : Nextcloud comprend également des fonctionnalités de calendrier et de contacts qui permettent aux utilisateurs de planifier des événements, de gérer des contacts et de synchroniser ces informations avec leurs appareils.

Notes et tâches : Nextcloud comprend également des fonctionnalités de prise de notes et de gestion de tâches qui permettent aux utilisateurs de créer et de gérer des listes de tâches, des notes et des rappels.

Gestion des utilisateurs : Nextcloud permet aux administrateurs de gérer les utilisateurs, les groupes et les autorisations d'accès.

Sécurité : Nextcloud est conçu pour être sécurisé et dispose de fonctionnalités telles que l'authentification à deux facteurs, la gestion des clés de chiffrement et la sécurité des données.

Annexe Imprimantes

HL-L2370DN

La Brother HL-L2370DW est une imprimante laser monochrome compacte et abordable, elle sera idéale en tant qu'imprimante dans les bureaux des professeurs. Elle offre des vitesses d'impression rapides et une connectivité réseau Ethernet. Elle dispose également de la fonction d'impression recto-verso automatique pour réduire la consommation de papier. Elle est capable d'imprimer jusqu'à 34 pages par minute de manière totalement silencieuse, parfaite dans le cadre de travail des professeurs.

Prix : 191,52 € TTC

MFC-L3750CDW

La Brother MFC-L3750CDW est une imprimante laser couleur multifonction qui convient parfaitement aux besoins d'un secrétariat. Elle offre des fonctions d'impression, de numérisation, de copie et de télécopie. Cette imprimante dispose d'une connectivité réseau Ethernet et Wi-Fi, ainsi que d'un chargeur automatique de documents (ADF) pour faciliter la numérisation et la copie de plusieurs pages.

Prix : 516,24 € TTC

MFC-L8900CDW

La Brother MFC-L8900CDW est une imprimante laser couleur multifonction haut de gamme qui offre des fonctions d'impression, de numérisation, de copie et de télécopie. Elle est idéale pour la salle des professeurs nécessitant un appareil polyvalent et performant. Elle dispose d'une connectivité réseau Ethernet et Wi-Fi, d'un chargeur automatique de documents (ADF) et d'un grand écran tactile pour faciliter l'utilisation. Elle prend également en charge l'impression recto-verso automatique et possède une capacité de papier élevée pour gérer de grands volumes d'impression.

Prix : 1 066,80 € TTC

Sécurité Physique

La sécurité du bâtiment sera assurée par des systèmes de la société ARD

ARD est une entreprise française spécialisée dans la conception, la fabrication et la distribution de systèmes de contrôle d'accès électroniques pour les bâtiments.

La société est engagée dans la sécurité de ses produits et a obtenu plusieurs certifications de sécurité pour ses dispositifs de contrôle d'accès. ARD est certifié ISO 9001, qui garantit que les systèmes de gestion de la qualité de l'entreprise répondent aux normes internationales. De plus, la société a obtenu la certification EN 1300 pour ses serrures de haute sécurité, la certification A2P pour ses cylindres et serrures, et la certification NF pour ses serrures électroniques.

Tous les contrôles de sécurité des serrures se feront via un contrôleur OTES II lié à un Superviseur ARD Access.

Le contrôleur OTES II est une unité de traitement pour le contrôle des accès et l'anti-intrusion. Avec la suite logicielle ARD ACCESS et les lecteurs sans contact ARD C2 (ISO 14443–A et B et NFC), il constitue l'ossature des solutions de sécurité ARD.

Un contrôleur sera mis en place dans le bureau du SI. Deux dans la baie de brassage du rez-de-chaussé. Un dans la baie de brassage du premier étage. Ces chiffres sont choisis car un contrôleur OTES II peut paramétrer 16 portes au maximum. Le rez-de -chaussée comptant 28 portes, il faudra donc 2 contrôleurs.

Les contrôleurs seront branchés à des Hubs.

Les cylindres sans fil communiquent par radiofréquences avec ces hubs, eux-mêmes raccordés à une unité de contrôle OTES II. La communication avec le hub se fait via des câbles RS-485 et est chiffrée AES 128 bits. Le hub vérifie régulièrement la présence de la béquille : en cas de problème, il envoie un message d'alerte au système central de contrôle d'accès. Un même hub peut adresser jusqu'à 8 portes en champ libre. Il faudra donc 2 hubs au premier étage, 4 au rez-de chaussé et un au sous sol.

Nous utiliserons les Cylindre radio APERIO sur les portes du bâtiment.

Pour déverrouiller la porte, il convient de passer simplement un badge autorisé devant le cylindre. Pour la verrouiller, il suffit de passer le badge à nouveau devant le cylindre. Le cylindre sans fil est donc une véritable « clé électronique » qui vient se mettre à la place du cylindre mécanique traditionnel à clé.
Les paramétrages de ces serrures se font via le contrôleur OTES II.

Pour les badges nous utiliserons les Badge DESFIRE EV1.

La puce est de technologie ISO/IEC 14443-1 de type Mifare DesFire EV2 avec chiffrement AES, un produit certifié critère commun EAL4+ conforme aux recommandations de l'ANSSI. La puce est également flexible en termes de compatibilité, car elle prend en charge les dernières normes de sécurité, telles que TLS, AES-128 et SHA-256. Nous utiliserons le ARC-G - 13.56 MHz DESFire® EV2 & EV3 pour encoder nos cartes DesFire. Nous aurons différents types de profils

Tous les élèves auront une carte étudiante. Chaque délégué de chaque classe se verra attribuer une salle qu'ils pourront ouvrir pour laisser leur classe respective utiliser la salle. Les profs et l'administration auront des clefs spécifiques pouvant ouvrir leurs bureaux de travail ainsi que les salles de classes. Les SI auront des cartes permettant d'ouvrir la totalité des serrures du bâtiment.

Tous les paramétrages se feront via le Superviseur ARD Access, un logiciel d'ARD. Celui-ci permet au superviseur de créer des profils d'utilisateurs avec des droits d'accès spécifiques, et de les affecter à des groupes pour faciliter la gestion des autorisations d'accès.
Le module d'import AD permettra au Superviseur ARD Access d'importer directement nos paramétrage Active Directory pour gérer plus facilement et rapidement les droits d'accès des usagers du bâtiment.

Au niveau des intrusions un système de détecteur volumétrique ainsi que de contact de porte tous ca lié à une sirène nous permettra d'analyser toute tentative d'intrusion dans le bâtiment.

Une alarme sera activée entre 19h et 7h30 pour éviter les intrusions. Un contact de porte sera présent au 4 portes d'entrée (2 du rez-de chaussé et 2 du sous-sol). Des détecteurs volumétriques seront également placés dans chaque salle et couloir pour permettre une sécurité maximum. Pour cela nous utiliserons le Optex LX-802N. Les Contact de porte utilisés seront des Honeywell 947-75TWH. Choisi grâce à leur protection anti-sabotage ainsi que la facilité d'installation. Ceux-ci seront placés au 4 portes extérieures.