TILENCIA

GT

Administrateur expert Splunk

FORMATIONS & CERTIFICATIONS

2019-2020 : Master en Réseaux et Télécommunications, École Centrale de Lille, France

2016-2019 : Diplôme d'Ingénieur d'État en Télécommunications et Technologies de l'information, Institut National des Postes et Télécommunications (I.N.P.T), Maroc.

COMPÉTENCES

Traitement de données / Gestion des logs
- Splunk, SplunkJS, ELK

Outils de Versionning
- Git

Configuration des servers
- Dell
- HP Proliant

Systèmes d'exploitation
- Linux (Redhat, Centos, Debian, Fedora et Ubuntu)
- Windows

Automatisation
- Ansible
- Jenkins
- AWX Tower

Conteneurisation
- Docker

Virtualisation
- Vmware vsphere
- Virtualbox

Langage de programmation
- PYTHON, SHELL
- HTML, CSS, JAVASCRIPT

LANGUES

Anglais : courant

TILENCIA

EXPÉRIENCES

Société : **BNPP** **01/2023 à ce jour**

Poste : **Administrateur Splunk**

Déploiement et configuration de la plateforme Splunk, niveau expert, composants : Indexers, Search Heads, Deployment Server, Forwarders

- Déploiement et configuration du cluster des search head, du cluster Search Peers
- Déploiement et configuration du cluster Master, du Monitoring Console et du Deployment
- Installation, configuration et gestion des collecteurs (UF, HF) et DS
- Installation, configuration et gestion des instances HEC et Syslog
- Déploiement des applications de collecte et gestion de la plateforme Splunk

Administration de la plateforme Splunk, niveau expert

- Administration du cluster Search head, et du cluster d'indexeur
- Management de la plateforme Splunk (Cluster master, Deployment, DS)
- Monitoring de la plateforme Splunk via le Monitoring Console
- Installation, configuration et gestion des applications Splunk
- Gestion des licences Splunk et suivi de l'évolution de la volumétrie des données
- Optimisation de la capacité et la performance de l'infrastructure Splunk
- Création et suivi des incidents (cases) chez l'éditeur Splunk
- Troubleshooting des incidents au sein du réseau Splunk
- Troubleshooting des incidents de collecte et d'indexation de données
- Configuration et gestion de l'authentification centralisée Splunk via LDAP

Indexation des données

- Collecte, parsing et ingestion de données
- Intégration des nouvelles sources de données

- Création, modification ou suppression des index, de sourcetypes et KO
- Définition de la politique de rétention des données et de stockage nécessaire
- Filtration, anonymisation des données et extraction des champs
- Déploiement et update des applications de collecte des forwarders
- Collecte des données Syslog, HEC, et monitoring des fichiers et dossiers
- Développement des scripts (python et Shell) pour la collecte des données

Visualisation et analyse

- Développement de requêtes de recherche avancées et de tableaux de bord
- Création et planification des rapports et alertes
- Optimisation des requêtes Splunk
- Création et gestion des knowledge object
- Assistance aux équipes de développement pour l'intégration des journaux applicatifs dans Splunk
- Développement des Endpoint Splunk (fonctionnalités supplémentaire)

Gestion des rôles et comptes utilisateurs

- Création des rôles LDAP et comptes utilisateurs
- Traitement des incidents et demandes utilisateurs

Automatisation et configuration centralisée

- Déploiement automatisé de configuration via ansible

Société **EDF** **2021 à 2022**

Poste : **Administateur Splunk**

Administration de la plateforme Splunk, niveau expert

- Coordination, vérification et validation des activités de migration de l'infrastructure Splunk
- Administration de l'infrastructure Splunk
- Déploiement et gestion des forwarders
- Intégration bout à bout des nouvelles sources de données

- Collecte et parsing des données
- Création des tableaux de bord, des rapports de statistiques et des alertes
- Gestion des index, des sourcetypes et des knowledge object
- Ingestion des données et mise en place des requêtes SPL avancées
- Gestion des logs et backup des données

Automatisation des opérations du réseau via Ansible

- Gestion centralisée de l'infrastructure réseau via des playbook
- Déploiement, configuration et maintenance centralisés des applications
- Déploiement et configuration des applications Splunk
- Gestion de l'infrastructure Splunk avec Ansible
- Développement des playbooks de détection de vulnérabilité du réseau
- Développement et installation des modules Ansible

Scripting en python et Shell

- Développement des scripts pour le heath check du réseau LTE
- Développement des scripts de collecte et gestion des données
- Développement des scripts d'interconnexion CA -Spectrum et Splunk
- Scripts de loadbalacing des opérations du réseau

Encadrement et Accompagnement

- Assurer un support technique Splunk et Ansible aux équipes
- Accompagner la montée en compétences des équipes
- Rédaction de documentation

Société **ERICSSON** **01/2020 à 12/2021**

Poste : **Ingénieur réseaux**

- Déploiement et configuration des solutions OSS Ericsson
- Automatisation du déploiement des solutions OSS de Ericsson
- Configuration des fonctions du réseau coeur 4G
- Support à l'intégration des noeuds radio 3G, 4G et 5G.
- Intégration des noeuds avec les outils de surveillance Ericsson Network Manager.
- Participation aux tests de validation de l'OMC
- Validation des solutions de supervision et d'administration réseau de Ericsson

- Rédaction de la documentation