AVIS N°2

PUBLICATION DES REPONSES AUX QUESTIONS FORMULEES DANS LE CADRE DE L'APPEL D'OFFRES AO/ZOO/DBA/021/2020 POUR LA FOURNITURE ET LE DÉPLOIEMENT D'OUTILS QRADAR ET GUARDIUM POUR L'EXTENSION DU PÉRIMÈTRE DE SUPERVISION DU SYSTÈME D'INFORMATION DE LA BCEAO

Question 1 : Guardium

Est ce que les services suivants sont inclus? ou bien il s'agit juste de l'installation des nouvelles composantes et leurs intégrations avec l'existant :

- Installation des agents sur les 10 serveurs BDD et les configurations relatives (datasources, failover....)?
- Implémentation des scénarios de découverte et classification des données sensibles sur les nouvelles BDD ajoutées? ou bien l'optimisation des scénarios de découverte existants?
- Conception est implémentation des scénarios de supervision relatives aux nouvelles BDD (supervision d'accès aux bdd, supervision d'accès aux données sensible, sql injection, masquage des données sensibles...)? ou bien l'optimisation des scénarios de supervision et protection existants?
- Création des tableaux de bord et rapports relatives aux activités des nouvelles BDD? ou bien l'optimisation des rapports et tableaux de bord existants?

Réponse question 1

Tous les services énoncés sont inclus.

Question 2 : Guardium

prière de clarifier les points suivants relatifs à l'architecture Guardium Cible (le schéma du CDC indique qu'il s'agit du site principale):

- Collecteurs: l'ensemble des collecteurs existants dans le site principale est 4 (3 physique et 1 virtuelle), le CDC demande l'acquisition de 2 collecteurs virtuels, pourquoi l'architecture cible du site affiche 8 collecteurs? A noter que chaque instance collecteur nécessite une licence.

Réponse question 2

Le collecteur virtuel existant sera décommissionné à la fin de l'installation des nouveaux collecteurs. Donc il y aura un collecteur virtuel au niveau de chaque site en plus des 3

collecteurs physiques existants. Cela justifie les 8 collecteurs sur les 2 sites agrégés.

Question 3 : Guardium

Agrégateurs: l'ensemble des agrégateurs existants dans le site principale est 1 (qui joue aussi le rôle du CM), le CDC demande l'acquisition de 1 agrégateurs, pourquoi l'architecture cible du site affiche 4 agrégateurs (dont deux joueront le rôle d'un CM dédié et son CM de secours)?, prière de noter que chaque instance d'agrégateur nécessite un licence quelque soit son rôle (agrégateur, CM dédié, CM de secours, agrégateur/CM). aussi le problème du nombre des collecteurs et agrégateurs se pose même si l'architecture cible affichée dans le CDC représente l'architecture des deux site (avec un changement du nombre).

Réponse question 3 : Quardium

Ce module n'est pas mentionné dans le dossier d'appel d'offres. Toutefois, les soumissionnaires peuvent la proposer en option en prenant le soin d'argumenter le besoin.

Question 4 : Qradar

Est ce que les services suivants sont inclus? ou bien il s'agit juste de l'installation des nouvelles composantes et leurs intégrations avec l'existant :

- Intégration/ré-intégration des nouvelles sources de log? si oui, prière de citer le nombre?

Réponse question 4

Le nombre de nouvelles sources de logs à intégrer est environ 200.

Question 5 : Qradar

- Création des connecteurs personnalisés pour des sources de logs non supportées nativement?, si oui, prière d'indiquer le nombre des sources?
- Conception et implémentation/optimisation des scénarios de supervision sous forme de règles de corrélation personnalisées?, si oui, indiquer le nombre souhaités?
- Création/optimisation des tableaux de bord et rapports?

Réponse question 5

Tous les services énoncés sont inclus.

Question 6

Les corrections des problèmes constatés sur les deux plateformes existantes avant l'entame des travaux relatifs à l'extension sont-ils à considérer ?

Réponse question 6

Oui

NB :

- Le point II.5 du CDC mention un point très important sur la suppression des événements, il faut noter à ce stade que la solution Qradar met les événements dans une file d'attente en cas de dépassement de la licence, cette file à une taille de 5 Go (il existe une file d'attente pour chaque protocole de collection: Syslog, JDBC...), cela veut dire que dans une situation de pic d'événement contenu qui dépasse la capacité de la licence (comme dans le cas d'un mauvais dimensionnement), la file d'attente sera remplis et dans ce cas, Qradar dropera des événements.

- Le déploiement d'un HA pour le processeur d'événements nécessite une licence, donc il doit être proposé en option.

Les caractéristiques et fonctionnalités décrites dans le cahier des charges sont minimales. Si les soumissionnaires jugent nécessaire de proposer des améliorations, ils peuvent le faire sous forme d'offres optionnelles en prenant le soin de les argumenter et de les chiffrer.

Question 7
Est-ce que la mise à jour des systèmes existant QRadar & Guardium devrait être inclus?

Réponse question 7

Oui. Les systèmes existants doivent avoir la même version de logiciel que les nouveaux systèmes déployés.

Question 8

Communication de la liste complète détaillée des nouveaux équipements à intégrer dans QRadar dans le cadre de l'extension de la License EPS (5,000)

Réponse question 8

Le Système d'Information de la BCEAO repose essentiellement sur des outils et technologies

ci-après :

- Bases de données : Oracle, SQL Server, Mysql ;
- Serveurs d'applications JEE : Tomcat, Jboss, Glassfish et Oracle Applications Server ;
- Systèmes d'exploitation : Linux et Windows Server ;
- Systèmes de messagerie : Google Suite ;
- Infrastructure de stockage et de sauvegarde : EMC VNX, EMC DATADOMAIN, EMC AVAMAR et EMC NETWORKER ;
- Outils de virtualisation : VMWare (vSphere, vCenter) ;
- Réseaux : commutateurs, routeurs, pare-feux, points d'accès VPN, IPS ;
- Outils de traçabilité : IBM Guardium et IBM QRADAR.

Le nombre de sources de logs à intégrer est environ 200.

Question 9

Est-ce que le développement de Scenario de Sécurité "Use Cases" devrait être inclus? Si oui, combien de uses cases ?

Réponse question 9

Cette prestation n'est pas prévue dans le cahier de charges. Toutefois le soumissionnaire pourrait faire une proposition optionnelle en prenant le soin de l'argumenter et de la chiffrer.

Question 10

La clause I.27 demande une Guarantie de 3 ans sur le matériel? Est-ce que le support du partenaire est aussi requis sur 3 ans?

Réponse question 10

Le contrat support sera renouvelé tous les ans.

Question 11

Communication de la liste détaillée des 10 Serveurs de Base de données à intégrer dans Guardium

Réponse question 11

Les bases de données ORACLE sont à la version 11.2.0.4 hébergées sur des Oracle Database Appliance X7-2-HA déployé en mode virtualisé ou bare metal avec une version de Oracle Database Appliance Software >= 12.2.1.3.0.

Les bases de données MySQL seront des versions supérieures ou égales 5.7.0 (enterprise) hébergées sur une Redhat Enterprise >=7.0.

Question 12

Est-ce que le développement des Polices de Sécurité pour les Base Données devrait être aussi inclus?

Réponse question 12

Cette prestation n'est pas prévue dans le cahier de charges. Toutefois le soumissionnaire pourrait faire une proposition optionnelle en prenant le soin de l'argumenter et de la chiffrer.

Question 13

Formation sur site ou virtuelle ? pour combien de ressources ?

Réponse question 13

En virtuelle si la situation sanitaire actuelle n'évolue pas dans le bon sens.

10 utilisateurs sont prévus pour la formation.