Hébergement des infrastructures du SITIV en Datacenter

Cahier des charges techniques particulières

1 OBJET DE LA CONSULTATION

Le SITIV exploite pour le compte de ses villes adhérentes une infrastructure sécurisée numérique d'hébergement des applications informatiques.

Le SITIV collabore avec la ville de Lyon et la Métropole de Lyon dans le cadre du projet France relance, il exploite une infrastructure mutualisée et sécurisée d'hébergement d'une série de solutions collaborative (Messagerie sécurisé, Visio, tchat, partage de documents, édition en ligne, gestion de projet, LMS, ETC.)

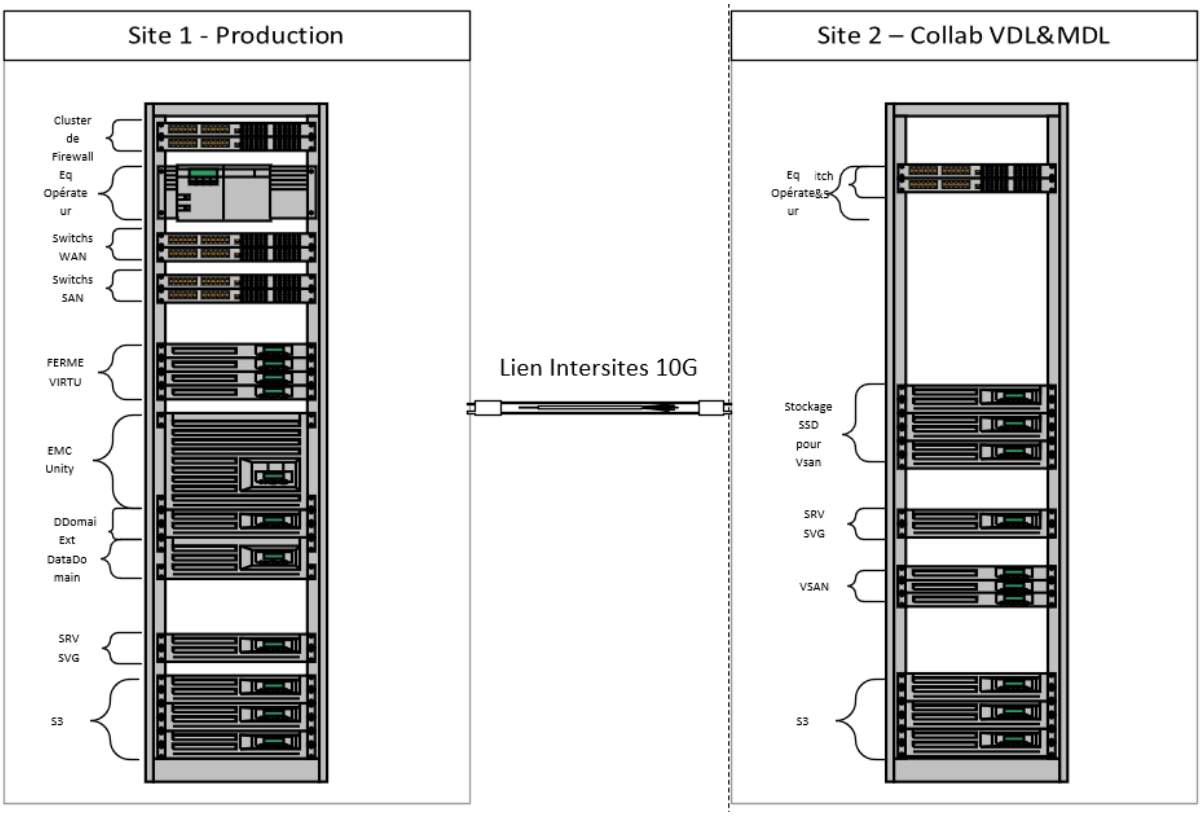
Ces deux infrastructures sont aujourd'hui hébergées dans deux Datacenter sécurisés de la région Lyonnaise ; le SITIV souhaite mettre en œuvre un service d'hébergement de nature « équivalente » en minimisant l'impact sur son exploitation et en assurant une totale continuité de service dans l'objectif d'évolution vers un troisième site à partir de 2024.

1.1 Infrastructures en place

Les deux infrastructures actuelles sont hébergées chez un même prestataire externe spécialisé sur deux sites distincts, avec un lien intersites fourni par le même prestaire et est accédée au travers d'un réseau d'interconnexion sécurisé des 8 Villes adhérentes du SITIV et du SITIV, proposée par l'opérateur télécom titulaire du marché d'interconnexion réseaux de données actuel du SITIV (Linkt).

Les besoins du SITIV en termes d'espace sont aujourd'hui de deux baies de 46 U, sur deux sites différents et pourront évoluer pendant la vie du marché, notamment pour permettre au SITIV de mettre en œuvre un Plan de Reprise d'Activité sur un troisième site.

Schéma physique de l'infrastructure à héberger :



1.2 Présentation du projet

1.2.1 Objectifs

Les objectifs du projet sont les suivants :

- Disposer d'une infrastructure disponible et neutre vis-à-vis des opérateurs de services
- Disposer d'une infrastructure robuste/performante
- Disposer d'une infrastructure sécurisée (au minimum Tiers 3)
- Disposer d'une infrastructure indépendante de potentiels titulaires de marchés passés par l'acheteur public sur d'autres domaines (opérateurs télécoms, intégrateurs d'applications, éditeurs, …)
- Disposer d'une infrastructure accessible facilement et rapidement, à tout moment, au meilleur coût.
- Disposer d'une infrastructure résiliente d'un site à l'autre avec deux accès internet
- Disposer d'une bascule automatique du trafic internet d'un site à l'autre en cas de coupure réseau sur l'un des sites.
- Disposer de liens d'interconnexion de faible latence.

1.2.2 Tierces parties

Le SITIV exploite avec l'aide de prestataires tierce son infrastructure de serveurs. Le titulaire doit préciser ses modalités d'accès et de contrôle au site.

1.2.3 Impératifs de moyens

Type d'infrastructure et capacité

La présente consultation porte sur la fourniture de deux baies minimums sur deux sites différents (ou tout infrastructure équivalente permettant la mise en place de serveurs en production rackables) d'une capacité d'au moins 46 U chacune.

Alimentation électrique :

L'infrastructure de chaque baie dans les deux sites doit être alimentée par au moins deux sources d'électricité distinctes, redondantes et secourues.
La puissance électrique totale devant être disponible est de 3000W par source.

Le prestataire précisera l'ensemble des moyens qui lui permettent :

- D'assurer l'alimentation électrique de son DC
- D'assurer la continuité de l'alimentation électrique des baies lors de coupure du réseau électrique

Le prestataire s'attachera à proposer une vision claire de l'évolution des prix de l'énergie dans son offre.

Dissipation calorifique et climatisation :

Un système redondant de dissipation des calories produites par l'infrastructure du SITIV sera mis en œuvre ; le SITIV appréciera l'ensemble des mesures prises pour permettre l'optimisation de la consommation énergétique et la réutilisation de cette source de chaleur.

Dispositifs de sécurité incendie / extinction départ de feu :

Le Sitiv souhaite connaitre les dispositifs de sécurité incendie mis en place au niveau du bâtiment, de la salle, de la baie.
Le prestataire précisera le type de garantie d'assurance qu'il a souscrit pour permettre l'indemnisation du SITIV en cas de sinistre majeur, et notamment les moyens mis à disposition pour reconstruire les données.

1.2.4 Impératifs de résultats

La qualité de la prestation et son adéquation avec les attentes de l'acheteur public seront mesurées en fonction des indicateurs suivants :

Disponibilité :
Le Sitiv souhaite avoir un taux de disponibilité sur les deux sites de type Tier 3, soit une disponibilité des machines de l'ordre de 99,995 %. La fourniture des services devra donc permettre d'atteindre cet objectif de disponibilité.

Performance :
La qualité de l'électricité fournie et le pouvoir de dissipation réel de la climatisation seront suivis par l'intermédiaire d'informations remontées par nos serveurs et, si le titulaire le souhaite, par le système de monitoring du titulaire. Le titulaire doit indiquer quelle est la température de fonctionnement disponible dans la salle d'hébergement. De même, il souhaite pouvoir bénéficier d'une fourniture électrique stable en tension.

Certifications
Le prestataire devra être certifié ISO27001 (ou équivalent) permettant ainsi au SITIV de s'assurer que le prestataire s'inscrit dans une démarche continue de la qualité que ce soit au niveau de ses processus, de la compétence des personnels ainsi que dans la protection des informations critiques.

La certification SecNumCloud serait fortement souhaitée, une inscription dans cette démarche le cas échéant ça permettra ainsi de rassurer le SITIV sur la prise en compte du prestataire des enjeux de la Cyber Sécurité.

La certification ISO50001 serait également fortement appréciée ; à défaut le prestataire montrera ainsi son engagement à réduire l'impact sur le climat, à préserver les ressources et à améliorer ses résultats grâce à un management efficace de l'énergie. (Une inscription dans cette démarche serait acceptée)

Sécurité d'accès :
Le Sitiv souhaite bénéficier d'une sécurité physique optimale 7/7J 24/24H, un contrôle d'accès doit être effectué. Les accès physiques doivent être listés et conservés en cas de recours.

1.2.5 Données publiques / Cloud Souverain / Archivage

Le SITIV, et ses villes adhérentes, en tant que collectivités locales, sont soumises à l'obligation de sauvegarde des données patrimoniales.
A ce titre, et dans le cadre de la directive nationale Secnumcloud, le prestataire décrira les engagements qu'il est susceptible de prendre pour répondre aux contraintes de cette instruction. Le prestataire fournira donc les éléments de composition de son capital.
Le SITIV souhaitant mettre en œuvre un réseau d'interconnexion public sécurisé, il sera très attentif à la capacité de l'hébergeur de s'interconnecter avec le RIP de la Métropole de Lyon et du département de la Loire et de la ville de Lyon.

2 DUREE

Ce marché sera notifié pour une période de 3 ans, reconductible 1 fois pour la même durée soit une durée totale de 6 ans.

3 MODE D'ACQUISITION DU MATERIEL DE LA PLATE-FORME

3.1 Aspects généraux

Le candidat devra fournir les dimensions des baies d'hébergement, la puissance maximale pouvant être tirées par arrivée électrique, ainsi que les PDU proposées (prises C13, prises C19 souhaitées).

3.1.1 Localisation

Le candidat devra préciser où sont situés les sites d'hébergement. Au vue des exigences techniques il démontrera sa capacité à offrir **un faible niveau de latence entre les sites** et à se conformer aux directives **secnumcloud**.

Il cherchera à offrir dans un espace territorial de faible distance deux à quatre sites dans lesquels il pourra offrir des espaces d'hébergement.

3.1.2 Electricité

Le candidat devra préciser :

- L'infrastructure principale d'alimentation électrique de la plateforme.
- L'infrastructure en place en cas de coupure électrique (nombre de groupes électrogènes, montage en cascade…).
- Si une dégradation du niveau de service peut avoir lieu en cas de rupture d'alimentation électrique externe. Si oui, à quel niveau ?
- Le mode d'activation du circuit de secours électrique de la plateforme :
    - Déclenchement automatique sans interruption du service
    - Déclenchement automatique avec interruption du service
    - Déclenchement manuel
    - Autre(s)
- Le délai sous lequel le système de secours prend le relais à la suite de la coupure d'alimentation principale.
- L'autonomie maximale de la plateforme en cas de coupure d'alimentation électrique externe.

3.1.3 Climatisation

Le candidat devra préciser :

- La ou les solutions de climatisation en place autour de la plateforme.
- Le niveau de température garanti.
- Le taux d'humidité garanti.
- Comment l'air climatisé est-il injecté et extrait dans la baie.

3.1.4 Sécurité incendie

Le candidat devra préciser :

- Si le bâtiment possède une infrastructure de sécurité incendie.
- L'infrastructure de sécurité incendie au niveau de la salle d'hébergement :
    - Utilisation d'un gaz inerte
    - Autre(s)
- S'il existe un dispositif anti-incendie au niveau de la baie
- Le niveau de certification APSAD (ou équivalent)

3.1.5 Sécurité physique des accès

Le candidat devra préciser :

- Le mode d'identification pour l'accès à la plateforme :
  - Accueil par personnel dédié
  - Badge magnétique
  - Code individuel pour les personnes autorisées
  - Autre(s)
- Les moyens mis en œuvre pour la sécurité physique globale du site ?

3.1.6 Réseau, Trafic internet & Sécurité

Le SITIV souhaite disposer d'une offre de trafic internet / symétrique à débit garantie accessible depuis la baie du Datacenter.

Au vue des besoins des projets du SITIV, la capacité du candidat à offrir les débits les plus élevés sera appréciée.

Le prestataire précisera les tarifs qu'il propose pour différents débits :

- 100 Mbps
- 200 Mbps
- 1 Gbps
- 2.5 Gbps
- 10 Gbps

Le SITIV souhaite également disposer d'adresse IP publiques.
Le prestataire précisera les tarifs qu'il propose pour :

- 15 adresses
- 30 adresses
- 62 adresses
- 126 adresses

Le prestataire précisera les tarifs qu'il propose pour une solution anti DDOS.

Le SITIV est à date engager avec l'opérateur Linkt dans le cadre d'un marché fournissant des liens d'interconnexion de données entre les sites des villes adhérentes au SITIV et les datacenters existant.
Le prestataire précisera le niveau de présence de l'opérateur dans ses locaux, une présence physique existante en Meet Me Room est souhaitée.
Il chiffrera les éventuels frais de construction d'un point de présence de cet opérateur et en garantira le délai de mise en œuvre. La livraison de ses prestations ne pourrait être prononcée en l'absence de ce point de présence.

Le prestataire décrira et chiffrera également ses capacités à interconnecter son réseau avec le réseau fibre de l'opérateur de délégation de service public de la Métropole de Lyon : interconnexion fibre directe, interconnexion gix, etc.
Il chiffrera la prestation éventuelle de raccordement.
Le prestataire peut proposer des prestations complémentaires dans le BPU du marché.

4 DISPONIBILITE GLOBALE

4.1 Gestion globale de la disponibilité (SLA - Service Level Agreement)

Le candidat devra préciser :

- Le pourcentage de disponibilité constaté depuis 5 ans ;
- Le pourcentage de disponibilité globale qu'il garantit.
- S'il met à disposition un service d'alerte en cas de défaillance du niveau de service. Si oui, il précisera comment sont reçues ces alertes (Intranet, Email, Téléphone, Autre(s))
- La procédure suivie en cas d'alerte.
- Le délai moyen d'intervention sur un dysfonctionnement.
- Comment sont gérés les alertes au cours des Heures Non-Ouvrées / Jours Non-Ouvrés.

4.2 Pénalités

Des pénalités seront associées au niveau de service. Elles seront appliquées par le SITIV dès que le taux de disponibilité ne sera pas respecté, c'est-à-dire dès que les arrêts cumulés seront supérieurs à 1,6 heures / an.
Les pénalités seront calculées en multipliant le nombre d'heures d'indisponibilité par un taux de 300 € / heure.

4.3 Plan de Reprise d'Activité (PRA) et plan de continuité d'activité

Pour ce qui concerne la livraison et l'acheminement du trafic internet sur les différents sites d'exploitation, le candidat devra préciser et chiffrer le dispositif qu'il propose pour assurer la continuité d'acheminement du trafic sur l'ensemble des sites de production même en cas de défaillance des équipements d'un des deux sites.

Dans le but d'évolution vers un troisième/quatrième site de production raccordé aux deux sites principaux, le SITIV souhaite connaitre la capacité du candidat à mettre à disposition des baies et une interconnexion de faible latence dans un troisième / quatrième site.

5 MISE EN OEUVRE / DEPLOIEMENT

Le candidat précisera quelles sont les étapes suivies lors du déploiement de l'infrastructure. En particulier, il indiquera s'il propose un interlocuteur dédié ou tout autre moyen d'information sur l'état d'avancement lors de cette phase d'installation. Il précisera également si des documents sont transmis pendant et à l'issue de la phase de déploiement :

- Planning
- Cahier technique
- PV de recette
- Procédure de contact et d'escalade
- Procédures techniques
- Autre(s)

Le candidat précisera également sous combien de temps il peut mettre en œuvre la plateforme proposée et, si nécessaire, comment se déroule la mise en production de l'infrastructure de l'acheteur public et la transition vers la phase d'exploitation.
La mise en œuvre de l'infrastructure d'hébergement devra être lancée dès la notification du marché et du premier bon de commande et livrée au plus tard le 1er août 2023, tout dépassement de ce délai donnera lieu à une pénalité de 300 € par jour calendaire.

Le candidat chiffrera les services suivants :

- Mise en œuvre de liens optiques et/ou cuivres entre la meet me room et la baie du SITIV, entre 2 baies du SITIV
- Mise à disposition d'une salle de travail équipée pour permettre aux équipes du SITIV de travailler et ponctuellement localement sur ses infrastructures
- Réception et stockage temporaire de matériels SITIV à installer dans la baie
- Divers gestes de proximité
- Mise à disposition d'un lien fibre intersites de 10G

6 RESPECT DES REFERENTIELS

En tant que personne publique, les dispositifs livrés devront être conformes en tous points avec :

- Référentiel Général de Sécurité (RGS) dans sa version actuelle
- Règlement Général sur la Protection des Données
- Recommandation de l'Agence nationale de la sécurité des systèmes d'informations (ANSSI)
  - Ex : les 42 règles de sécurité simple éditées dans le guide d'hygiène informatique – éditions 2017 et à venir de l'ANSSI
- Référentiel Général d'Accessibilité des Administrations (R.G.A.A) dans leur version actuelle, **le cas échéant**.
- La Politique de sécurité du système d'information du SITIV (PSSI)

Le candidat précisera toute information qui lui paraitra pertinente sur ces sujets.

6.1 R.G.S. – Règlement Général de Sécurité

Suite au décret numéro 2010-112 du 02 février 2010 et de l'arrêté RGS publié au Journal Officiel le 18 mai 2010, l'application doit respecter les contraintes imposées par le référentiel général de sécurité (RGS) étendu aux utilisateurs des collectivités.

Ce respect doit s'appliquer tant à l'accès à l'application qu'au stockage des données. Le candidat décrira de façon détaillée les dispositifs qu'il a mis en œuvre pour respecter ces contraintes et notamment, sa capacité à anonymiser/détruire/archiver/crypter des données personnelles et à tenir compte dans ses versions du cycle de mise à jour des composants de base de l'application (versions de java, de php, etc)

Une procédure d'homologation RGS sera réalisée par le SITIV. À la suite des conclusions rendues par la commission d'homologation du SITIV, le candidat devra se mettre en conformité. A minima, les critères précédents seront vérifiés.

Pour obtenir des informations plus poussées sur la sécurité des systèmes d'information, le candidat peut consulter le site de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

6.2 R.G.P.D. – Règlement général sur la Protection des Données

De plus le prestataire devra fournir toutes les informations utiles et prendre en compte dans son produit le Règlement général sur la protection des données (RGPD).

En effet le nouveau règlement européen sur la protection des données a été définitivement adopté par le Parlement européen le 14 avril 2016. Ses dispositions seront directement applicables dans l'ensemble des 28 États membres de l'Union Européenne à compter du 25 mai 2018. Le logiciel devra prévoir :

· Un consentement « explicite » et « positif » de la part des citoyens.

· Le droit à l'effacement (version allégée du droit à l'oubli) : la personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais pour 6 motifs (article 17).

· Le droit à la portabilité des données personnelles : les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement.

· Profilage : toute personne a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire (article 22 du Règlement).

· Des principes de « protection des données dès la conception » et de « sécurité par défaut » : le règlement européen définit le principe de « protection des données dès la conception » qui impose aux organisations de prendre en compte des exigences relatives à la protection des données personnelles dès la conception des produits, services et systèmes exploitant des données à caractère personnel. De plus, le règlement consacre la nouvelle règle de la « sécurité par défaut » qui impose à toute organisation de disposer d'un système d'information sécurisé (article 25 du Règlement).

· Des notifications en cas de fuite de données. L'importance des sanctions oblige les collectivités à de la prudence : le règlement donne aux régulateurs le pouvoir d'infliger des sanctions financières allant jusqu'à 4 % du chiffre d'affaires mondial annuel d'une entreprise ou 20 millions d'euros (le montant le plus élevé étant retenu), en cas de non-respect (article 83.6 du Règlement).

6.3 R.G.A.A – Référentiel Général d'Accessibilité pour les Administrations

Le prestataire devra prendre en compte et s'assurer du respect de l'ensemble du référentiel tel que décrit dans les documents officiels comme le Référentiel Général d'Accessibilité pour les Administrations (RGAA) dans sa version courante.

La prise en compte des normes d'accessibilité en vigueur : W3C et niveau AA minimum des exigences d'accessibilité RGAA est obligatoire.

Le titulaire en tant que maitre d'œuvre a le droit d'alerter la maitrise d'ouvrage si elle détecte des contraintes techniques insurmontables pour l'accessibilité ou nécessitant des compromis dans la conception ou les choix opérés.

Le référentiel général d'accessibilité pour les administrations repose sur les 4 grands principes d'un site internet ou intranet accessible :

- Un site perceptible
- Un site utilisable
- Un site compréhensible
- Un site robuste

Toutes les informations de référence sont disponibles sur le site http://references.modernisation.gouv.fr/accessibilite-numerique

6.4 P.S.S.I. – Politique de sécurité du système d'information (SITIV)

Conformément à la PSSI mutualisée avec les villes adhérentes du SITIV, la confidentialité et l'intégrité des flux en interaction avec les systèmes d'information du SITIV doivent respectés les conditions de sécurités suivantes :

Tous les flux d'administration doivent être chiffrés par des procédés fiables (SSH, SSL, Ipsec,etc.), garantissant la confidentialité et l'intégrité des données. De façon générale, tous les flux contenant des informations sensibles et circulant sur un réseau public doivent être chiffrés par des procédés apportant ces mêmes garanties. Le choix et le dimensionnement des algorithmes cryptographiques doivent être effectués conformément aux règles et recommandations du RGS en la matière. Le titulaire indiquera l'ensemble des mécanismes et mesures mis en œuvre pour garantir la confidentialité et l'intégrité des flux d'administration. (cf Annexe 1 : PSSI) ;

Le cahier des clauses simplifiées de cybersécurité (annexe 2) relatif à l'article 2 du CCAP encadre la PSSI.