REPONSES AU QUESTIONS DES SOUMISSIONNAIRES

Bonjour Messieurs /Dames

Merci pour l'intérêt que vous portez à l'appel d'offres de l'ARCEP N° 009/ARCEP/PRMP/2024. Veuillez trouver ci-dessous des éclaircissements à vos préoccupations.

Les réponses aux questions posées sont en bleu.

1- Conflit entre Lot 1 et Lot 2 dans les résultats attendus du Lot 2. Il est mentionné un point qui relève des travaux du Lot 1. Qui est responsable de l'architecture du système : Lot 1 ou Lot 2 ?
Les services réseau et le portail sont déployés et disponibles en IPv4 et IPv6.
Un HLD (High-Level Design) et un LLD (Low-Level Design) détaillés du système et des services déployés. Ces documents doivent mettre en évidence l'architecture du système et des services du registre, l'organisation de chaque composante de cette architecture (physique et logique), les interactions entre les composants du réseau virtuel à bâtir (hôtes, VM, vSwitchs, etc.), ainsi que les interconnexions avec le réseau physique et le réseau de stockage."

Réponse 1 :

Il n'y a pas de conflit entre les missions dévolues aux Lots 1 et 2, mais simplement une nécessité de coordination des actions entre les deux lots. La séparation des fonctions est claire et se résume comme suit :

- *L'architecture du système est sous la responsabilité de l'adjudicataire du Lot 1. Les grandes lignes et les principes de mise en œuvre de cette architecture sont donnés au paragraphe 4.1.2 du DAO. Dans cette architecture, la mise en œuvre du réseau local (interconnexion des serveurs virtuels, des serveurs physiques et du stockage) est sous la responsabilité du Lot 1.*

- *Le Lot 2 s'occupe de la visibilité extérieure des services (adressage public) conformément aux directives du paragraphe 4.2.1.*

- *Le service compétent de l'ARCEP en charge de la mise en œuvre du projet coordonnera les tâches afférentes à chaque partie afin d'éviter tout double emploi*

2- résultats attendus lot1

Les résultats attendus du Lot 1 semblent indiquer que ce dernier est responsable du projet... Le Lot 1 devrait-il assurer le suivi du projet global ?

=== **Page 74, 4.1.4**
4.1.4. Résultats attendus
À l'issue de la mission, la nouvelle plateforme de services du ccTLD national ainsi que le site de repli .TG doivent être opérationnels conformément aux spécifications définies.

- La migration des données de l'ancienne plateforme vers la nouvelle doit être effective, et les nouveaux DNS doivent être renseignés dans le registre de l'ICANN.
- La gestion du registre s'effectue grâce au nouveau SRS déployé.
- La zone .TG ainsi que les enregistrements sont signés.
- Les services offerts par le ccTLD .TG sont disponibles en IPv4 et IPv6.
- Les mécanismes de reprise d'activités en cas de sinistres sont mis en place et testés.
- Le soumissionnaire doit remettre à l'Autorité de régulation un rapport de mission détaillé présentant les architectures systèmes, réseau et services mises en œuvre.
- Le renforcement des capacités des administrateurs du registre ainsi que des registrars est réalisé

======

Réponse 2:
Les résultats attendus, tels qu'ils sont listés à ce niveau, correspondent en réalité aux résultats attendus du projet global et non spécifiquement à ceux du Lot 1. Les résultats attendus pour le Lot 1 se limitent aux éléments suivants, tandis que les autres points dépassent les attributions du Lot 1 :

- *La livraison des équipements de la plateforme conformément aux spécifications de l'annexe A ;*
- *Le déploiement de la plateforme et la création des machines virtuelles conformément aux dispositions de l'annexe B ;*
- *La mise à disposition du HLD (High-Level Design) et du LLD (Low-Level Design) pour le système et le réseau local (virtuel et physique) déployé ;*
- *Le renforcement des capacités des ingénieurs de l'ARCEP en matière de virtualisation ;*
- *La remise d'un rapport de mission détaillé présentant, point par point, toutes les activités réalisées.*

3- Routeur et pare-feu

Il est prévu un routeur et un pare-feu. Un de chaque pour un système qui se veut hyper redondant ?

***Réponse 3**:*
La redondance sera garantie, car l'ARCEP dispose en réserve de routeurs et de pare-feux aux mêmes caractéristiques, qui pourront être mis à disposition en cas de besoin.

4- Déploiement des équipements réseaux

Le lot 1 fournit le matériel y compris le pare-feu et le routeur que le lot 2 doit installer. Rien

n'est dit sur les compétences nécessaires au niveau de lot2 pour installer et déployer ces équipements.

Réponse 4:

a. *Les mécanismes de passation des marchés publics ne nous autorisent pas à fournir des indications permettant aux soumissionnaires de déterminer les marques des équipements à déployer. Cependant, si un soumissionnaire ne dispose pas des compétences nécessaires pour configurer ces équipements réseau et de sécurité, il a toujours la possibilité de faire appel aux services d'un tiers compétent de son choix.*

Si le consultant lot2 ne maitrise pas ces équipements, comment se fera la répartition des tâches entre lot1 et lot2 ?

b. *Maitrise des configurations*

L'adjudicataire du Lot 1 met à disposition les équipements conformément aux spécifications techniques définies dans l'annexe A, et rien de plus.

L'adjudicataire du Lot 2 sera chargé de la configuration de ces équipements :

- ***Pour le pare-feu** : une matrice de flux de sécurité, qui lui sera transmise, fera l'objet d'une analyse consensuelle avec l'autorité contractante avant sa mise en œuvre.*
- ***Pour le routeur** : des règles d'interconnexion et de peering seront étudiées conjointement par l'adjudicataire du Lot 2 et l'autorité contractante.*

L'adjudicataire du Lot 2 devra, si nécessaire, acquérir les compétences requises pour la configuration desdits équipements

5- Service DNS du .TG

En ce qui concerne les services DNS (lot2). Rien n'est dit sur l'existant et les améliorations souhaitées. Quelle couverture géographique et réseau pour le service DNS du .tg? Le TG a en ce moment, la configuration DNS suivante:

;;		ANSWER		SECTION
tg.	21600	IN	NS	ns4.admin.net
tg.	21600	IN	NS	ns2.admin.net
tg.	21600	IN	NS	ns1.nic.tg
tg.	21600	IN	NS	ns1.admin.net
tg.	21600	IN	NS	tld.cafe.tg
tg.	21600	IN	NS	ns5.admin.net
tg.	21600	IN	NS	ns3.admin.net
tg.	21600	IN	NS	ns2.nic.tg

Qui couvre les systèmes autonomes suivants : 14061, 16276, 24691, 30982, 36864, 136557
La liste des machines à la page 73 indique : 2 Hidden Masters et 3 serveurs autoritaires : les 3 serveurs autoritaires seront déployés sur le réseau du registre ?

Réponse 5:

L'objectif de la plateforme en projet est de remplacer, à terme, l'actuelle plateforme de gestion du .TG. La migration des serveurs autoritaires est attribuée au Lot 3.
Toute action nécessitant des interactions entre les parties prenantes, notamment les adjudicataires des Lots 1, 2 et 3, sera effectuée sous la supervision de l'autorité contractante, qui analysera et coordonnera ces interactions.

6-SIEM
Lot 2 doit déployer un SIEM dont les spécifications et l'acquisition ne sont pas définies.

Réponse : Dernière ligne du tableau de l'annexe C. D'autre détails sont complétés à la ligne 4 du tableau « erratum sur les spécifications techniques de l'annexe A», joint au présent document.

7- Site web du registre

Aucune spécification du site désiré, ainsi qu'aucune mention des améliorations désirées par rapport à l'existant : https://www.nic.tg

Réponse 7 *:*

« Le DAO indique qu'un nouveau portail web sera développé pour le NIC.TG. Ce portail permettra de décrire le registre TG et ses activités, ainsi que de référencer tous les services disponibles. Des termes de référence spécifiques seront mis à la disposition du soumissionnaire pour le déploiement de ce portail. »

Il est prévu de repenser entièrement l'apparence et l'ergonomie (« look and feel ») du portail actuel tout en actualisant les informations disponibles sur le site www.nic.tg*. Ce nouveau portail deviendra le point d'entrée principal pour les services offerts par le registre « .tg ». Parmi ces services figurent le site web, les fonctionnalités WHOIS/RDAP, les plateformes pour les registrars, les statistiques sur les noms de domaine du registre, et bien d'autres. Le développement de ce nouveau portail sera réalisé de manière indépendante par rapport au site web existant.*

Les soumissionnaires doivent présenter une proposition détaillée des services et des développements qu'ils envisagent de réaliser. Afin de permettre une évaluation précise de la pertinence des coûts indiqués, ils doivent veiller à être aussi explicites que possible dans leurs offres, en identifiant clairement chaque élément de coût et en fournissant des explications pour chacun d'eux.

8- Connexion au IXP
Le .TG n'est pas en moment membre du TGIX. Qui prend en charge les frais? https://www.peeringdb.com/ix/2388

- Qui paiera les frais de d'adhésion, de membre et de port au IXP pour le .TG?
- Qui fournira le routeur du .TG au niveau de l'IXP ?
- Qui paiera pour la liaison .TG/IXP

Réponse 8 :

Il s'agit d'une procédure administrative qui sera conduite par l'autorité contractante, en collaboration avec l'adjudicataire du Lot 2, auprès de l'Agence en charge de la gestion des infrastructures numériques nationales (SIN) responsable de la gestion de l'IXP, afin d'inscrire le ccTLD comme membre du TGIX.

Les frais d'adhésion, d'interconnexion et la première cotisation annuelle seront entièrement à la charge de l'adjudicataire du Lot 2.

Le routeur de transit du ccTLD sera utilisé depuis son NOC pour l'interconnexion à l'IXP. Le cas échéant, l'autorité contractante mettra à disposition un routeur au ccTLD à l'IXP.

9- Transit IP

- Quelle bande passe requise pour chacun des transits IP ?
- Qui paiera pour les Liaisons Internet vers les deux upstreams de transit IP ?

Réponse 9:

- *Pour le transit IP, une capacité de 10 Mbps est suffisante au niveau des upstreams, tandis qu'une capacité de 100 Mbps sera requise à l'IXP ;*

- *L'adjudicataire paiera les liaisons pour la première année d'utilisation.*

10- Frais AFRINIC

C'est compris que les frais AFRINIC sont à la charge du lot2. Combien d'années doivent être prises en charge ?

Réponse 10 *:*

L'adjudicataire du lot2 prend en charge les frais d'AFRINIC pour la première année

11- Pour le SRS

- Rien n'est dit sur le type de base de données utilisée par l'existant, ni sur la structure des données pour l'évaluation de la migration de la base de données et des données.

- idem pour les relations registry-registrars existantes qui devront être migrées vers le nouveau SRS

Réponse 11 *:*

- ***Pour la base de données*** *: Il s'agit d'une base de données PostgreSQL. La structure de cette base de données ne pourra être communiquée qu'après la signature d'un NDA avec le*

demandeur. En cas d'adjudication, toutes les informations nécessaires pour la migration vers la nouvelle base de données seront mises à disposition de l'adjudicataire ;

Les données des relations entre le registre et les registraires existants sont stockées dans la même base de données. Leur migration fait partie intégrante du processus de migration de la base de données.

Question 12 :
A la page 66, dans le tableau « 1. Liste des Fournitures et calendrier de livraison » il est mentionné logiciel de virtualisation pour 32 cœurs alors que nous avons deux serveurs avec 32 cœurs chacun. Devrions nous considérer 64 cœurs pour couvrir les deux serveurs ?

*Réponse 12 : **Le nombre de licences est mentionné dans l'annexe A (ligne 4) et s'élève à 56**. Cette valeur est liée au nombre de cœurs par serveur, qui peut varier entre 16 et 32. Dans ce cas-ci, une légère majoration a été appliquée afin de constituer un stock de réserve. Par ailleurs, la valeur indiquée à la page 66 est erronée et ne correspond pas à la réalité.*

Question 13 :
@ A la page 93, dans le tableau « Annexe A » il est mentionné 'Souscription et support à la dernière version de Vmware vSphere Enterprise Plus pour 3 ans Qté: 56 alors que nous avons deux serveurs avec 32 cœurs chacun. Devrions nous considérer 64 cœurs pour couvrir les deux serveurs ?

Réponse 13 : voir la réponse à la question 12

Question 14 :
@ Nous comprenons par services, que les équipements livrés seront installés et mises en exploitation selon la norme sur le site de production, vous pouvez confirmer svp ?

Réponse 14 :
Les services se réfèrent :

- ***Pour le lot 1** : à la construction de la plateforme, conformément aux exigences du paragraphe **4.1.2** du DAO ;*
- ***Pour le lot 2** : au déploiement du réseau ISP (architecture des réseaux et sécurité), conformément aux directives des paragraphes **4.2.1 et 4.2.2 du DAO** ;*
- ***Pour le lot 3** : au déploiement du SRS et à la migration des bases de données de l'ancienne plateforme vers la nouvelle, conformément aux directives des paragraphes **4.3.1 à 4.3.4 du DAO**.*

Question 15 :
@ Formation et transfert de compétences : devrions nous proposer des formations dans des centres agrées sur le logiciel de virtualisation uniquement ?

Réponse 15 :
L'objectif de cette exigence est de s'assurer que le centre de formation sélectionné dispose des accréditations requises ainsi que de la logistique nécessaire pour offrir une formation de qualité sur

le logiciel de virtualisation choisi. Par ailleurs, si le centre est agréé par d'autres éditeurs, cela constituerait un atout supplémentaire.

REPUBLIQUE TOGOLAISE
Travail - Liberté - Patrie

arcep
autorité de régulation des communications électroniques et des postes

REPONSES AU QUESTIONS DES SOUMISSIONNAIRES

Erratum sur les caractéristiques techniques de l'annexe A :

	Spéficiations techniques demandées	Quantité	Spéficiations techniques proposées	Quantité
1	**MacBoock**			
	Ecran: Liquid Retina XDR display 14.2 inch. Résolution native de 3024 x 1964 pixels à 254 pixels par pouce. **Finition**: Space Black **Processeur:** M4 Max with 16-core CPU **Mémoire**: 48 Go de mémoire unifiée, configurable à 64 Go ou 128 Go **Disque dur**: 2TB **Adaptateur secteur :** USB-C 96W **Clavier:** Backlit Magic Keyboard avec Touch ID français AZERTY FR **Sans fils:** - Wi-Fi 6E (802.11ax) - Bluetooth 5.3 **Système d'exploitation** : dernière version de **macOS** **Camera :** Caméra Center Stage de 12 MP avec prise en charge de Desk View, Enregistrement vidéo HD 1080p. Processeur de signal d'image avancé avec vidéo computationnelle. **Sacoche:** Bellroy Caddy for 13" and 14" Mac Laptops	2		

	Protection: Incase Hardshell Case for MacBook Pro 14", Color - Black **MS Officice:** Licence Microsoft Office Home & Business 2024 **Autres accessoires :** - USB-C to SD Card Reader - Satechi Multiport Pro Adapter V2 (with Ethernet)			
2	**Licences de virtualisation :**			
	Souscription et support à la dernière version de Vmware vSphere Enterprise Plus pour 3 ans	56		
3	**Pare -feu (Firewall) suite :**			
	Licence Advanced Malware Prevention (AMP) pour 3 ans	3		
4	**SIEM**			
	1. Architecture - Le SIEM doit être basé sur Elasticsearch pour l'indexation et l'analyse des données de sécurité en temps réel. - Capacité à gérer des volumes élevés de données (logs, événements) avec une scalabilité horizontale. - Indexation en temps réel pour permettre des recherches rapides sur de grandes quantités de données. **2. Visualisation des données** - Utilisation de Kibana pour la visualisation et la création de tableaux de bord interactifs et personnalisés. - Tableau de bord de surveillance pour l'analyse des incidents et des alertes. - Vue centralisée des données pour faciliter la gestion des incidents. - 3. Ingestion des données - Logstash ou Beats pour l'ingestion de données depuis des sources multiples (serveurs, applications, équipements réseau, etc.). - Support de l'enrichissement des données avec des informations supplémentaires pour mieux contextualiser les alertes.	1		

	- **4. de Détection et Analyse** **Moteur de détection des menaces :** - Détection avancée des menaces via des règles et l'usage d'algorithmes d'apprentissage automatique. - Prise en charge de l'analyse comportementale et de l'identification des anomalies. - Capacité à définir des règles de détection personnalisées en fonction des besoins spécifiques de sécurité. **Règles de détection :** - Possibilité d'ajouter, personnaliser et modifier des règles de détection pour s'adapter à l'évolution des menaces. - Intégration de règles de détection standards (ex. MITRE ATT&CK, Elastic Common Schema - ECS). - **Analyse des incidents :** - Capacité à analyser les incidents et corréler les événements provenant de multiples sources pour identifier les menaces potentielles. - Intégration d'une gestion d'incidents et d'alertes avec des flux de travail automatisés. **5. Intégration et Extensibilité** **API et intégrations :** - Le système doit offrir des API RESTful pour une intégration fluide avec d'autres outils de sécurité (gestion des vulnérabilités, analyse des malwares, etc.). - Capacité à intégrer des sources de données externes (comme des systèmes SIEM tiers, des outils de ticketing, des solutions de réponse aux incidents). **Connecteurs et plugins :** - Des connecteurs natifs pour des sources de données populaires (pare-feu, serveurs, systèmes de gestion des identités, équipements réseau). - Possibilité de créer et de déployer des plugins personnalisés. **6. Sécurité et Contrôle d'Accès**			

	Contrôle d'accès basé sur les rôles (RBAC) : - Gestion granulaire des droits d'accès avec des rôles définis (administrateurs, analystes, utilisateurs). - Prise en charge de l'audit des actions des utilisateurs pour des fins de traçabilité et de conformité. **Chiffrement des données :** Chiffrement des données au repos et en transit pour garantir la confidentialité et l'intégrité des données collectées. **Authentification :** Support de l'authentification unique (SSO), de l'authentification multifacteur (MFA) et de l'authentification via des systèmes externes (ex. LDAP, Active Directory). **7. Performances et Scalabilité** **Scalabilité horizontale :** Capacité à évoluer horizontalement en fonction de la croissance des données et des exigences de l'organisation. **Haute disponibilité et tolérance aux pannes :** Déploiement en cluster pour garantir la disponibilité continue des services SIEM et la résilience face aux pannes. **Optimisation des performances :** Optimisation des requêtes et des processus de recherche pour minimiser les latences dans les environnements à fort trafic. **8. Gestion des Données et Reporting** **Collecte de données :** - Collecte de données en temps réel depuis les systèmes, applications, équipements réseau, serveurs, etc. - Support des formats de logs standards (Syslog, CEF, JSON, etc.). **Rapports et alertes :** - Génération de rapports personnalisables sur les incidents, les menaces détectées, les tendances de sécurité, et la conformité.			

	- Alertes en temps réel via des notifications par email, SMS, ou intégration avec d'autres outils de gestion des incidents. **9. Déploiement et Maintenance** **Options de déploiement :** - Le SIEM doit être déployable en mode cloud, sur site ou dans un environnement hybride. - Support des environnements multi-cloud et déploiement dans des infrastructures conteneurisées (Kubernetes, Docker). **Maintenance et mise à jour :** - Processus de mise à jour régulière pour intégrer les dernières fonctionnalités et les patches de sécurité. - Documentation détaillée pour l'installation, la configuration et la maintenance du système. **10. Conformité et Réglementations** **Conformité aux normes :** - Le SIEM doit permettre la conformité avec les principales normes de sécurité et de confidentialité (ex. ISO 27001, GDPR, PCI DSS, NIST). **Archivage et rétention des données :** - Capacités d'archivage des données pour respecter les exigences de rétention à long terme et les politiques de gestion des logs			