REQUEA
Open Solutions

SECURITE

Cœur de réseau REQUEA

C.I.A.

Confidentiality, Integrity, Availability

Confidentialité

Intégrité des données

Haute disponibilité

139 rue Vendôme, 69003 Lyon
www.requea.com

Table des matières

1. Sécurité

1.1. Principes généraux de sécurité

La sécurité des plateformes REQUEA (Réseau, firmware embarqués, IoT) est une problématique qui a été intégrée dès la conception des logiciels REQUEA (2006). Elle s'est renforcée au cours du temps et est devenue un axe d'amélioration continue de nos produits et solutions.

2006 – Développement de la première plateforme**. JAVA est choisi et imposé pour des raisons sécuritaires**. PHP est interdit dans tous les développements REQUEA.

2010 – REQUEA est choisi par CapGemini et Orange pour déploiement dans les SI internes des opérateurs de télécommunication ou opérateurs de réseaux (SFR, Orange, RTE, M2OCity). **Les premiers audits sont réalisés**. Ces plateformes sont pour la plupart déployées en mode haute disponibilité et on premise.

2012 – REQUEA est mis en place dans les SI de Schneider Electric et les **audits de sécurité externes** sont réalisés par Sogetti.

2013 – Support des **architectures PKI** pour authentification et cryptage des systèmes distribués (passerelles)

2014 – Support des **authentifications SAML et ADFS**. Support généralisé des **protocoles https et wss**.

2018 – REQUEA est audité par Ernst & Young pour déploiement pour le compte des Services du Premier Ministre pour **déploiement dans le réseau OIV sécurisé de l'Etat** (Opérateur d'importance vitale – Hotel Matignon). Premier audit en black et white box.

2020 – REQUEA choisit de ne plus supporter les passerelles dont les constructeurs refusent d'ouvrir leur firmware pour audit par REQUEA. Abandon des marques chinoises. Concentration sur Multitech (USA) et Kerlink (France)

2023 – Lancement du processus devant mener à la **certification ISO 27001.**

1.2. Sécurité et Radio (LoRaWAN)

La sécurité est renforcée par l'utilisation de protocoles ouverts, où chaque acteur de l'Alliance LoRa discute, critique et apporte une contribution à la sécurité globale des systèmes. De fait, les systèmes basés sur des protocoles ouverts et construis sur une base de collaboration avec des niveaux de sécurité beaucoup plus élevés que les systèmes propriétaires.
A titre d'exemple, Linux est reconnu ayant un niveau de sécurité supérieur à Windows même si l'utilisation par Microsoft de technologies open source a énormément fait progresser la sécurité des solutions Microsoft ces dernières années.
En radio, on retrouve les mêmes problématiques. REQUEA détecte, évalue et collabore avec les constructeurs pour améliorer la sécurité. Des incidents de cyber-sécurité récents sur des capteurs ont été détectés par REQUEA et la collaboration avec les constructeurs permet une amélioration permanente.
Les aspects sécurité font l'objet d'un document (PAS) qui est mis à jour en fonction des spécificités du projet.

1.3. Mise en œuvre des principes généraux

1.3.1. Chiffrement des flux

La totalité des échanges sont cryptés :

- Toutes les communications entre les capteurs et les passerelles : cryptage standard LoRaWAN (clés NetSkey)
- Toutes les communications entre les passerelles et le cœur de réseau LoRaWAN sont cryptées via une connexion TCP / TLS (certificat SSL X509)
- Toutes les communications entre le cœur de réseau LoRaWAN et la plateforme de services sont cryptées via le protocole MQTTS (sécurisé)
- Toutes les communications entre la plateforme de services et le système tiers sont cryptées par utilisation d'une liaison https (sécurisé)

1.3.2. Authentification des utilisateurs

L'application peut utiliser des solutions de type SSO (Single Sign On) et délègue l'authentification à une application de type IdP. Elle supporte les protocoles SAML, CAS, OpenID, Auth0. Dans tous les cas, les jetons de sécurité sont vérifiés par le serveur applicatif qui communique avec le serveur IdP par des mécanismes de type « Back Channel » (CAS, OpenID Connect en mode « authorization code flow ») ou par du Frant Channel sécurisé (SAML/ ADFS). Les entrées en session sont inscrites dans la base de données et consultables simplement par les administrateurs. Les échecs de session sont inscrits dans un fichier de log spécifique.

1.3.3. Traçabilité des opérations et audit

Les modifications d'objets importants (paramétrage de capteurs, passerelles) sont enregistrées dans la base de données et une interface utilisateur simple et intuitive permet au gestionnaire la consultation des modifications (auteur de la modification, date et heure, champ modifié avec ancienne valeur et nouvelle valeur). Une modification sur une passerelle, date d'installation d'un capteurs, etc... sont ainsi enregistrés et consultables par les gestionnaires (avec ancienne et nouvelle valeur).

1.3.4. Cybersécurité et tests de sécurité

La plateforme REQUEA est fréquemment testée et audités à l'initiative de clients. Les audits sont réalisés par des experts en sécurité. Dans les dernières années, ont notamment été testés les aspects suivants :

- Injection SQL
- Cross-Site Scripting (XSS)
- Références directes non sécurisées à un objet
- Redirection et Renvois non validés
- Falsification de requête intersites (CSRF)
- Violation de Gestion d'authentification et de Session

Lorsque des failles ont été trouvées lors de ces audits, un correctif a été mis à disposition de tous les clients impactés.
L'attention et la sensibilité des développeurs aux problématiques de cyber-sécurité ont été à l'origine de choix d'architecture qui ont renforcé la sécurité, comme en témoigne le nombre des plugins de type SSO supportés, ou la large couverture des mécanismes de protection des données mis en œuvre.
Un traitement spécifique des points du top 10 OWASP a été apporté.

1.3.5. Segmentation des profils et droits utilisateurs (sécurité verticale)

L'application permet de définir des groupes utilisateurs qui donnent des droits sur des actions possibles ou des visualisations ou non de certaines données (certains champs par exemple).
Les menus qui permettent d'exécuter ces actions ne sont pas visibles aux utilisateurs qui n'ont pas ces droits. Ces droits sont de nouveau vérifiés avant chaque action utilisateur, afin d'éviter l'accès à certaines fonctions par copie d'URL. Les échecs d'exécution sont inscrits dans un journal de log.
Par défaut les groupes admin système, admin radio, visu seule, supervision sont présents. Les groupes sont paramétrables pour retirer / ajouter des droits d'accès. Des nouveaux groupes peuvent être créés pour certains type de populations.

1.3.6. Segmentation des données (sécurité horizontale)

Les différents capteurs peuvent être segmentés par groupes de capteurs. Les utilisateurs ont alors accès à un ou plusieurs groupes de capteurs.

1.3.7. Affectation des profils

Des profils utilisateurs sont affectés aux utilisateurs par l'administrateur.
L'authentification des utilisateurs (saisie du login / vérification des accès) se fait :

- Soit par login / mot de passe – géré par l'administrateur (ou les administrateurs)

- Soit par mise en place d'un SSO. Les protocoles suivants sont supportés nativement : ADFS Microsoft / Active Directory LDAP Microsoft, SAML (Shibboleth, NetIQ), OpenID et CAS.

L'association utilisateur / groupe d'habilitation qui détermine les droits et les objets qu'un utilisateur va avoir se fait :

- soit via l'interface par un administrateur système
- soit automatiquement par récupération des informations d'organisation qui peuvent être présentes dans l'AD (Active Directory) via une passerelle LDAP, ou par récupération des informations de la personne lors du login via SSO (ADFS, OpenID Connect, CAS, …). Des règles de correspondance organisation AD / groupe d'habilitation paramétrables sont mise en place pour assurer la cohérence automatique

Ce type d'intégration et d'automatisation des habilitation lors du login est en place par exemple sur la plateforme déployée aux Services du Premier Ministre (SPM, réseau sécurisé de l'État), au CESE (Conseil Social et Environnemental), et chez de nombreux autres clients privés et publics. (via ADFS, OpenID ou CAS).

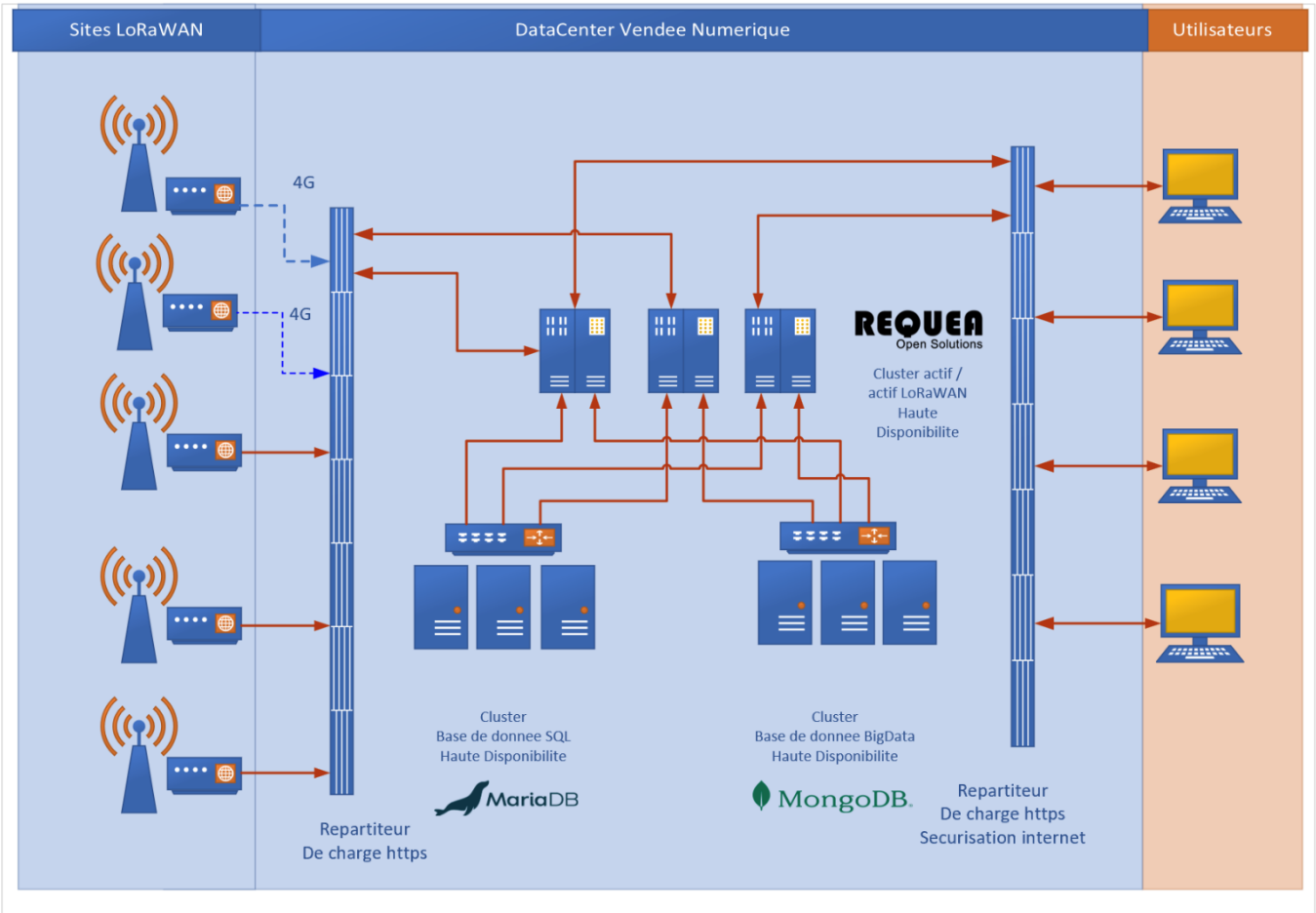
2. Haute disponibilité

2.1. Mise en œuvre des principes généraux

Un déploiement Haute Disponibilité est entièrement supporté sur les architectures REQUEA. Le service en mode SaaS est déployé en architecture Haute Dispo. REQUEA met en place des architectures haute dispo depuis 2014.

L'architecture Haute dispo repose sur plusieurs principes :

- Une absence de « single point of failure », avec une redondance des différents composants. Ces composants sont donc déployés en mode dit « cluster » soit en mode actif / actif soit en mode actif / passif avec failover automatique.
- Les nœuds en mode actif / actif sont dimensionnés pour une charge totale supportable sur un seul nœud. Le mode actif / actif n'est pas utilisé pour de la répartition de charge mais uniquement pour de la redondance.
- Une capacité à faire des mises à jour en permanence par mise à jour des composants individuels par désactiviation des proxys ou répartiteurs de charge, puis mise à jour, puis réactivation du nœud et replcement du nœud dans le cluster.
- Un monitoring individuel des nœuds via DataDog et un monitoring global de chaque composant du service.



2.2. Composants Logiciels

Les composants logiciels déployés en mode cluster / haute dispo sont les suivants :

2.2.1. Plateforme REQUEA / Cœur de réseau

Elle est déployée en mode actif / actif. Les points d'entrée étant des points d'entrée HTTPS ou WSS, la répartition de charge / Failover est un répartiteur standard https qui en général assure aussi le point de terminaison TLS.
La communication entre les nœuds passe par des échanges de données en cache distribué REDIS.

2.2.2. Cache De données : REDIS

Le cache de données et les queues distribuées sont assurés par un cluster REDIS avec une Haute disponibilité configurée avec une architecture de sentinelles REDIS. Le cluster est en mode actif / passif. C'est une architecture standard REDIS. Les clés sont backupées sur disque de manière régulière.

2.2.3. Base de données Relationelle

Les bases de données relationnelles supportées en mode haute dispo sont :

Postgres SQL en version cluster actif / passif avec failover automatique

MariaDB en mode cluster actif / passif (réplication temps réel) avec failover automatique

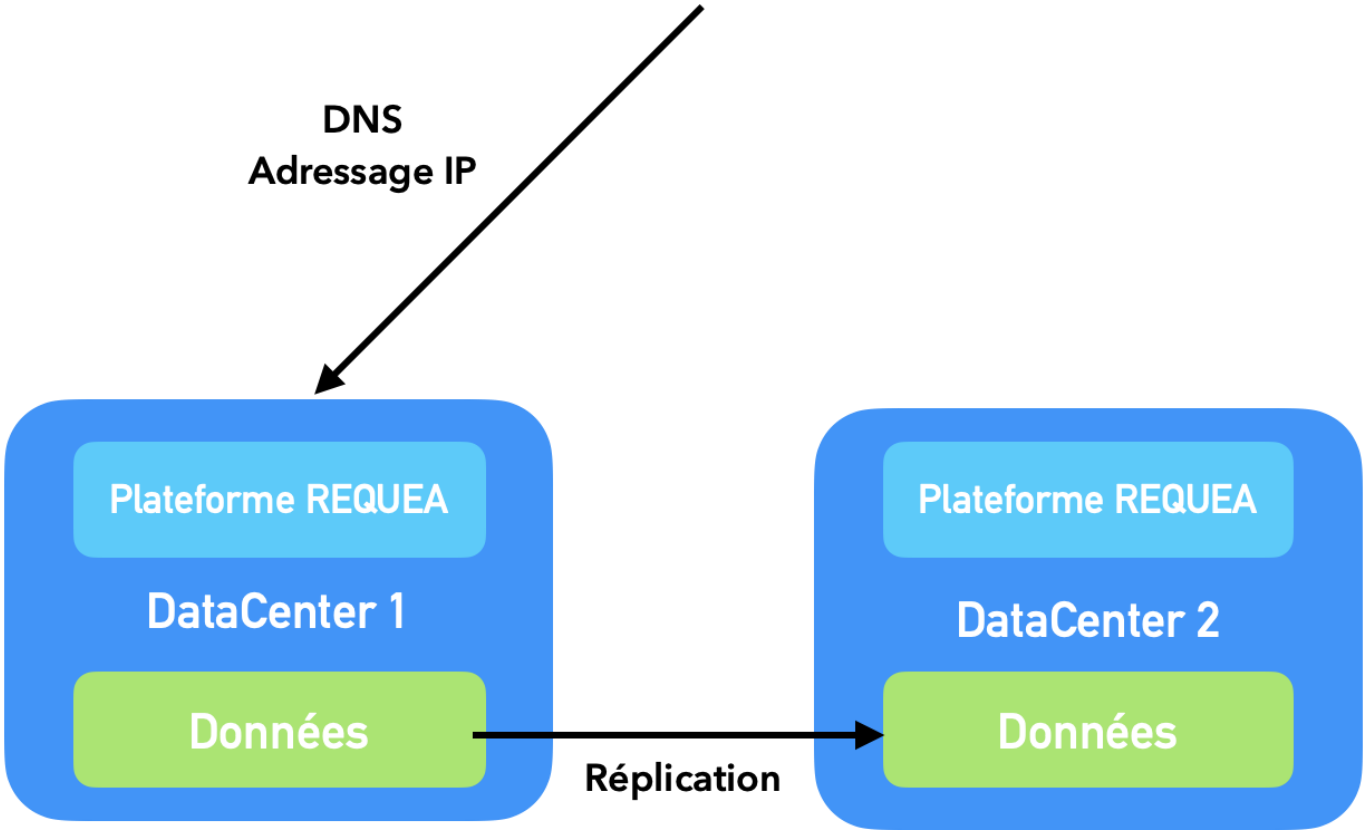
2.2.4. Base de données « Big Data »

Les données à Haut Volume sont gérées dans une base MongoDB. Cette base est déployée en mode Haute dispo en mode actif / passif avec failover automatique.

2.3. Réplication spatiale / Failover

Les bases de données sont réplicables (et répliquées dans le service SaaS) sur un site différent. Cela permet une bascule rapide (moins de 30mns) en cas de rupture complète du site d'hébergement (DataCenter principal). La bascule se faisant dans ce cas par mise à jour des DNS vers le nouveau site.

Le schéma est le suivant :



3. Exigences du SI

Le tableau suivant regroupe les exigences caractéristiques d'un SI client vis-à-vis de la plateforme REQUEA.

N°	Exigences système du S.I.	Réponses	Conformité
	L'hébergement		
1	A qui est sous-traité l'hébergement ?	OVH sur serveurs dédiés sécurisés ou serveurs On Premise	Conforme
2	Quels sont les engagement des services si c'est un sous traitant ?	sécurité physique. Le sous traitant n'a pas d'accès logique aux serveurs	Conforme
3	Quelle est la localisation des données ?	FRANCE	Conforme
4	Fréquence, horaire et localisation des sauvegardes d'infrastructures ?	en permanence en local (arch HD) et 1 fois par jour, durant la nuit sur des NAS offsite (au siège social)	Conforme
5	Rétention des sauvegardes ?	7 jours en local / serveurs, 12 mois en distant	Conforme
6	Combien d'environnement seront mis à disposition ?	2	Conforme
	Sécurité des données		
7	Le fournisseur et/ou l'hébergeur est-il certifié ISO 27001 ?	En cours	Partiellement conforme
	Sécurité de l'infrastructure		
9	>Qui a accès aux serveurs (physiquement ou logiquement) hébergeant l'application ?	Logiquement : Employes qualifiés REQUEA	Conforme
10	>Quelles sont les mesures prises pour protéger les serveurs (patching, segmentation, firewall, …) ?	patching, segmentation, firewall, access double auth	Conforme
	Sécurité applicative		
11	>L'application fait-elle l'objet d'audit de code ?	Oui	Conforme
12	>L'application fait-elle l'objet de tests d'intrusion ?	Oui	Conforme
13	>Dans le cas d'une application mode Web, quels sont les dispositifs de protection du site ?	securisation anti DDoS, point d'entrée https TLS uniquement	Conforme
14	>Qui a accès aux fonctions d'administration de l'application et des accès ?	Employes qualifiés REQUEA	Conforme
	Protection des données		

15	>Comment est assurée l'isolation vis-à-vis des autres clients ?	Base de données séparées	Conforme
16	>Est-on assuré de l'isolation vis-à-vis des équipes de support ?	oui	Conforme
17	>Quels sont les mécanismes de sauvegarde des données ?	Sauvegarde automatique 1 fois par jour	Conforme
18	Pouvez-vous fournir le plan d'assurance sécurité ?	oui, sur demande	Conforme
19	Dans le cadre de données personnelles, est-ce que le futur partenaire Saas répond aux dernier critère concernant le RGPD ?	oui	Conforme
	Les mises à jour et le traitement des anomalies		
20	A quelle fréquence moyenne des mises à jour sont-elles proposées ?	MAJ de sécurités immédiates sous 24h, MAJ autres 1 fois/semaine	Conforme
21	Sous quel délai et comment le client est-il informé d'une prochaine mise à jour ?	sur demande	Conforme
22	Le client a-t-il possibilité de refuser ou reporter le passage sur une nouvelle version ?	Reporter en cas de nécessité	Conforme
23	Sous quel délai une correction peut-elle être apportée dans le cas d'une anomalie majeure (fonctionnalité bloquée) ?	Dans la journée	Conforme
24	Existe-t-il un environnement de recette pour permettre au client de valider les mises à jour (correctives ou évolutives) ?	Oui	Conforme
25	Quelles sont les conditions de prise en compte d'une demande d'évolution touchant le logiciel ?	Validation par un responsable REQUEA	Conforme
26	Est-on sujet à des évolutions règlementaires ? Si oui, quels sont les engagements ?	oui	Conforme
	L'exploitation		
	Engagement de service (SLA)		
27	>Disponibilité du service logiciel, RTO et RPO	0,999	Conforme
28	>Temps de réponse applicatif (définir les points de mesure)	250ms	Conforme
29	>Eventuellement, vitesse de traitement (volumétrie/durée)	selon traitement	Conforme
	Sauvegarde		
30	>Y-a-t-il des sauvegardes « légales » ?	oui	Conforme
31	>Quels sont les engagements qui peuvent être pris ?	conservation et sécurisation des données	Conforme
32	>Peut-on faire un retour arrière sur les données ? Si oui, avec quelle granularité ou à quel moment précis ?	oui, sur demande	Conforme

	Support et communication		
33	>En cas de panne ou de maintenance planifiée, indiquez le mode de communication mis en place - Sachant qu'on privilégie le mode push to user (via mail par exemple) et non pas l'utilisateur va chercher l'info		Conforme
34	>Y-a-t-il des créneaux de maintenance prédéfinis ?	6h00-8h00	
35	>Comment joindre le support et sur quels créneaux ?	Adresse mail, téléphone; 8h - 18h	Conforme
36	>Précisez si le support est bien en français	Oui	Conforme
37	>Décrire l'arbre résolution préconisé sachant que le client dispose d'un assistance informatique pouvant effectuer les premières mesures et que le client détachera une entité (ou un collaborateur) pour jouer le rôle de relais et de contrôle de la bonne application du partenariat	Client ou intégrateur niveau 1, et 2, REQUEA niveau 3	Conforme
	Montée en charge		
38	>Quels sont les principes de montée en charge	Test de montée en charge quand la charge dépasse des volumétries habituelle	Conforme
	Impressions		
39	>Décrire le mécanisme d'impression (téléchargement de fichiers, ouverture de pdf en ligne, etc.)	impression directe ou ouverture de pdf	Conforme
	KPI		
40	>Préciser les KPI fournis (en terme de Performances, disponibilités et audit d'accès)	Taux de disponibilité, Taux de pertes de message	Conforme
41	>Le client sollicitera un compte non SSO pour dérouler une routine simple permettant de mesurer la dispo et la performance - Indiquez si cela pose une contrainte	non pas de contrainte	Conforme
	Tâches d'exploitation		
42	>Quels sont les engagements de service (Délai) pour une tâche technique standard (Demande de restauration vers l'environnement de recette, changement @ip VPN etc..)	24h	Conforme
	L'accès à l'application		
	Voies d'accès à l'application		
43	>Quels sont les canaux de transports proposés (Internet, VPN IPSec, Liaison privée) ?	Internet https	Conforme

44	>Dans le cas d'accès via Internet, quelles sont les mesures de sécurité prises ? Qui les réalise ?	Accès via login/mot de passe ou SSO	Conforme
45	>Quels sont les mécanismes de sécurité mis en place pour protéger contre les attaques web (SQL injection, XSS, vulnérabilité du serveur web…)	Respect OWASP top 10	Conforme
46	>L'application supporte-t-elle que l'utilisateur se présente avec différentes adresses IP au cours de sa session ?	Oui	Conforme
47	>Est-il possible de restreindre l'accès à une liste de plages d'adresses IP ?	oui	Conforme
	Contrôle d'accès		
48	>La solution supporte-t-elle des mécanismes de SSO ? Si oui lesquels ?	SAML, ADFS, OpenID Connect, Oauth, CAS	Conforme
49	>En cas de support du SSO :		
50	. Pour certains rôles, est-il possible d'avoir une double authentification (ex. authentification SSO + authentification applicative) ?	oui	Conforme
51	. Peut-on mixer contrôle accès via SSO et contrôle d'accès applicatif en fonction des rôles ou des personnes ?	oui	Conforme
52	. Peut-il y avoir une redirection de l'authentification vers nos serveurs d'authentification ? Via quel protocole ?	oui, SAML ou OpenID	Conforme
53	. La définition des rôles peut-elle s'appuyer sur des attributs externes (attributs AD, requête sur annuaire, informations dans jeton SAML, …) Quels sont les mécanismes utilisés ?	oui, SAML	Conforme
54	>Est-il possible d'automatiser le provisionning des accès (déclaration automatisée des utilisateurs) ?	oui via SAML	Conforme
55	>Quelles sont les durées de vie des sessions ? Existe-t-il un mécanisme de libération des sessions déconnectées ?	oui, 30ms	Conforme
56	>Quelle est la politique de sécurité en cas d'authentification applicative ?	politique par roles	Conforme
57	>Comment les administrateurs auront accès aux traces, aux logs de connexion entre autres ?	via l'application	Conforme
	Plan de secours		
58	Le fournisseur a-t-il élaborer un plan de secours ?	oui	Conforme
59	Description de l'architecture mis en œuvre pour assurer le secours et du principe de la reprise	reprise des backups et redémarrage sur architecture distincte	Conforme

60	Le site de secours est-il à un emplacement différent du site principal ?	oui	Conforme
61	Le fournisseur prend-il des engagements ?	oui	Conforme
62	>Quelle est la perte maximale de données en cas de sinistre ?	24h	Conforme
63	>Sous quel délai est assuré le rétablissement nominal du service ?	6h	Conforme
	Réseau		
64	Débit minimum : Débit réseau minimum utilisé par un utilisateur de l'application sur un site distant	appli web utilisable sur cnx ADSL 1MB	Conforme
65	Débit maximum : Début réseau maximum utilisé par un utilisateur de l'application sur un site distant	appli web utilisable sur cnx ADSL 1MB	Conforme
	L'intéropérabilité avec le S.I.		
	Quels sont les méthodes proposées pour intégrer des données dans l'application ?		
66	>Pour l'intégration par lot	API ou Excel	Conforme
67	>Pour l'intégration au fil de l'eau	API	Conforme
	Quels sont les méthodes proposées pour exporter des données de l'application vers le SI ?		
68	>Export par lots	Export fichiers	Conforme
69	>Exports au fil de l'eau (sortie événementielle)	MQTT(s), push http(s)	Conforme
	Exposition d'API		
70	>Quels sont les API exposées par l'application ? Quelles sont les mesures de contrôles d'accès à ces API ?	Contrôle via clé API	Conforme
71	>L'application peut-elle être appelée par des API ?	Oui	Conforme
72	>Existe-t-il des connecteurs vers des solutions du marché ?	Témétra, Nogema, Dioptase…	Conforme
73	Sur quels référentiels externes l'application peut-elle s'appuyer ?	REST	Conforme
	Interactions avec le poste de travail		
74	>Quels sont les formats de fichiers produits ou intégrables ?	PDF, Excel	Conforme
75	>Existe-t-il d'autres interactions ?	Navigateur	Conforme
	Envoi de mails		
76	>L'application envoie-t-elle des mails (ex. tâche à faire) ? Depuis quel(s) adresse(s) uu domaine SMTP ?	Mails d'alarmes via serveur SMTP Amazon	Conforme
	Echange de données		
77	Deux principes : - Si l'application source (Saas ou application) dispose d'API pour la mise à disposition de données, le client (Partenaire Saas ou Saur) vient chercher ses données, pour ses applications propre, via ces API exposées (si elles	Via API	Conforme

	répondent bien aux besoins) - Si l'application source (Saas ou application) propose plutôt de produire des données sur un depôt accessible en mode sécurisé (SFTP) : L'application source dépose ces données directement chez le client et elle assure la supervision de cette bonne mise à disposition jusqu'au dépôt cible		
	Environnement technique client		
	La solution globale respecte-elle les contraintes d'environnement technique actuel pour les postes d'administration et de développement, les postes de production, les postes de consultation (argumenter la réponse) ? :		
78	- Windows 10	Application Web	Conforme
79	- Office 2013 et supérieur	Application Web	Conforme
80	- Acrobat Reader 11	Application Web	Conforme
81	- IE 10 et supérieur	Application Web	Conforme
82	Les modules type Java Runtime environnement à installé sur les PC end-user ne sont pas préconisés - Indiquez si la solution s'affranchit bien de ce type de module	Oui	Conforme
83	Les utilisateurs ne sont pas administrateur de leur poste - indiquer si cela pose un problême pour l'utilisation de la solution	Non	Conforme
84	Préciser si le fonctionnement des solutions en mode HTTP est compatible en environnement sécurisé HTTPS.	Oui	Conforme
	Réversibilité de la solution		
85	Préciser les méthodes de réversibilité de la solution ? Et pour les clés de signatures des documents ?	Réversibilité par extraction des données	Conforme

4. Architecture technique (DAT / Flux)

4.1. A PROPOS

4.1.1. OBJET DU DOCUMENT

Ce document présente le dossier d'architecture technique de la plateforme IoT et cœur de réseau LoRaWAN déployée dans les infrastructures REQUEA ou celle de clients en cas de déploiement dit « On Premise ».

Il décrit comment la solution est implémentée, ses principaux composants et comment ces composants fonctionnent ensemble pour supporter les utilisateurs de la solution.

Certaines considérations opérationnelles sont aussi incluses et servent de fondation au design et à l'organisation des tâches opérationnelles (sauvegarde,…)

4.1.2. PERSONNES CONCERNÉES

Ce document est rédigé à l'attention des personnes suivantes :

- REQUEA : personnels techniques pour revue et approbation
- Client : Services informatique et autres personnels techniques : direction, architectes, testeurs, pour revue et approbation.

4.1.3. PRÉ-REQUIS

Une familiarité avec les architectures réseau est indispensable.

Une connaissance des problématiques de sécurité sur des systèmes distribués est aussi préférable.

4.1.4. STRUCTURE DU DOCUMENT

Ce document est divisé en quatre parties:

- la description de l'architecture générale logique de la solution
- les problématiques de sécurité
- la description des différents composants logiques de la solution
- la description des différents composants en terme de déploiement dans l'environnement de production. Cette partie couvre l'architecture physique

4.1.5. TABLE DES ACRONYMES

HTTP	HyperText Transfer Protocol
JRE	Java Runtime Environment
SSO	Single Sign On
VM	Virtual Machine (VMWare)

4.2. ARCHITECTURE LOGIQUE

4.2.1. PRÉSENTATION GÉNÉRALE

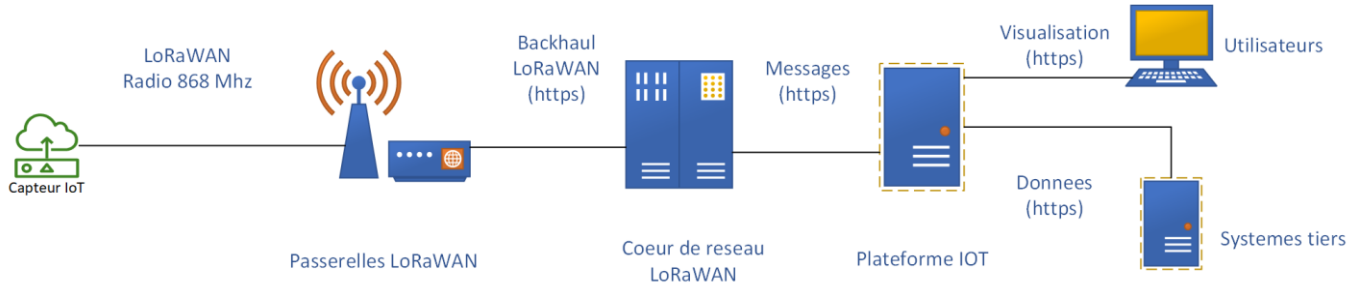
Cette partie est une présentation générale. Les composants sont présentés de manière logique. La description de chaque composant et leur implémentation au niveau physique sont présentées dans les chapitres suivants.

4.2.2. DÉCOUPAGE MÉTIER

La solution IoT répond à deux besoins :

- La gestion du réseau LoRaWAN, et en particulier la supervision des passerelles déployées sur le terrain et l'optimisation des paramètres réseau en lien avec les capteurs déployés
- La plateforme IoT dont le rôle est de traiter, stocker et distribuer les données issues des capteurs

4.2.3. DIAGRAMME GÉNÉRAL



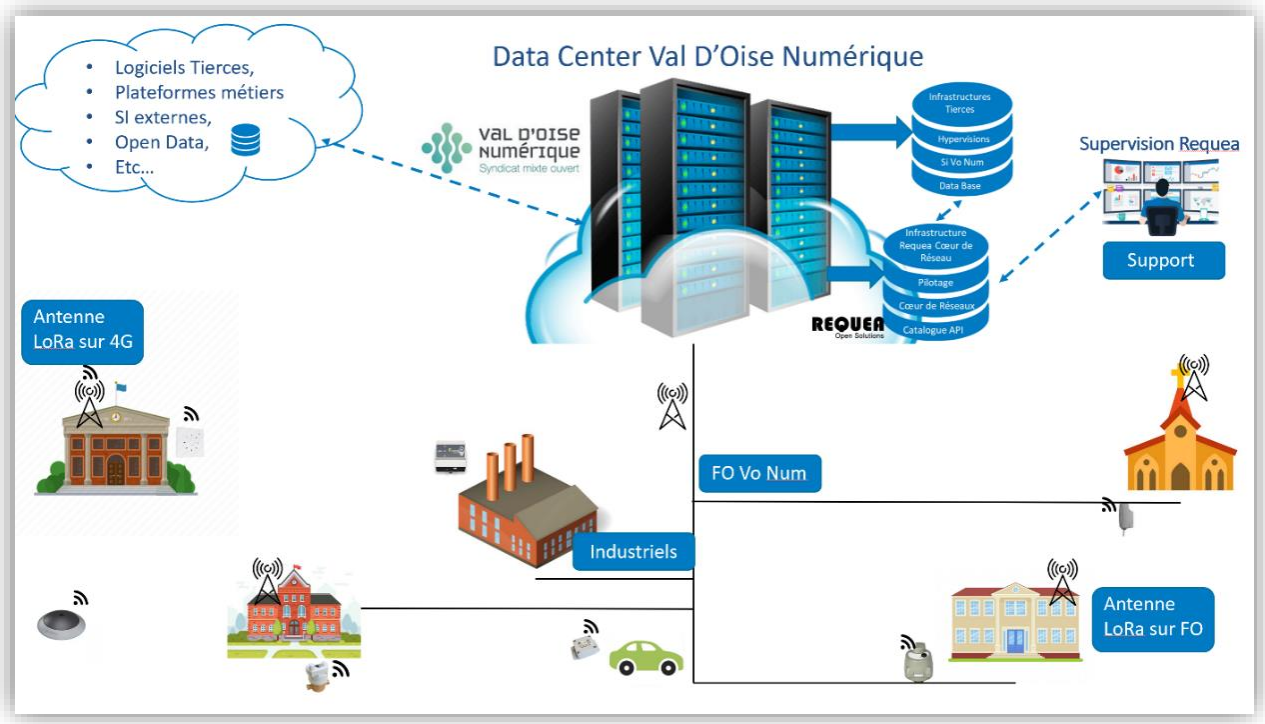
- Les capteurs IoT transmettent leurs données via une communication radio (LoRaWAN) : communication cryptée (double cryptage) avec des clés de chiffrement gérées par le cœur de réseau (Join Server)
- Les passerelles communiquent avec le cœur de réseau (backhaul LoRaWAN) avec une communication sécurisée https (web sockets)
- Les deux principaux composants logiciels de la solution (cœur de réseau et plateforme IoT) échangent leurs messages via des communication https (appels Rest et push https)

- La plateforme met à disposition des utilisateurs des tableaux de bord via un lien classique https et une interface Web sécurisée. Elle pousse aussi les données vers des systèmes tiers (via https)

4.2.4. Mise en œuvre On Premise

Les architectures REQUEA peuvent être déployés en mode SaaS (dans datacenter OVH) ou en mode On Premise (Datacenter client).

Le schéma suivant illustre un déploiement en mode On Premise dans un Datacenter souverain d'une collectivité.

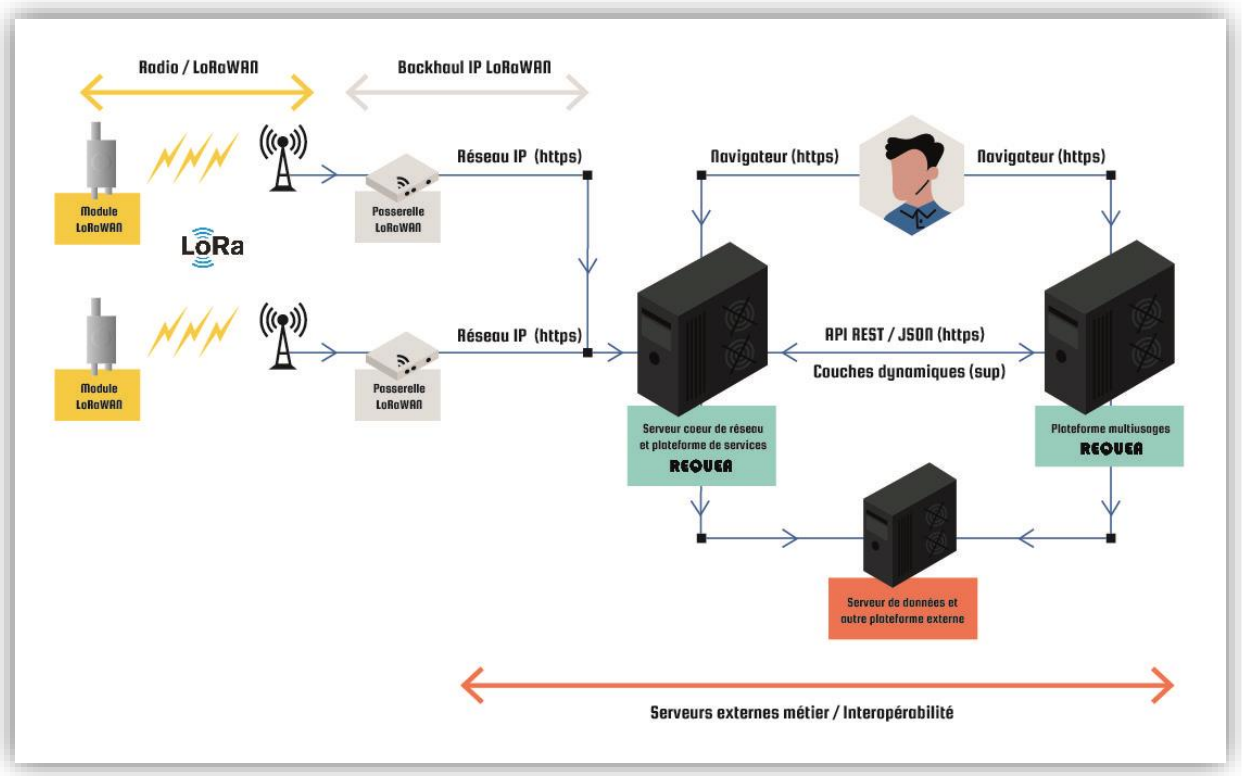


4.2.5. VUE TABLEAU DES COMPOSANTS ET RÔLES

COMPOSANT	COUCHE	NATURE	IMPLÉMENTATION	SYSTÈME D'EXPLOITA- TION	BASE	OWNER	COMMENTAIRE
Capteurs IoT	Capteur	Matériel		na	na		Les capteurs sont déployés sur le terrain et transmettent leurs données via radio
Passerelles	Réseau LoRaWAN radio	Matériel et micro logiciel embarqué	Agents sur couche linux embarquée	Linux	na	REQUEA	
Coeur de réseau	Réseau LoRaWAN radio	Logiciel serveur	Java / Tomcat et process Go Lang / Serveur	Linux	Maria Db Mong oDB Redis	REQUEA	
Plateforme IoT	Données et Visualisation	Plateforme	Java / Tomcat	Linux	Maria Db Mong oDB Redis	REQUEA	
Interface utilisateur / Web	Visualisation	Plateforme	Java / Tomcat	Linux 8	Maria Db Mong oDB Redis	REQUEA	

4.2.6. INTERACTIONS ENTRE COMPOSANTS / Flux

Le schéma suivant précise les flux entre les différents composants. Les tableaux suivant reprennent la matrice des flux.



Tous les flux sont sécurisés (https, ssh) avec un protocole par défaut (https) avec utilisation des dernières version TLS et un respect des règles OWASP top 10.

COMPOSANT	COUCHE	FLUX	IN	OUT	CONTRAINTE DE DÉPLOIEMENT / ROUTAGE	COMMENTAIRE
Passerelles	Réseau LoRaWAN	HTTPS		443 / https	routage vers Coeur de reseau via Reverse Proxy qui assure la sécurisation du point d'entrée	
Coeur de reseau LoRaWAN	Réseau LoRaWAN	HTTP/ HTTPS	Port 80 / Port 443	Port 80 / Port 443	Forward HTTP ou https vers plateforme Iot Forward HTTP ou https dans l'autre sensvers plateforme Iot	http utilisable sur réseau VLN privé
Web users (desktop / navigateur)	Visualisation	HTTPS	443 / https		routage vers Plateforme IoT via Reverse Proxy qui assure la sécurisation du point d'entrée	
Plateforme IoT	Métier	HTTPS		443 / https	Sortie https vers systèmes tiers des collectivités	
Plateforme IoT	Messagerie	SMTPS (StartTLS) ou https		785 / 443	Envoi des notifications (email sortants) ou des SMS (via Esendex)	
Composants logiciels	Maintenance	SSH	22		Access ssh pour maintenance (REQUEA)	

4.3. SÉCURITÉ

4.3.1. ACCÈS RÉSEAU

Les principes de base retenus sont:

Accès utilisateurs par https (443) uniquement. Aucun accès externe via http n'est autorisé.
Les accès publics (https) se font par une ip publique qui écoute que sur le port https(443), à l'exclusion de tout autre protocole non sécurisé
Accès sysadmin par ssh (22) uniquement, avec authentification via certificat ou mot de passe fort.

4.3.2. SEGMENTATION DES DONNÉES

Les données sont segmentées dans la base MariaDb. Une structuration hiérarchique des données, des capteurs est mise en place avec des droits d'accès. Une segmentation par VM avec une base de données isolée par client est possible (et prévue) pour les clients qui le souhaitent.

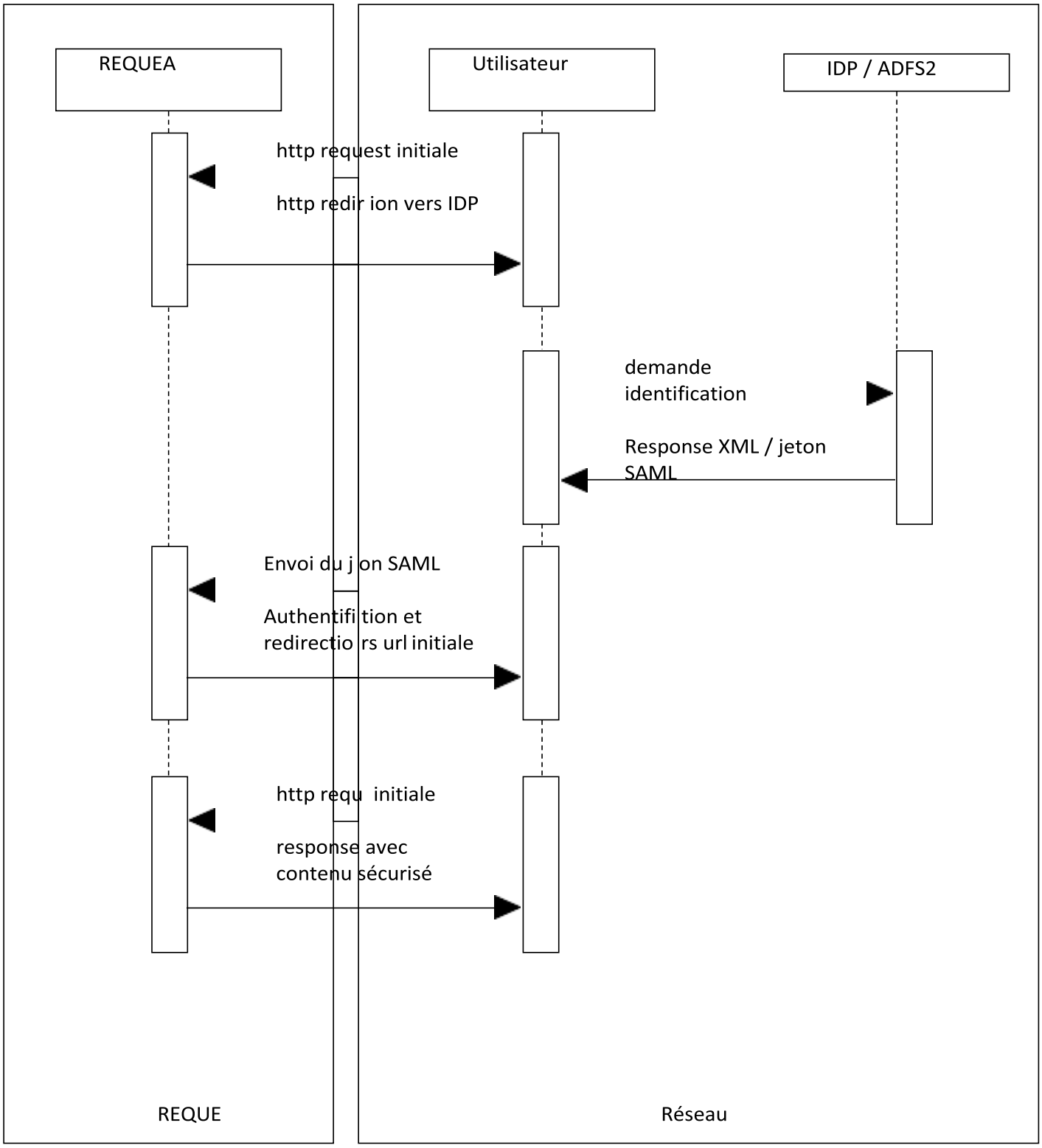
4.3.3. SEGMENTATION DES PROCESS

Chaque Tomcat ou tout autre process serveur est exécuté dans son propre contexte utilisateur Unix. Il n'a pas accès au compte root des machines.

4.3.4. AUTHENTIFICATION UTILISATEURS APPLICATIFS

Les utilisateurs sont authentifiés par login / mot de passe et ont un profil qui leur donne plus ou moins de droits. La vérification du mot de passe peut être effectuée selon deux modes:

- vérification par utilisation de la base de donnée propre aux applications REQUEA
- vérification par SSO sur base SAML (ADFS ou autre). Dans ce cas, la vérification du mot de passe est effectué par l'"Identity provider" du client à l'intérieur de son domaine (AD) :


REQUEA
Utilisateur
IDP / ADFS2
http request initiale
http redir ion vers IDP
demande
identification
Response XML / jeton
SAML
Envoi du j on SAML
Authentifi tion et
redirectio rs url initiale
http requ initiale
response avec
contenu sécurisé
REQUE
Réseau

4.4. ARCHITECTURE LOGICIELLE

Dans cette partie nous intéressons plus particulièrement à la couche métier REQUEA où résident les différentes couches de traitement de l'application :

- Couche présentation. Technologie Web client léger servie par des servlets / jsp sur architecture Java / TOMCAT
- Couche logique métier en technologie REQUEA open source (Dynapage) sur le serveur applicatif
- Couche Workflow servie par la plateforme REQUEA (envoi des notifications)
- Couche persistence pour le stockage des données dans la base MariaDb / MySQL via le driver JDBC, et dans la base MongoDB pour les données à haut volume

4.4.1. ORGANISATION LOGICIELLE

La plateforme IoT et le cœur de réseau sont des applications OSGi (Open Services Gateway interface) orientée service (SOA) implémentées sur la plateforme REQUEA. Elles fonctionnent dans un environnement serveur applicatifs Java de type TOMCAT.

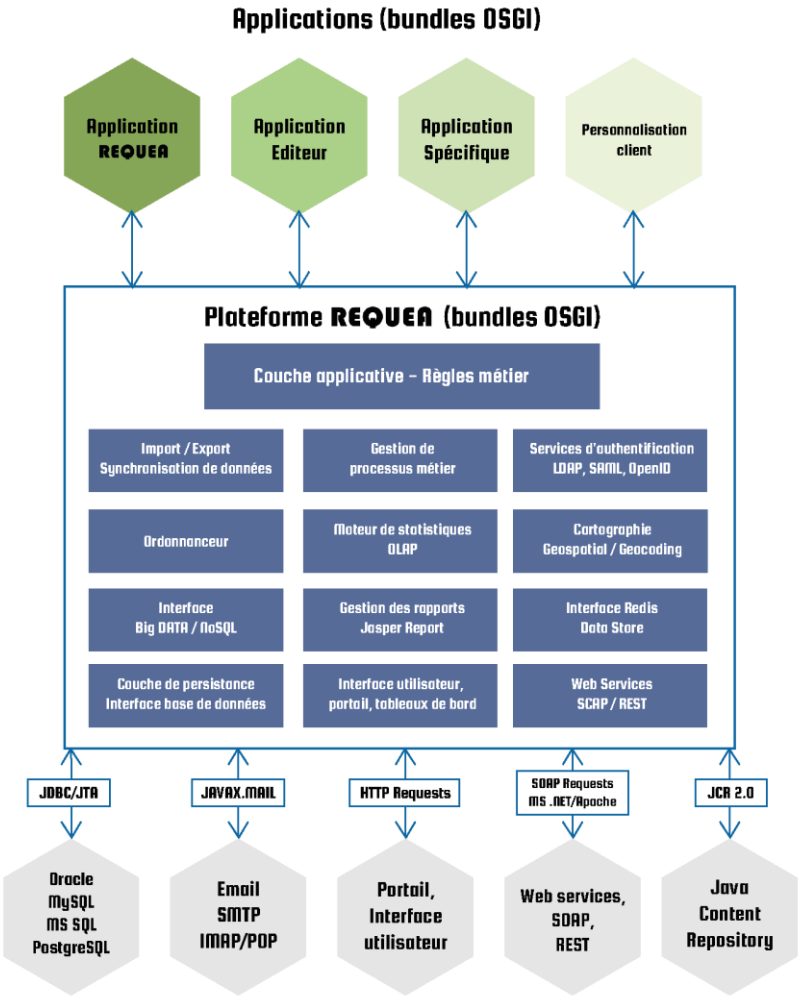
4.4.2. AVANTAGES DE LA PLATEFORME OSGI

OSGi a été introduit pour faciliter l'adoption de JAVA dans les systèmes embarqués. Cependant, les avantages fournis par OSGi ont rapidement été reconnus dans le monde des serveurs d'entreprise. Aujourd'hui de nombreux systèmes sont construits au dessus de plateformes OSGi (Oracle AS, ESB/EAI, Eclipse, ...).

L'intérêt d'OSGi repose sur:

- modularité très forte
- upgrade dynamique et facilité de mise à jour
- gestion des versions et des dépendances entre services

La gestion des versions des plateformes et composants logiciels fournis et déployés sur les différentes plateformes (production, pré- production, test) ainsi que la gestion des versions du paramétrage déployé pour chaque client est ainsi géré directement par le système de gestion des configurations OSGi intégré à la plateforme REQUEA.



Services fournis par l'environnement J2EE

4.4.3. MISES À JOUR DES SERVICES ET PARAMÉTRAGE

Les solutions REQUEA ont une configuration gérée par un service centralisé de gestion des configurations et des versions. Ce service est utilisé pour effectuer les mises à jour des services de la plateforme et des applications déployées.

4.5. ENVIRONNEMENT DE PRODUCTION

Dans ce chapitre nous nous intéressons à l'implémentation physique de l'application et en particulier à l'environnement de production. Ce chapitre décrit le ou les serveurs nécessaires dans l'environnement de production.

Ce chapitre décrit aussi la matrice des flux techniques à prendre en compte ainsi que les aspects plus généraux de sécurité

4.5.1. PRINCIPES DE MISE EN PLACE DE L'ENVIRONNEMENT DE PRODUCTION

Les principes suivants ont été retenus pour la mise en place de l'environnement de production:

Les points d'entrée https (entrée des passerelles et entrée des requetes Web des utilisateurs) sont implémentées par des VM qui servent de reverse Proxy sur base Linux / NginX

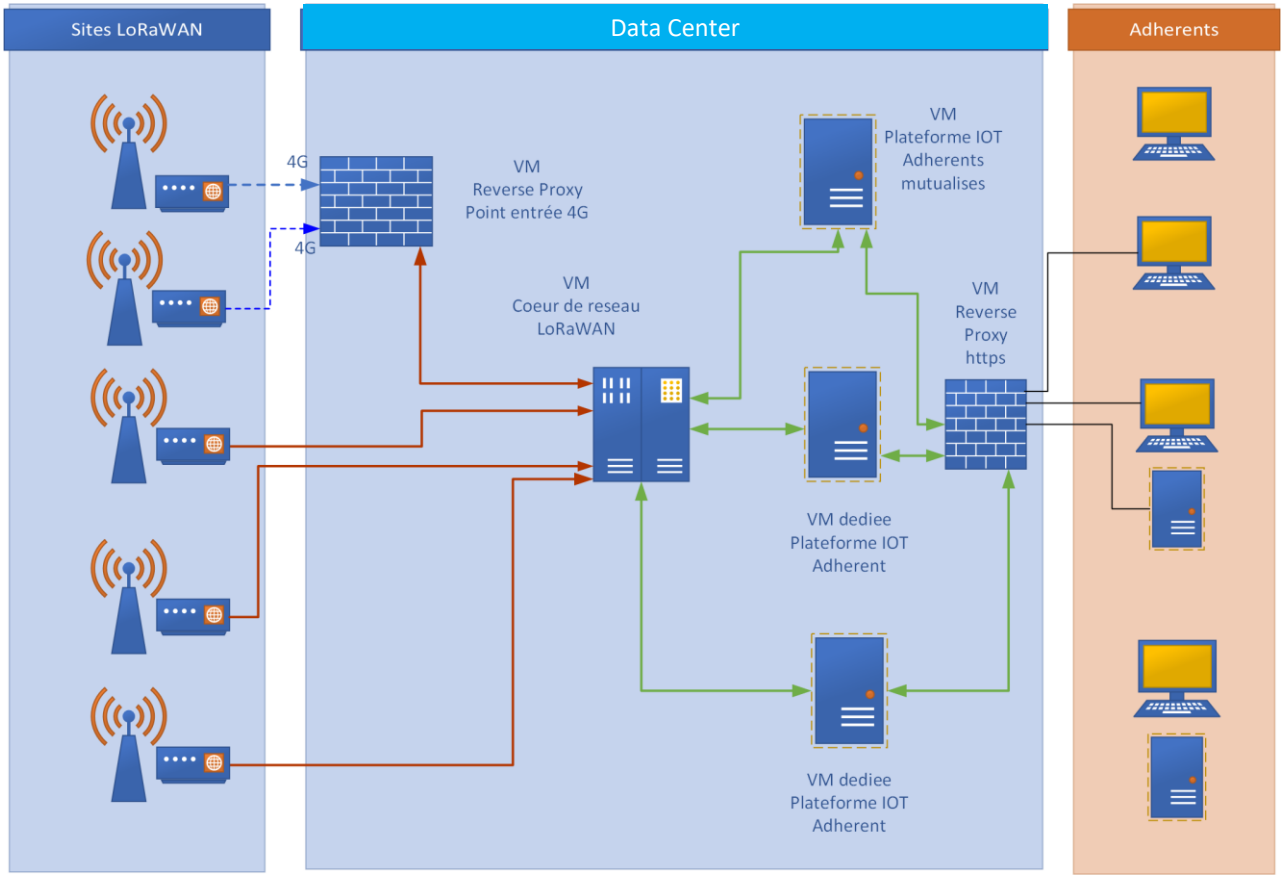
Le cœur de réseau dispose de sa propre VM

Plusieurs plateformes IoT sont déployées sur des VM séparées

Ces principes nous ont conduit à l'architecture suivante:

- En entrée réseau, accès multiples depuis Internet vers les reverse Proxy
- Terminaison HTTPS faite au niveau des reverse proxy puis distribution vers les serveurs applicatifs TOMCAT via http (sur V
- Base de donnée MySQL-MariaDB déployée dans les VM applicatives
- Réseau privé VLAN entre les VM déployées à l'interieur du DataCenter
- PRA et P basé sur la continuté de service fournie par l'infrastructure VM

4.5.2. SCHÉMA GÉNERAL



4.5.3. DIMENSIONNEMENT DES SERVEURS (VM)

4.5.4. VM de production

NATURE	VALEUR MIN / VALEUR RECOMMANDÉE	COMMENTAIRE
RAM	8GB/ 16GB pour les plateformes IoT	
DISQUE	512 GB / SSD pour les plateformes IOT 128GB pour les autres VM	

PARTITIONEMENT	Partition standard Linux datas sur partition spécifique	
COEURS	4 cœurs pour les plateformes IOT et cœur de réseau LoRaWAN 2 cœurs pour les reverse proxy	

4.5.5. SAUVEGARDES en mode SaaS

La plateforme REQUEA en mode SaaS est déployée en mode haute disponibilité avec un objectif de continuité de service et de reprise d'activité (détaillée dans le PRA) :

- Cluster de serveurs applicatifs avec répartiteur de charge en entrée. Le répartiteur de charge a pour objectif d'assurer la haute disponibilité de la solution
- Cluster de serveurs de données (MariaDB et MongoDB) en mode actif – passif avec réplication temps réel. Ces serveurs sont sistués à Roubaix (OVH) dans deux datacenters.
- Backup local des données toutes les 24h vers un serveur situé dans le DataCenter
- Backup en mode hors sol (transfert sécurisé, crypté à 02h00 tous les jours) vers un système de stockage sécurisé situé au siège social de REQUEA à Lyon. Ce backup permet la remontée des système en cas de destruction totale de plusieurs DataCenter OVH.

- Séparation du DNS (hébergé chez AWS / Europe) afin de rebasculer la totalité des services par changement de DNS à tout moment vers un autre prestataire

4.5.6. Sauvegardes en mode On Premise

En mode OnPremise, les sauvegardes sont à la charge du client. Cependant, l'architecture étant standard et classique, elle n'apporte pas de commentaire ou de difficulté particulière.

Elle est détaillée dans le DAT spécifique et inscrite dans le PRA et le PAS du client.

4.6. Exigences de sécurité globales

Les protocoles ouverts au service de la sécurité

La sécurité est renforcée par l'utilisation de protocole ouvert, où chaque acteur de l'Alliance LoRa discute, critique et apporte une contribution à la sécurité globale des systèmes. De fait, les systèmes basés sur des protocoles ouverts et construis sur une base de collaboration avec des niveaux de sécurité beaucoup plus élevés que les systèmes propriétaires.

.

En radio, on retrouve les mêmes problématiques. REQUEA détecte, évalue et collabore avec les constructeurs pour améliorer la sécurité. Des incidents de cyber-sécurité récents sur des capteurs ont été détectés par REQUEA et la collaboration avec les constructeurs permet une amélioration permanente.

Les aspects sécurité font l'objet d'un document (PAS) qui est mis à jour en fonction des spécificités du projet.

Chiffrement des flux :

La totalité des échanges sont cryptés :

- Toutes les communications entre les modules Diehl-G3 et les passerelles : cryptage standard LoRaWAN (clés NetSkey)
- Toutes les communications entre les passerelles et le network serveur sont cryptées via une connexion TCP / TLS (certificat SSL X509)
- Toutes les communications entre le network serveur et la plateforme de service sont cryptées via le protocole MQTTS (sécurisé)

Authentification des utilisateurs :

L'application peut utiliser des solutions de type SSO (Single Sign On) et délègue l'authentification à une application de type IdP. Elle supporte les protocoles SAML, CAS, OpenID, Auth0. Dans tous les cas, les jetons de sécurité sont vérifiés par le serveur applicatif qui communique avec le serveur IdP par des mécanismes de type « Back Channel » (CAS, OpenID Connect en mode « authorization code flow ») ou par du Frant Channel sécurisé (SAML/ ADFS). Les entrées en session sont inscrites dans la base de données et consultables simplement par les administrateurs. Les échecs de session sont inscrits dans un fichier de log spécifique.

Traçabilité des opérations et audit :

Les modifications d'objets importants (paramétrage de modules, passerelles) sont enregistrées dans la base de données et une interface utilisateur simple et intuitive permet au gestionnaire la consultation des modifications (auteur de la modification, date et heure, champ modifié avec ancienne valeur et nouvelle valeur). Une modification sur une passerelle, date d'installation d'un module, etc... sont ainsi enregistrés et consultables par les gestionnaires (avec ancienne et nouvelle valeur).

Cybersécurité et tests de sécurité :

La plateforme REQUEA est fréquemment testée et audités à l'initiative de clients. Les audits sont réalisés par des experts en sécurité.

Dans les dernières années, ont notamment été testés les aspects suivants :

- Injection SQL
- Cross-Site Scripting (XSS)
- Références directes non sécurisées à un objet
- Redirection et Renvois non validés
- Falsification de requête intersites (CSRF)
- Violation de Gestion d'authentification et de Session

Lorsque des failles ont été trouvées lors de ces audits, un correctif a été mis à disposition de tous les clients impactés. L'attention et la sensibilité des développeurs aux problématiques de cyber-sécurité ont été à l'origine de choix d'architecture qui ont renforcé la sécurité, comme en témoigne le nombre des plugins de type SSO supportés, ou la large couverture des mécanismes de protection des données mis en œuvre.

Un traitement spécifique des points du top 10 OWASP a été apporté