Dossier d'implantation technique

Offre de services Siham-PMS

AVERTISSEMENT

Ce document a été rédigé à partir du modèle **SIHAM_MOD_SOL_ModeOperatoire.V1.00.docx**

Table d'approbation du document

Approbateur	Service	Date d'approbation
DUPORT NAEM Thierry	Siham - DCSI	24/07/2018

Table des révisions du document

Version	Auteur	Date	Objet de la mise à jour
2.02	Eric Sainct	24/07/2018	Modification suite à l'homologation de sécurité
2.01	Bruno Chabal	29/06/2015	Modifications sur les prérequis établissement
2.00	Bruno Chabal	07/04/2015	Modification suite à l'homologation de sécurité
1.00	Joseph Bezzina Bruno Chabal	23/10/2014	Initialisation du document

Modifications depuis la dernière version

Paragraphe	Page	Nature de la Modification
7	12	Modification du lien
3.2	8	Mise en forme
N/A	N/A	Mise en conformité PGD et charte

A chaque nouvelle version du document, la table des révisions et des modifications doit être mise à jour.

Table des matières

1. PREAMBULE 5

2. CONTEXTE D'IMPLANTATION 6

3. CONTENU TECHNIQUE 7

3.1. PRESTATIONS TECHNIQUES 7

3.2. PLAGES HORAIRES 8

4. DANS L'INFRASTRUCTURE DE L'HEBERGEUR 9

5. ARCHITECTURE 10

6. PREREQUIS 11

3.3. PRINCIPE DE FONCTIONNEMENT 11

3.4. FILTRAGES SUR NOTRE PARE-FEU 11

3.5. PORTS POSTE CLIENT 11

3.6. FILTRAGES EN SORTIE SITE 11

3.7. RESOLUTION DE NOMS 12

3.8. COMPTE UTILISATEUR 12

3.9. CONFIGURATION DU POSTE DE TRAVAIL 12

7. LA SECURITE DANS SIHAM-PMS 12

8. REVERSIBILITE ET TRANSFERABILITE 12

1. PREAMBULE

Siham-PMS est une offre de services de l'AMUE qui permet aux établissements, via un abonnement et une connexion sécurisée, d'accéder à des fonctionnalités de pilotage de la masse salariale et des emplois.
Siham-PMS est bâti à partir de la solution standard Scenario-RH de l'éditeur Allshare.

Ce document, destiné aux Directions des Systèmes d'Informations des établissements, a pour objectif de fournir des informations générales et techniques sur les points suivants :

- Le contexte d'implantation,
- Le contenu technique de l'offre de services,
- L'infrastructure,
- L'architecture,
- Les prérequis en établissement,
- La sécurité,
- La réversibilité et la transférabilité.

2. CONTEXTE D'IMPLANTATION

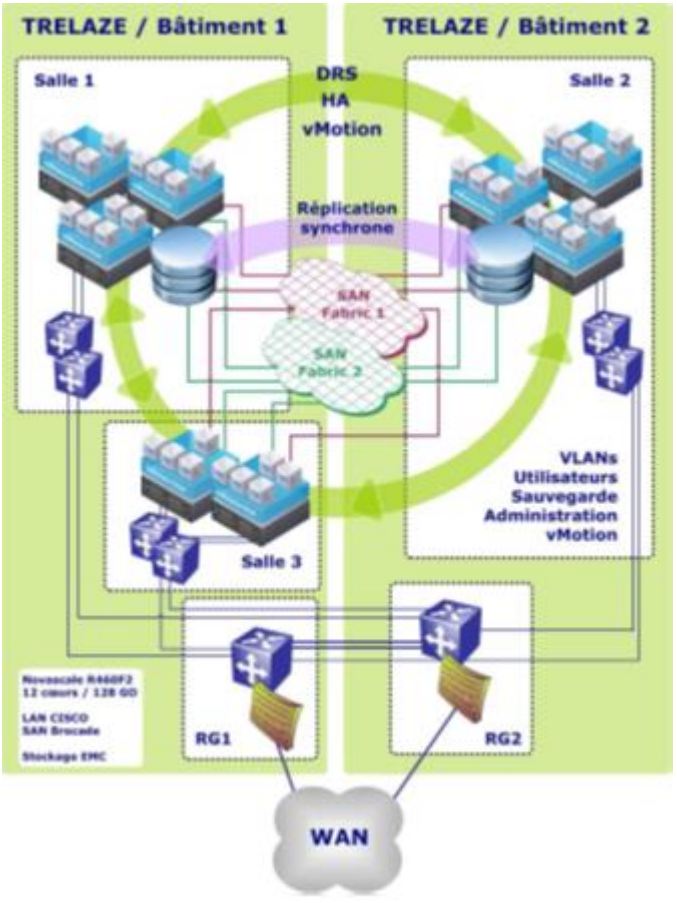
L'offre de services Siham-PMS s'appuie sur l'accord-cadre AMUE relatif à la mise en place d'un centre d'infogérance, dont le titulaire est la société ATOS (anciennement BULL).
Pour la mise en œuvre, l'AMUE a contractualisé avec le titulaire sur la base de deux marchés subséquents distincts afin d'assurer la modularité de l'offre de services :

- Un marché dédié à la mise à disposition de l'infrastructure système et réseau,
- Un marché dédié à l'installation et à l'administration de la plateforme de production Siham-PMS.

Du point de vue des établissements, l'Amue est l'unique interlocuteur. Elle assure elle-même les relations avec la société ATOS.
Ce marché prévoit les prestations de réversibilité permettant à l'AMUE d'assurer une continuité de service (cf. chapitre 8 ci-dessous).
Le mémoire technique relatif à l'accord-cadre est disponible auprès du pôle Achats Mutualisés de l'AMUE.

L'activité d'infogérance d'ATOS en France est certifiée ISO 27001, garantissant un management de la sécurité de l'information pour l'ensemble de son périmètre (hébergement, administration, supervision et exploitation d'infrastructures, de systèmes, de réseaux et d'applications informatiques).
Les enjeux de qualité et de sécurité de l'offre de services Siham-PMS sont couverts par un Plan d'Assurance Qualité et un Plan d'Assurance Sécurité prévus par l'accord-cadre.

Le Datacenter proposé dans l'offre ATOS est situé à Trélazé (Maine-Et-Loire), conformément à la clause du marché qui stipule que les données doivent être hébergées exclusivement en France.
Le site, classé TIER III selon la classification de l'Uptime Institute, fournit une garantie de haute disponibilité grâce notamment à une implantation de l'architecture dans un site de type dual-building.



Sur le plan de l'infrastructure, l'AMUE a fait le choix de bénéficier de l'offre Cloud d'ATOS, construite sur des architectures de serveurs virtualisés utilisant la technologie VMware, ainsi que d'un mécanisme de réplication synchrone du stockage. La réplication est réalisée entre deux baies distinctes situées dans deux bâtiments différents du site de Trélazé. Ce mécanisme permet d'atteindre un RPO optimisé dans tous les cas de dysfonctionnements autres que le sinistre total du site. De plus, l'offre Cloud d'ATOS nous permettra de bénéficier de manière transparente des évolutions futures en termes de matériels et de logiciels liés à l'infrastructure.

En termes de niveau de support, Siham-PMS bénéficie d'une couverture de type « PREMIUM » incluant notamment une supervision 24h/24 7j/7 et une résolution des incidents sur cette même plage pour les interventions ne nécessitant pas une décision de l'Amue.

3. CONTENU TECHNIQUE

Au travers de son offre de services, l'Amue fournit aux établissements abonnés un accès via le réseau RENATER à la solution Siham-PMS.
L'abonnement initial inclut la fourniture des licences nécessaires (Licences ScenarioRH et runtime base de données) ainsi que la mise en place d'un environnement spécifique à l'établissement (VPN, applicatif client, base de données) dans une infrastructure mutualisée et virtualisée dédiée à l'offre Siham-PMS (Cf. chapitres ci-dessous).

3.1. PRESTATIONS TECHNIQUES

L'abonnement récurrent comprend les prestations suivantes :

- Mise à disposition de l'infrastructure permettant d'exécuter l'outil Siham-PMS dans un environnement sécurisé avec notamment :
  - Un logiciel préconfiguré client VPN, permettant d'initier un tunnel IPsec entre le poste de travail de chaque utilisateur et la plateforme dédiée à Siham-PMS
  - Une infrastructure Citrix dédiée à Siham-PMS
  - Une Etanchéité de l'environnement d'exécution de Siham-PMS entre chaque établissement
  - Un filtrage des flux
- Mise à disposition d'une base de données dédiée à chaque établissement.
- Gestion et configuration des accès utilisateurs.
- Administration, exploitation et supervision de l'ensemble des composants de la plateforme.
  - Surveillance des services applicatifs, de sauvegarde et d'infrastructure
  - Résolution des incidents d'exploitation
  - Administration des infrastructures et des bases de données
- Maintenance applicative de la solution Siham-PMS.
  - Montées de version mineure (plan produit de l'éditeur Allshare, évolutions règlementaires, …) ; généralement 3 par an.
  - Montées de version majeure (OS et SGBD par exemple) ; généralement 1 tous les 2 ans.

- Service de sauvegarde des données de chaque établissement.
  - Les sauvegardes sont exécutées 7j/7 une fois par jour,
  - Les rétentions et planifications suivantes sont appliquées :

Périodicité	Durée de rétention	Type de Stockage	Garantie de Délai de Lancement de la Restauration (hors restauration système)	Planification Standard
Journalière	14 jours révolus	D2D2T[1,2]	<30 minutes 24/7	Du Samedi au Jeudi inclus
Hebdomadaire	31 jours révolus	D2D2T	<30 minutes 24/7	Le second, troisième, quatrième et dernier Vendredi du mois.
Mensuelle	365 jours révolus	D2T[3]	8 heures ouvrées	Le premier Vendredi du mois
Annuelle	1460 jours révolus	D2T	8 heures ouvrées	Le premier vendredi du mois de Janvier

  - Une sauvegarde complète est exécutée au moins une fois par semaine, elle sert de référence pour les sauvegardes incrémentales,
  - Le RPO (Recovery Point Objective)[4] maximum est de 24h,
  - Toutes les sauvegardes sont exécutées sur un réseau de sauvegarde dédié,
  - Externalisation de la dernière itération du cycle de sauvegarde :
    - Du lundi au samedi Inclus chez un prestataire externe
    - Externalisation en véhicule banalisé et climatisé
    - Toutes les cartouches physiques sont chiffrées avec AES 256 bits
    - Valises IP67, norme ATA 300, fermées avec scellé

3.2. PLAGES HORAIRES

Les plages horaires de disponibilité et d'indisponibilité de Siham-PMS sur une semaine type sont :

- **Plage des utilisateurs** : Siham-PMS est ouvert aux utilisateurs du lundi au dimanche de 6h00 à 23h00.
- **Plage de calculs planifiés hors ligne :** Les calculs planifiés hors ligne peuvent s'exécuter du lundi au dimanche de 3h00 à 6h00, hormis un dimanche par mois où la plage de maintenance est étendue (voir chapitre 3.1). Durant cette période, les services applicatifs Siham-PMS sont fonctionnels pour des traitements planifiés par les utilisateurs mais les accès utilisateurs sont coupés.
- **Plage de maintenance quotidienne** : Les services Siham-PMS sont arrêtés pour sauvegarde et maintenance du lundi au dimanche de 23h00 à 3h00 le lendemain. Les sauvegardes sont lancées à partir de 23h00 selon le plan de sauvegarde décrit plus bas.
- **Plage de maintenance exceptionnelle :** Un dimanche par mois, afin de permettre la réorganisation de la base de données, la plage de maintenance est étendue de 23h00 la veille au dimanche 14h00.

Les plages horaires de support Amue auprès des établissements sont conformes à la charte d'assistance Amue.

[1] D2D : disque vers disque, rétention sur disque.

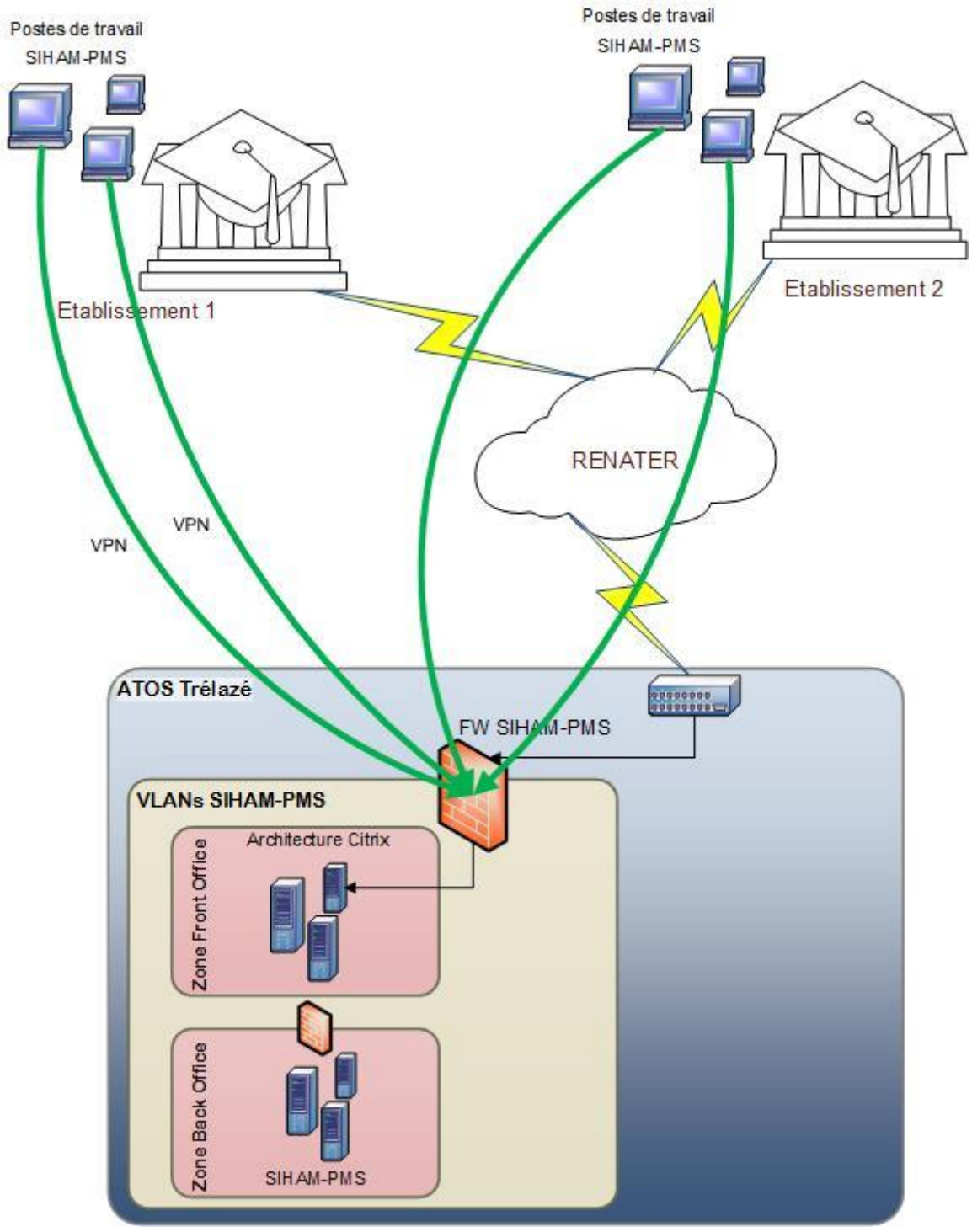
[2] D2D2T : disque vers disque vers cartouche physique, rétention sur disque et sur cartouche.

[3] D2T : disque vers cartouche, rétention sur cartouche.

[4] Le RPO désigne la durée maximum d'enregistrement des données qu'il est acceptable de perdre lors d'une panne.

4. DANS L'INFRASTRUCTURE DE L'HEBERGEUR

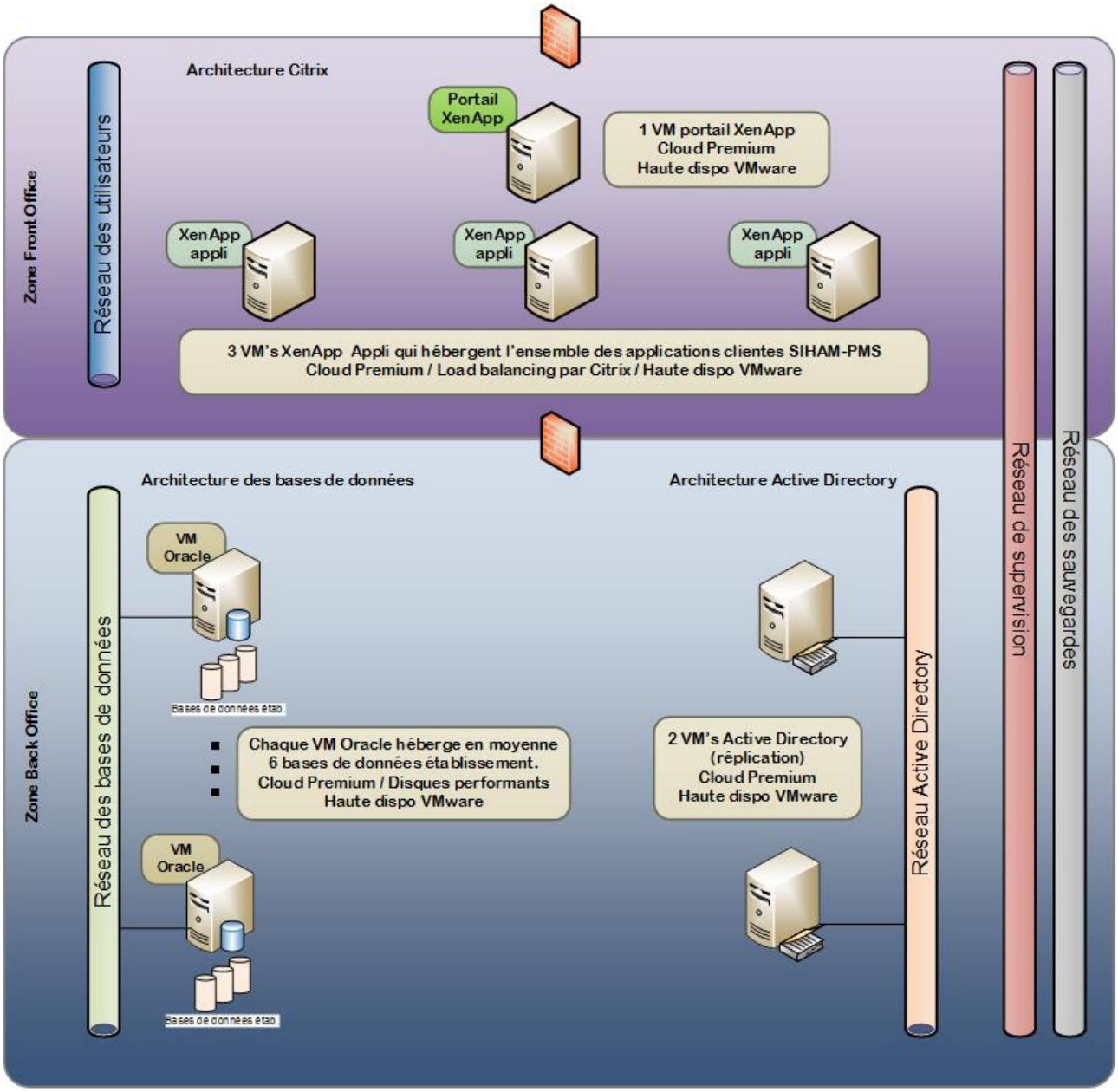
L'accès à Siham-PMS se fait au travers d'un logiciel client VPN installé sur chaque poste utilisateur. Ce VPN IPsec de type « site à site » relie obligatoirement le poste de travail à la plateforme Siham-PMS via un équipement réseau de l'établissement puis le réseau RENATER.
Les VPN aboutissent sur un équipement de sécurité dédié à l'AMUE et protégeant la plateforme Siham-PMS.
Au sein de ces canaux sécurisés, les flux qui transitent sont eux-mêmes chiffrés par la technologie Citrix.



5. ARCHITECTURE

La plateforme de production repose sur des serveurs virtualisés dédiés à Siham-PMS dans une infrastructure mutualisée hautement disponible et dupliquée sur une salle de secours.
A ce jour, l'infrastructure de virtualisation mise à disposition par ATOS est composée d'une ferme de 9 serveurs VMware. Chaque serveur est équipé de deux processeurs Xeon e5-2660 v1.
Cette plateforme Siham-PMS se compose :

- D'une architecture Active Directory : permet la gestion centralisée des utilisateurs, des serveurs et des stratégies de sécurité.
- D'une architecture Citrix : ensemble de serveurs Windows permettant de mutualiser les accès des établissements à leur application cliente Siham-PMS dédiée, tout en assurant des fonctions de sécurité.
- D'une architecture bases de données Oracle : ensemble de serveurs Redhat/Oracle, chacun pouvant héberger en moyenne 6 bases de données établissement indépendantes. Chaque base de données héberge la configuration de la logique métier et les données d'un seul établissement.



6. PREREQUIS

L'accès à Siham-PMS nécessite un certain nombre de prérequis techniques dont un résumé est rassemblé dans ce chapitre.
Tous ces prérequis sont détaillés au sein d'un document fourni à tout établissement qui s'engage dans le déploiement de Siham-PMS.

3.3. PRINCIPE DE FONCTIONNEMENT

Siham-PMS n'est accessible qu'au travers d'un réseau privé virtuel (VPN IPsec) établi obligatoirement au travers d'une passerelle de votre établissement.
Le tunnel VPN relie alors directement, via le réseau RENATER, le poste de travail de l'utilisateur au pare-feu protégeant l'accès à la plateforme Siham-PMS. Côté poste de travail, le tunnel VPN est mis en œuvre via le logiciel « TheGreenBow VPN Client », fourni par l'AMUE et accompagné d'une configuration spécifique à votre établissement. Il n'est pas prévu d'accès à Siham-PMS en mode nomadisme et en particulier depuis le domicile des utilisateurs.
Une fois le tunnel ouvert, les utilisateurs continuent d'avoir accès aux ressources de bureautique fournies par le réseau local (split-tunneling) telles que les imprimantes réseaux, les lecteurs partagés, …

3.4. FILTRAGES SUR NOTRE PARE-FEU

Afin que nous puissions configurer les VPN sur notre pare-feu, ainsi que pour activer une restriction d'accès à chaque base établissement, il nous est nécessaire de connaître les adresses IP des postes utilisateurs et l'adresse IP publique de la passerelle par laquelle ceux-ci sortent de votre réseau établissement.
Si les postes des utilisateurs Siham-PMS sont dotés chacun d'une adresse IP publique, seules ces adresses nous sont nécessaires.
Si les postes des utilisateurs Siham-PMS sont dotées d'adresses IP privées, nous attendons pour chaque poste l'adresse privée (ou à défaut la plage d'adresses en cas d'allocation dynamique) ainsi que l'adresse publique de NAT.

3.5. PORTS POSTE CLIENT

Les communications réseau sur un petit nombre de ports doivent être autorisées entre chaque poste de travail en établissement et les serveurs Siham-PMS.

3.6. FILTRAGES EN SORTIE SITE

Le document des prérequis client vous donnera également l'adresse IP de notre pare-feu à filtrer.

3.7. RESOLUTION DE NOMS

Le nom « sihampms.services.amue.fr » du portail de connexion Siham-PMS doit être résolu au niveau de chaque poste de travail, soit par une entrée spécifique dans le fichier « hosts », soit par une entrée sur votre serveur DNS.

3.8. COMPTE UTILISATEUR

Afin de pouvoir accéder au service Siham-PMS, tout utilisateur doit obtenir auprès de l'AMUE les informations de connexion (comptes nominatifs et mots de passe) permettant de s'authentifier sur la plateforme Citrix dans un premier temps et dans l'application Siham-PMS proprement dite.

3.9. CONFIGURATION DU POSTE DE TRAVAIL

Chaque poste de travail doit être un ordinateur de bureau Windows équipé de Microsoft Excel, d'un navigateur récent, du client VPN TheGreenBow et du client Citrix Receiver téléchargeable depuis le portail de connexion Siham-PMS.

7. LA SECURITE DANS SIHAM-PMS

Siham-PMS s'efforce de garantir un niveau de sécurité à « l'état de l'art », en mettant un accent particulier sur la confidentialité des données des établissements.
Par ailleurs, l'offre de services Siham-PMS doit se conformer au Référentiel Général de Sécurité (RGS).
Dans ce cadre, une analyse de risques et un audit de sécurité ont été menés par l'AMUE, avec le soutien d'un prestataire d'audit de la sécurité des systèmes d'information (PASSI) qualifié par l'ANSSI.
L'homologation de sécurité du télé-service Siham-PMS a été prononcée le 24 mars 2015 pour une durée de trois ans. Vous pouvez retrouver la décision d'homologation sur le site internet de l'AMUE.

8. REVERSIBILITE ET TRANSFERABILITE

L'AMUE ne diffuse pas Siham-PMS de façon classique et ne prévoit donc pas d'installation en établissement. Siham-PMS est uniquement accessible en mode services.
Au travers de l'accord-cadre relatif à la mise en place d'un centre d'infogérance, l'AMUE bénéficie d'un plan de réversibilité activable sur toute la durée du marché.
Cette réversibilité assure :

- La continuité des services Siham-PMS en cas de changement du titulaire du marché,
- La possibilité de transférer sur une structure publique tout ou partie des prestations assurées par le titulaire.

Dans le cas où un établissement souhaiterait mettre fin à la convention Siham-PMS conclue avec l'AMUE, et exclusivement dans ce cas, l'AMUE s'engage à fournir sur demande la base de données Scenario-RH de cet établissement sous forme d'export Oracle. Cet export contiendra les données métier propres à l'établissement ainsi que la configuration spécifique à Siham-PMS au jour de l'exportation.
L'AMUE pourra également fournir à l'établissement qui en fera la demande une prestation d'accompagnement dans la mise en place de sa propre solution Scenario-RH.