Référence du document : KMN 00001 – A

Référence client : AXMRSLU-UNIV1

CAHIER DE SPECIFICATIONS SYSTEME

Résumé :

Ce cahier de spécification décrit l'ensemble des système et sous-système que notre solution comprendra ainsi que leur interconnexion avec le réseau.

Elaboration :

IND.	DATE	Rédacteur		Vérificateur		Approbateur	
		NOM	VISA	NOM	VISA	NOM	VISA
A	14/02/18	P.MOYSE	x	L.GRIMAUDO	x	P.CARLES	x

Historique :

IND.	DATE	MODIFICATIONS (ORIGINE, OBJET ...)	REDACTEUR
A1	17/02/18	Première diffusion	P.MOYSE
A2	23/02/18	Ajout du cartouche KMN	P.MOYSE
A3	24/02/18	Cahier des charges	P.MOYSE
A4	25/02/18	Supervision + LDAP	P.MOYSE
A5	10/03/18	Refonte du document	P.MOYSE
A6	31/03/18	Ajout du service de backup + amélioration solution supervision	P.MOYSE
A7	16/04/18	Validation des schémas	P.MOYSE
A8	13/04/18	Amélioration backup + ajout solution alarme	P.MOYSE
A9	14/05/18	Finalisation et ajout des dernières parties	P.MOYSE

KAMENETWORK SOLUTION

SARL au capital de 666 M€

Siège social : 70, Avenue des champs Elysée 75017 PARIS RCS PARIS B 444 159 164

Agence de Marseille : 10 Avenue de la Corse 13007 Marseille

SOMMAIRE

1. IDENTIFICATION DES BESOINS

Ce cahier de spécification ne prendra en compte uniquement l'aspect système de l'architecture proposé.
Dans le cadre de ce projet, il nous a été donné le cahier des charges suivants.

1.1. CAHIER DES CHARGES

- L'architecture doit pouvoir supporter plus de 400 personnes en simultané
- La solution système doit comprendre une interconnexion avec trois sites distants
- Cette solution doit avoir des politiques de sécurité personnalisé en fonction des besoins.
- Ces serveurs seront virtualisés sur plusieurs machines virtuelles et effectuerons les services suivants :
    - Annuaire LDAP & DNS
    - Hébergement de fichier distant
    - Serveur d'authentification RADIUS
    - Serveur de log Syslog
    - Serveur Web Nginx
    - Serveur de supervision
    - Service de gestion des incidents & inventoring
    - Service de gestion des emplois du temps & absences
    - Service d'enregistrement vidéo
    - Service d'alarme connectée
    - Serveur de backup externe

Nous détaillerons ci-après les services les plus complexes à mettre en œuvres. Le reste des services sera inclut de base dans l'offre standard.

1.2. REFERENCES

Ce document applicable fait références à d'autres documents du groupe :

ID	Document	Référence	Indice
1	Logigramme de répartition des données	KMN-ANX-001	A
2	Solutions smartphones & badges Locken	KMN-ANX-002	BPE
3	Solution alarme et vidéosurveillance	KMN-ANX-003	BPE

Terminologie

BPE	Bon Pour Execution
A	Conception interne

2. SERVICES

2.1. LDAP & STOCKAGE

Le service LDAP permet une authentification sécurisée de vos utilisateurs. Nous proposons d'ajouter à cette solution une solution de stockage centralisée, cela permettra à vos utilisateurs de retrouver leurs fichiers quel que soit la sale d'études où ils se trouvent.

Dans le cadre d'une haute disponibilité et d'une adaptabilité à votre projet, nous proposons l'utilisation d'architecture virtualisée. Pour ce faire nous utiliserons VmWare ESXi en version 6.5, la plus récente à ce jour. Nous reviendrons sur les avantages de cette solution. La solution DNS sera gérée par l'outils bind9 couplé à l'annuaire LDAP.

2.1.1. PREREQUIS

L'utilisation du service LDAP et du stockage distant requiert certains prérequis :

- Bande passante élevée : Accès aux fichiers distants
- Utilisation avancée de la mémoire : Les fichiers les plus souvent utilisés devront être accessible rapidement
- Disposition intelligente des serveurs : En effet nous utiliserons une solution redondée ce qui permettra une utilisation homogène de votre réseau ainsi que de votre infrastructure système.

Ce système permettra de gérer les données en fonction du poste occupé et de son itinérance. Par exemple un étudiant étant affecté sur le site n°1 n'aura pas besoin d'avoir accès à ses données sur le site n°2 ; en revanche, un professeur intervenant sur les deux sites devra retrouver ses données d'un site à l'autre. Il a donc besoin d'un profil itinérant.

2.1.2. MATERIEL

Pour réaliser ce projet, nous proposons une solution comportant 3 serveurs **HP Proliant ML350e Gen8 V2.** Ces serveurs comportent plusieurs avantages :

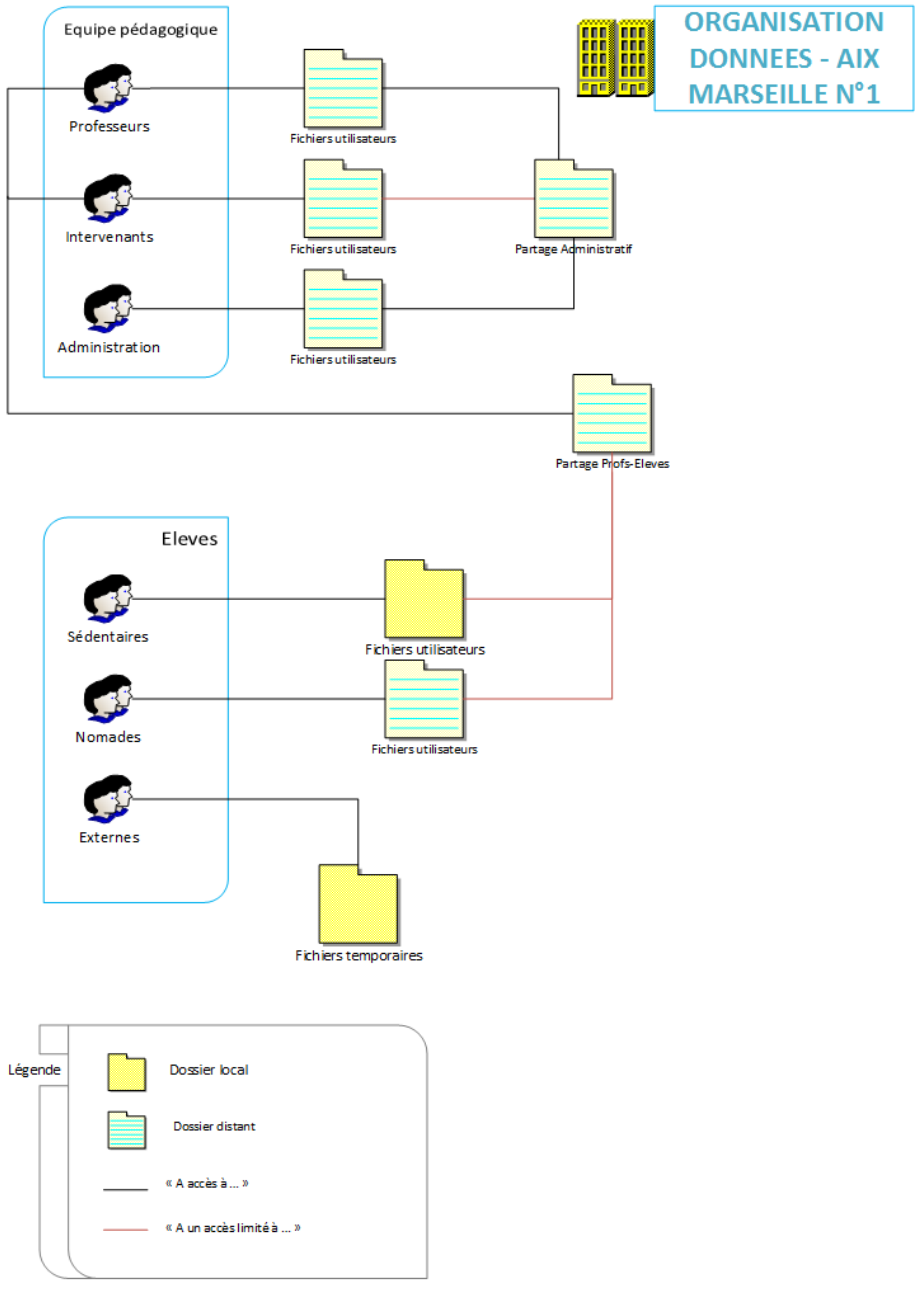
- Jusqu'à 24 disques durs
- Processeur Intel Xeon E5 -2420 2.2GHz 6 cœurs
- Mémoire RAM 1*4Go (Extensible jusqu'à 192Go)
- Double alimentation (460W)
- 2 Ports Gigabits (Extensible à 6)
- Port de management et de monitoring ILO4
- Faible dégagement thermique
- Ventilation modulable

Prix HT : 910€/Unité

Figure 1 : HP Proliant ML350e Gen8 V2

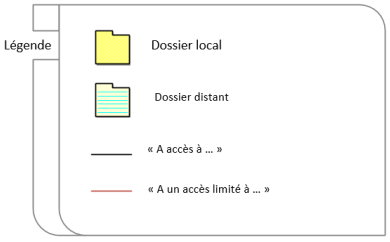
2.1.3. ORGANISATION

L'architecture d'annuaire sera composée comme ci-dessous avec les différents profils :



REF : KMN-ANX-001-A

Figure 2 : Annuaire LDAP



Vous pouvez retrouver ce logigramme en annexe Ref [1]

2.1.4. DISPOSITION

Ce service doit être disposé intelligemment : l'utilisation de bande passante étant élevée, il convient d'étudier les besoins étages par étages :

- Sous-sol : Demande élevée : Réplication VPN site à site pour mise à jour distante.
- RDC : Demande moyenne
- 1er étage : Demande élevée : Salle de TP + Salle informatique de TD
- 2ème étage : Demande moyenne : Salle de présentation + Salle de TP

Les serveurs LDAP devront être positionner à chaque étage car leur utilisation de bande passante sera accrue et dans le souci de qualité de services, un débit optimal se doit d'être maintenu. Aussi chaque serveur possèdera 3 sorties Gigabits pour convenablement répondre à la demande. A noter que ces serveurs possèderont une réplication des données pour éviter la surcharge d'un de ces serveurs.

Un serveur LDAP sera positionner dans un local sécurisé au sous-sol, à proximité direct avec l'interconnexion internet et possèdera toute la base LDAP pour réplication via VPN sur les sites distants afin de permettre une mobilité accrue.

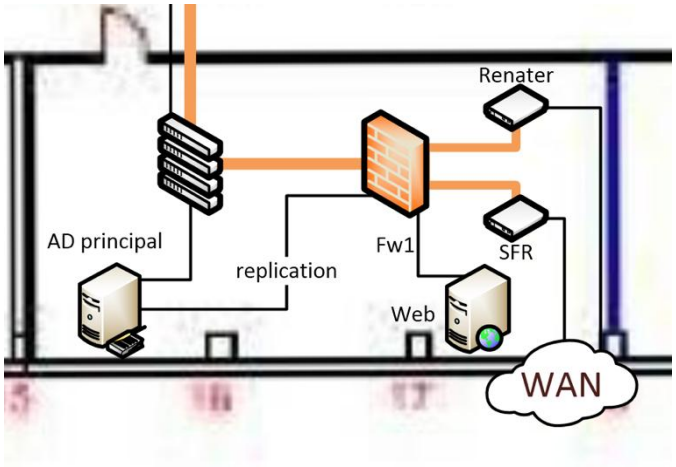


Figure 3 : Salle sous-sol

2.2. SUPERVISION

En complément d'une remontée de log de la part de toutes les machines, nous nous devons, dans le cadre de la surveillance centralisée, d'installer un serveur de supervision pour pouvoir monitorer l'ensemble du parc informatique que contiendra votre université. Cet outil de supervision se doit également d'être adaptable : en effet, pour l'instant le nombre de postes + serveurs est limité à environ 420-450 unités, mais notre solution sera également adaptable à des parcs informatiques de plus de 15 000 unités.

Pour réaliser cette tâche, nous proposons d'utiliser l'outil Zabbix en version 3.4, la plus avancé à ce jour. Cette supervision est parfaitement adaptable à l'ensemble de vos parcs informatiques et nécessiterai l'installation de client léger sur chacun de vos postes. Cette solution permettra une remontée des données efficace et personnalisable. Ce service sera virtualisé au sein de ce serveur via l'hyperviseur VMWare ESXi 6.5, leader du marché à ce jour. Nous prévoyons d'accueillir un autre service virtualisé sur ce serveur. C'est pourquoi il a été volontairement surdimensionné.

2.2.1. PREREQUIS

Le service de monitoring se doit d'être réactif pour nous avertir de tout problème afin de nous permettre d'intervenir rapidement. C'est pourquoi le serveur a été surdimensionnée : en effet ce service peut être gourmand en ressource c'est pourquoi nous avons prévus une haute adaptabilité sur ce serveur. L'alliance ESXI 6.5 + Service Zabbix est totalement justifiée : vous pourrez augmenter rapidement et efficacement la performance de ce serveur en vue d'une augmentation de votre parc informatique en adaptant la machine virtuelle en fonction du besoin.

2.2.2. MATERIEL

Nous proposons donc de virtualiser ce service Zabbix au sein d'un serveur **HP ProLiant DL360p Gen8 :**

- Jusqu'à 8 Disques durs
- Processeur Intel Xeon 2.5GHz 5 cœurs
- Mémoire RAM 1*8Go (Extensible jusqu'à 32Go)
- Double alimentation (350W)
- 2 Ports Gigabits
- Port de management et de monitoring ILO4
- Faible dégagement thermique
- Ventilation modulable

Prix HT : 1750€/Unité

Figure 4 : HP Proliant DL360p G8

2.2.3. DISPOSITION

Un service de supervision doit être disposé dans un local sûr, à la périphérie du réseau pour un accès distant aisée. Dans le cadre de ce contrat, nous assurons la supervision distante et la prévention de panne via nos services.

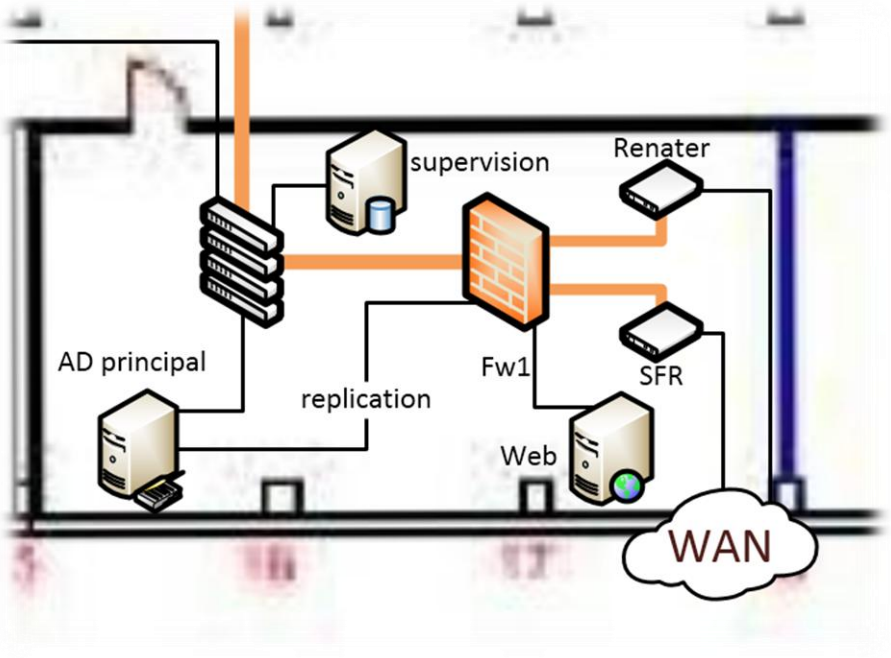


Figure 5 : Supervision Sous-sol

La remonté d'informations des clients Zabbix sera locale et sécurisé via une encryptions TLS. Cela permet de prévenir toute tentative d'apprentissage du réseau via une écoute de celui-ci.

2.2.4. LOGICIEL

Comme annoncé précédemment, nous utiliserons pour cette solution de supervision l'outil Zabbix 3.4. Cet outil à pour particularité sont architecture client-serveur. En effet, contrairement à ses conçurent, Zabbix embarque un client léger à installer sur les machines à monitorer, cela permet une remontée fluide et personnalisé du flux de surveillance. Nous possédons, au sein de notre infrastructure un Zabbix et nous vous proposons une architecture logicielle hiérarchique : Un serveur par site, hébergé dans vos locaux, se chargera de condenser les données ainsi que de vous permettre un accès pour une surveillance.

Dans un même temps, ce serveur envoie les données de supervision à notre centrale de supervision, ce qui nous permettra de surveiller à distance votre infrastructure et de vous avertir en cas de panne ainsi que de rapidement prévoir une intervention. Pour ceci, nous vous proposons l'architecture d'interconnexion système ci-après :

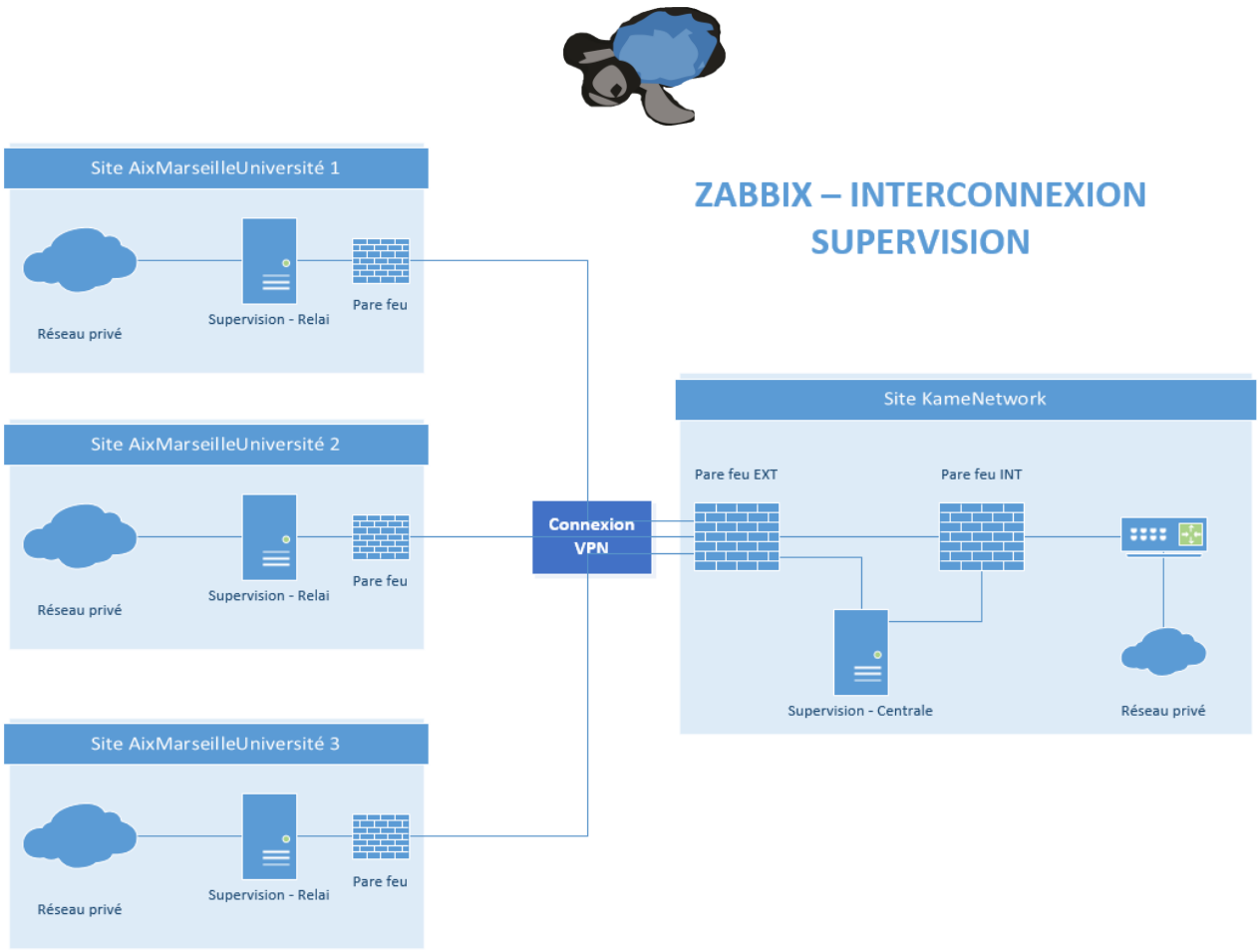


Figure 6 : interconnexion supervision Zabbix

2.3. GESTIONS DES INCIDENTS & INVENTORING

Pour assurer une haute disponibilité de votre infrastructure, il convient d'implanter un service d'inventoring. C'est-à-dire un service permettant de recenser tous vos postes informatiques, aussi bien serveurs que postes client, et de permettre à vos utilisateurs de faire rapidement et efficacement une remonté d'incident.

Cela permettra par la suite une gestion du stock facilité et un assurera un changement rapide du matériel par notre part en cas de défaut de celui-ci.

2.3.1. PREREQUIS

En ce qui concerne ce service. Il n'y a pas de prérequis particuliers. Nous proposons d'héberger ce service au sein de notre infrastructure situé dans des locaux sécurisés à notre agence. Celle solution est redondé à un Cloud chez notre fournisseur Amazon Web Servicies. Cela garantira une haute disponibilité de ce service, même en cas de panne généralisée sur nos infrastructures.

2.3.2. MATERIEL

Aucun matériel ne sera installé dans vos locaux, ce service sera virtualisé au sein de nos plateformes informatiques dans nos locaux.
Pour information, ce service sera virtualisé via une architecture VMWare ESXi 6.5 sur un serveur **HPE ProLiant DL560 Gen10**

Figure 7 : HPE ProLiant DL560 Gen10

2.3.3. LOGICIEL

Afin de mener à bien cette tâche d'inventorring et de gestion des incidents, nous proposons d'utiliser la solution libre GLPI. Cette solution est aussi connue que complexe à configurer, nous proposons d'implanter une configuration adaptée à votre infrastructure pour vous permettre le cas échéant de gérer vous-même votre stock ainsi que votre gestion d'incident. Nous pouvons également prendre en charge cette action (Réf. Options [1])

Figure 8 : Logo GLPI

2.4. SERVICE DE BACKUP

Une erreur n'arrivant jamais seule, une perte des données est toujours le pire cauchemar des informaticiens. Heureusement, notre solution proposée comporte un système de backup intelligent. Disponible en plusieurs option, cette solution permettra une sauvegarde efficace de vos données et une restauration rapide, même en cas de perte totale.
Nous avons choisi de détailler quelques option listées ci-dessous

- Plan BRONZE : Backup en local seulement :
  - Incrémentale tous les jours / totale toutes les semaines
  - Archivage intelligent à moyen terme.
- Plan SILVER : Backup local + Backup sur site distant
  - Incrémentale tous les jours / totales toutes les semaines
  - Archivage intelligent à long terme
- PLAN GOLD : Backup local + Backup sur nos infrastructures
  - Incrémentale tous les jours / totale toutes les semaines
  - Archivage intelligent à moyen terme.
- PLAN DIAMOND : Backup local + Backup sur site distant + Backup dans le cloud
  - Incrémentale toutes les heures / totale tous les trois jours
  - Archivage intelligent à très long terme
  - Déploiement de sauvegarde rapide
  - Reconstruction facilitée

2.4.1. PREREQUIS

Ce service étant assez lourd à gérer, il requiert un certain nombre de prérequis parmi les plus notable nous retrouverons :

- Besoin de bande passante accrue : localisé et ponctuel
- Vitesse de lecture/écriture élevée
- Besoin de disponibilité à certaines heures et pendant un créneau défini
- Contrôle automatisé de la sauvegarde

2.4.2. MATERIEL

Pour réaliser cette tache de sauvegarde nous opterons pour une solution SAN via le **HPE D3700** qui, à ce jour, répond parfaitement à votre besoin

Figure 10 : HPE DS3700 - Back

Ce serveur possède la connectique XXX propriétaire HP permettant le transfert de fichier à très haut débit (jusqu'à 40Gps). Cette solution permettra une restauration de backup « à chaud » à la fois rapide et sécurisée.

Figure 9 : HPE DS3700 - Front

2.4.3. LOGICIEL

Pour permettre une gestion intelligente de vos sauvegardes, nous proposons d'utiliser notre logiciel de gestion des backups : **TIBS** « *Trully Innovative Backup System* ». Ce logiciel a été développé par nos soins et s'interfaces parfaitement avec des infrastructure complexes. Nous utilisons actuellement cet outil dans nos structures avec un taux de perte de 0.1% des données en production. Ce logiciel sera proposé en option.

Figure 11 : Logo TIBS

2.5. SERVICE DE GESTION DES ACCES ET ALARMES

Dans le but de garantir une sécurité optimale aux utilisateurs ainsi qu'aux données, il apparait le besoin d'un système de surveillance centralisé. Ce système doit pouvoir permettre de contrôler l'accès à certaines salles notées comme étant sensibles ainsi que de surveiller les utilisateurs afin de remarquer tout comportement suspect ou incorrect au sein de l'établissement. Nous commencerons par détailler la solution de contrôle d'accès, puis nous vous proposerons une solution de vidéosurveillance intelligente.

Votre bâtiment accueillant plus de 400 personnes en simultané le besoin d'un service de sécurité informatisée est omniprésent. Ce document décrit les aspects à prendre en compte dans l'élaboration de notre solution ainsi que les aboutissements de celle-ci.

Le cahier des charges se représente, dans ce cas, comme ceci :

Fait	Besoin	Solution
+ de 400 personnes présentes en simultané dans le bâtiment	- Surveillance vidéo - Accès restreint - Détection d'évènement - Connaitre le nombre précis de personnes présentes	- Monitoring vidéo - Enregistrement automatisé - Détection des visages - Référencement des étudiant - Badge d'accès NFC
Serveurs sensibles présent dans le bâtiment	- Sécurité du local - Accès règlementé - Salle anti-incendie - Sécurité des serveurs - Indépendance électrique	- Porte blindé - Accès badgé - Système anti incendie au CO2 - Baie protégée - Serveurs ondulées - Onduleurs dans une autre salle
Moyenne structure	- Faible cout de la sécurité - Efficacité au long terme	- Surveillance automatisé avec accès à distance pour nos services - Accès sécurisé pour un membre de votre équipe.
Données sensible	- Sauvegarde locale et distante - Sécurité des NAS	- Deux solution : une en local, l'autre sur un site distant ou un en local et l'autre dans le cloud. - Protection IPS
Locaux distant des forces d'intervention	- Possibilité d'alerter rapidement	- Système d'avertissement direct avec les forces de l'ordre.

Notre solution de contrôle d'accès s'appuie sur une solution propriétaire Locken®, leader du marché à ce jour : SOLUTIONS SMARTPHONES & BADGES. Cette solution est détaillée dans le document annexe Ref [2].

Figure 12 : Locken SAS

2.5.1. PREREQUIS

Comme dit précédemment, ce système doit se porter garant de la sécurité du bâtiment ainsi que de ses utilisateurs (données comprises). Nous proposons de coupler la solution Locken à une solution de vidéo surveillance et d'alarme connectée, capable de prévenir les secours rapidement.

2.5.2. MATERIEL

Locken apportera au projet sa solution propriétaire ainsi que ses machines de production (Barillet & serveurs). Les caméras seront fournies par la société AVIDEON, leader du marché à ce jour.

2.5.3. LOGICIEL

Le logiciel utilisé dans le traitement d'image et de stockage sera également fournis par AVIDEON, la société accepte d'installer son logiciel ainsi que ses machines au sein de l'architecture proposée.

L'ensembles des solutions AVIDEON sont décrites dans l'annexe Ref [3] Solution alarme et vidéosurveillance

3. PARC INFORMATIQUE UTILISATEUR

3.1. POSTES BUREAUTIQUES

Notre solution embarque un pack de postes utilisateurs dit « Bureautique ». Ces postes doivent permettre un apprentissage convenable de la programmation ainsi que de la suite Office.

Les postes seront les suivants :

- HP Z440 8Gb
  - 8Gb de RAM
  - Processeur intel XEON 2.5GHz
  - 1 * 1Gps Ethernet
  - 1*500Go de stockage

3.2. POSTES SPECIALISEE – CISCO CHALLENGE LAB

Nous proposons une salle dédiée à l'apprentissage Cisco via les Challenge lab en partenariat avec Cisco. Ces salles seront isolées du réseau extérieur pour ne pas perturber le travail des étudiant. Un accès internet sera réservé au professeur pour permettre une administration étudiante aisée.

Ces salles disposeront également de postes informatiques de dernière génération aux spécifications techniques plus élevées, adaptées à l'apprentissage des nouvelles technologies.

Les postes seront les suivants :

- HP Z440 16Gb
  - 16Gb de RAM
  - Processeur intel XEON 3.4GHz
  - 2 * 1Gps Ethernet
  - 2*500Go de stockage

La salle *Cisco challenge lab* sera élaborée comme présenter ci-après :

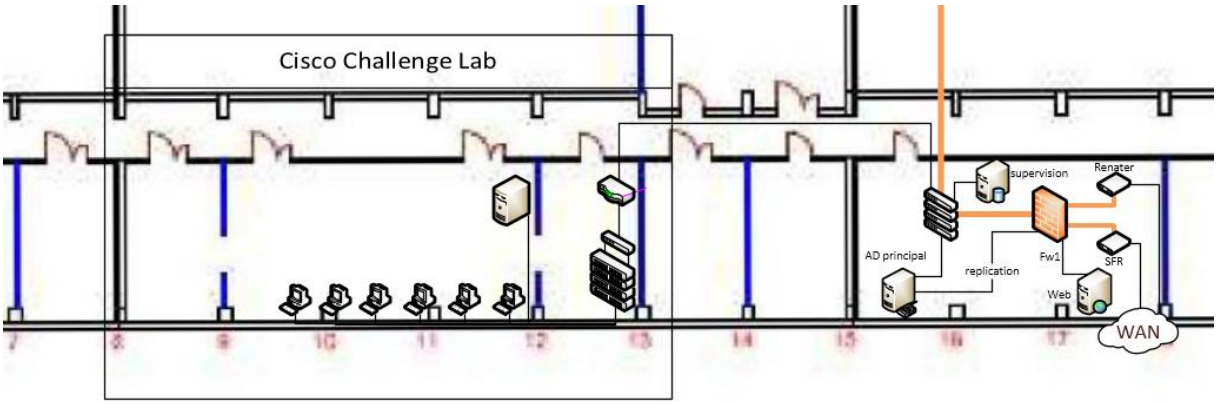


Figure 13 : Cisco Challenge Lab

4. REPONSE AUX BESOINS

Le présent document a décrit l'ensemble des solutions pour permettre de répondre aux besoins de notre demandeur Aix-Marseille Université.

Pour rappel, le projet doit répondre aux besoins d'étudiants, du personnel administratif, des professeurs et des personnes invitées peuvent être amenées à utiliser le système d'information. Par cela, il faut comprendre qu'un utilisateur doit pouvoir :

- Utiliser pleinement et à tout moment son espace personnel que ce soit par wifi ou par câble ethernet, quel que soit le site dans lequel il se trouve
- Utiliser la téléphonie s'il est habilité à l'utiliser
- Disposer de salles dédiées à l'apprentissage de l'informatique par les outils numériques
- Disposer d'un accès vers internet mondial
- Disposer d'un accès sécurisé