

Yacine Bachkat

066-744-4053

Bachkat@protonmail.com • <https://www.linkedin.com/in/yacine-bachkat-22bb18175>

Hussein Dey, Alger, Algeria

OBJECTIVE

En tant qu'administrateur système expérimenté, je suis compétent dans la gestion des serveurs Linux et Windows, la virtualisation, la containerisation et l'automatisation avec des outils tels qu'Ansible et Terraform. Mes compétences techniques incluent également les réseaux, le cloud computing et la sécurité informatique. Je m'efforce de garantir la fiabilité, la disponibilité et la sécurité des systèmes critiques, tout en travaillant en étroite collaboration avec les équipes de développement et les parties prenantes de l'entreprise pour fournir des solutions informatiques répondant à leurs besoins. Si vous recherchez un administrateur système compétent et fiable, je serais ravi de discuter de la façon dont je peux aider votre organisation à atteindre ses objectifs informatiques.

EDUCATION

Master sciences d'informatique

Sep 2018 - Aug 2020

université de constantine 2 • Constantine, Algeria

Un programme enseigne aux étudiants la théorie avancée et les applications de la technologie informatique. En plus de développer des compétences de raisonnement et de résolution de problèmes, les apprenants étudient l'architecture informatique, les derniers langages de programmation, le génie logiciel, les bases de données, l'administration des systèmes, la cybersécurité, l'intelligence artificielle, la conception d'algorithmes et le réseautage.

license computer science

Sep 2015 - Aug 2018

université de constantine 2 • Constantine, Algeria

Un programme de trois ans qui comprend l'étude des concepts et des théories informatiques, des fondements algorithmiques et des nouveaux développements en informatique.

SKILLS

- Expertise technique : Une solide compréhension des systèmes informatiques, des réseaux et des logiciels : je connais divers systèmes d'exploitation tels que Windows, Linux et macOS, et j'ai de l'expérience dans la configuration et le dépannage de matériel et de logiciels.
- Résolution de problèmes : pour identifier et résoudre les problèmes techniques. et la capacité de penser de manière critique et logique.
- Communication : compétences de communication efficaces, je suis capable de communiquer de manière claire et concise avec les utilisateurs techniques et non techniques, et capable de traduire le jargon technique en termes simples.
- Souci du détail : je suis capable d'être méticuleux et de porter une attention particulière aux détails pour m'assurer que les systèmes fonctionnent de manière optimale et que les problèmes potentiels sont détectés et résolus avant qu'ils ne deviennent critiques.
- Gestion du temps : La capacité de hiérarchiser les tâches et de gérer efficacement le temps.

Je suis capable d'équilibrer des demandes concurrentes et de respecter des délais serrés, tout en m'assurant que les systèmes fonctionnent au mieux.

- Sensibilisation à la sécurité : je suis conscient des risques de sécurité potentiels et je suis en mesure de prendre des mesures pour les atténuer. Cela comprend la mise en œuvre de protocoles de sécurité, l'exécution de sauvegardes régulières du système et la garantie que les comptes d'utilisateurs sont sécurisés.
- Apprentissage continu : La technologie évolue constamment, et je suis prêt à acquérir de nouvelles compétences et à rester au courant des dernières tendances et des meilleures pratiques dans le domaine.

WORK EXPERIENCE

Administrateur des systèmes informatiques

Jan 2022 - Apr 2023

Ministère de la Défense nationale • Oran, Algeria

- Installation et configuration de logiciels et de matériel : installation, configuration et maintenance de divers systèmes matériels et logiciels. Cela inclut les serveurs, les périphériques de stockage, les équipements réseau, les systèmes d'exploitation et les applications.
- Surveillance des performances du système : surveillez les performances du système, identifiez les problèmes potentiels et prenez des mesures correctives si nécessaire. utiliser divers outils pour surveiller les ressources système, telles que l'utilisation du processeur, l'utilisation de la mémoire et l'espace disque.
- Dépannage et résolution de problèmes : lorsque des problèmes techniques surviennent, identifier la cause première du problème et prendre des mesures correctives. Cela inclut le diagnostic des problèmes liés au matériel, aux logiciels et aux réseaux.
- Sécurité du système : assurez-vous que les systèmes sont sécurisés et protégés contre les accès non autorisés, les virus et autres menaces de sécurité. la mise en œuvre et l'application des politiques et procédures de sécurité, et la surveillance des failles de sécurité.
- Support utilisateur : le premier point de contact pour les utilisateurs qui rencontrent des problèmes techniques. fournir un support technique et des conseils aux utilisateurs et aider à résoudre tout problème.
- Sauvegarde et reprise après sinistre : s'assurer que les données sont sauvegardées régulièrement et que des plans de reprise après sinistre sont en place en cas de panne ou de sinistre inattendu.
- Documentation et rapports : conservez des enregistrements et une documentation précis des configurations, des modifications et des procédures du système. fournir des rapports réguliers sur les performances et l'état du système à la direction et aux autres parties prenantes.

Penetration Tester

Jul 2018 - Present

Bugcrowd -freelancer- • Mostaganem, Algeria

- Bug Bounty Hunting
- effectuer des tests et tenter délibérément d'exploiter les systèmes informatiques et logiciels existants pour détecter et corriger les faiblesses du système.

LANGUE

- Arabic - Langue maternelle
- English - conversationnelle
- French - conversationnelle

CERTIFICATIONS

- Fortinet Network Security Expert 1,2
- Cisco CCNA R&S
- Cisco CyberOps
- Cisco Cybersecurity Essentials
- Cisco IT Essentials
- Certified Network Security Specialist ICSI,UK
- Practical Ethical Hacker TCM Security
- Google IT support Specialist

COURSES

- Certified Information Systems Security Professional (CISSP)
- Certified Ethical Hacker (CEH)
- CompTIA Security+
- Offensive Security Certified Professional (OSCP)
- Certified Hacking Forensic Investigator (CHFI)
- CompTIA A+
- CompTIA Network+
- AWS Certified Solutions Architect

PROJECTS

- Projet de consolidation de serveurs pour "SarL LENA Algérie" : consolider plusieurs serveurs physiques en un plus petit nombre de serveurs virtuels afin de réduire les coûts de matériel, de simplifier l'administration du système et d'améliorer l'utilisation des serveurs en :
 - 1- Évaluation : Réalisation d'une évaluation de l'infrastructure existante afin d'identifier les serveurs qui pourraient être consolidés. Cela impliquait d'évaluer les spécifications matérielles, les logiciels installés et les niveaux d'utilisation de chaque serveur.
 - 2- Virtualisation : logiciel de virtualisation installé sur le serveur cible pour créer des machines virtuelles (VM) qui hébergeraient les applications consolidées.
 - 3- Migration d'applications : applications migrées des serveurs physiques vers les VM. Cela impliquait de configurer les machines virtuelles pour qu'elles correspondent aux spécifications matérielles et logicielles des serveurs d'origine.
 - 4- Migration des données : migration des données des serveurs physiques vers les VM. Cela

impliquait le transfert de données des périphériques de stockage existants vers les périphériques de stockage alloués aux machines virtuelles.

- 5- Tests : tests approfondis effectués pour s'assurer que les applications et les données fonctionnaient comme prévu sur les nouvelles machines virtuelles. Cela comprenait la vérification des performances du système, les tests de charge et la validation des procédures de sauvegarde et de restauration.
 - 6- Mise hors service : mise hors service des serveurs physiques qui n'étaient plus nécessaires et redirection du trafic vers les nouveaux serveurs virtuels.
-
- projet d'amélioration de la sécurité pour "SARL ALGERIA WAREHOUSE COMPANY" : renforcer la sécurité de l'infrastructure réseau d'une organisation afin de se protéger contre les cyberattaques et les violations de données en :
 - 1 - Contrôle d'accès : Mise en place de mesures de contrôle d'accès pour restreindre l'accès aux données et systèmes sensibles. Cela comprenait la mise en œuvre de mots de passe forts, d'une authentification à deux facteurs et d'un contrôle d'accès basé sur les rôles.
 - 2 - Segmentation du réseau : Segmentation du réseau en sous-réseaux plus petits pour limiter la portée des attaques potentielles. Cela impliquait la configuration de pare-feu et d'autres périphériques réseau pour limiter le trafic entre les sous-réseaux.
 - 3 - Chiffrement : chiffrement mis en œuvre pour protéger les données sensibles en transit et au repos. Cela comprenait la configuration des protocoles SSL/TLS pour le trafic Web, la mise en œuvre de VPN pour l'accès à distance et le chiffrement des données stockées sur les serveurs et les périphériques de stockage.
 - 4 - Surveillance de la sécurité : mise en place d'outils de surveillance de la sécurité pour détecter et répondre aux incidents de sécurité en temps réel. Cela comprenait la configuration des systèmes de détection et de prévention des intrusions, la configuration de la journalisation des événements de sécurité et la mise en œuvre d'un plan de réponse aux incidents de sécurité.
 - 5 - Formation et sensibilisation : Mené des programmes de formation et de sensibilisation pour éduquer les employés sur les meilleures pratiques de sécurité et pour promouvoir une culture de sécurité au sein de l'organisation.