Durée :	158 jours soit 1106 heures	Référence :	IF-MAST-38823

Public visé :

Cette formation en alternance s'adresse à toute personne titulaire d'un BTS et Bachelor dans le domaine de l'informatique ou d'un Bac+4/5 scientifique, technique, mathématique, etc.

Pré-requis :

Pour suivre cette formation, les apprenants doivent remplir les critères suivants :

- Être titulaire d'un BTS et d'un Bachelor en informatique ou d'un Bac+4/5 dans les domaines scientifiques, mathématiques ou techniques.
- Maîtriser les fondamentaux des réseaux TCP/IP.
- Avoir une bonne connaissance des environnements Windows Server et Linux.
- Maîtriser les environnements et architectures Cloud (AWS, Microsoft Azure, etc.).
- Posséder une maîtrise de l'anglais professionnel.
- Démontrer d'excellentes compétences relationnelles.
- Être capable de s'adapter et de communiquer efficacement avec divers interlocuteurs (clients, spécialistes techniques, etc.).
- Faire preuve d'aisance dans la communication.
- Avoir la capacité de travailler en équipe de manière collaborative.
- Démontrer d'excellentes compétences rédactionnelles.
- Avoir un réel intérêt pour l'informatique, avec une capacité d'auto-formation et une expérience concrète dans la réalisation de projets.

Objectifs pédagogiques :

Objectifs et contexte de la certification :

La certification "Expert en architectures systèmes, réseaux et sécurité informatique" , s'inscrivant dans le contexte dynamique des professions numériques, est conçue pour équiper les professionnels avec des compétences spécialisées répondant aux exigences croissantes du secteur de l'IT. Cette certification couvre un large éventail de rôles stratégiques tels que Architecte réseau informatique, Expert en cybersécurité, et Ingénieur système réseau informatique. Elle répond à une forte demande du marché.

L'objectif de cette certification est de former des experts capables de concevoir, gérer et sécuriser des architectures systèmes et réseaux complexes. Elle vise à développer une expertise approfondie dans les domaines de l'informatique, du traitement de l'information, ainsi que dans l'analyse informatique et la conception d'architecture de réseaux. Cela inclut une compréhension solide des systèmes informatiques, la capacité à gérer de grandes quantités de données, et la compétence pour développer des infrastructures réseau sécurisées et efficaces.

Cette certification assure que les professionnels sont équipés pour naviguer dans le paysage technologique en évolution, avec des compétences spécifiques en systèmes informatiques, en analyse de données, en architecture réseau et en cybersécurité.

Activités visées :

Planifier et organiser un projet d'architecture systèmes et réseaux / Organisation du projet systèmes et réseaux

- Analyse approfondie de l'architecture systèmes et réseaux existante
- Mise en place du plan de veille technologique et réglementaire des systèmes et réseaux informatiques
- Analyse de faisabilité du projet d'architecture informatique
- Description de la solution d'architecture informatique proposée à l'entreprise
- Élaboration du projet d'architecture informatique
- Mise en œuvre du projet d'architecture informatique
- Evaluation de la performance du projet d'architecture informatique
- Contrôle du projet d'architecture informatique

Développer des solutions d'infrastructure systèmes et réseaux / Construire la solution technique du projet de systèmes-réseaux et sécurité

- Élaboration de l'architecture informatique évolutive
- Mise en place de l'architecture informatique
- Maintenance du niveau de service optimal de l'infrastructure informatique
- Surveillance du bon fonctionnement de l'infrastructure informatique
- Pilotage de l'amélioration de la qualité du service informatique
- Evolution de l'architecture informatique
- Elaboration de la documentation technique

Piloter la sécurité de l'infrastructure informatique / Organiser la sécurité de l'infrastructure informatique

- Evaluation de la sécurité existante des systèmes et réseaux informatiques
- Mise en place du plan de veille de sécurité des systèmes et réseaux informatiques
- Construction de la politique de sécurité des systèmes et réseaux informatiques
- Implémentation des solutions de sécurité des systèmes et réseaux informatiques

- Détection des incidents de sécurité de l'infrastructure informatique
- Gestion des incidents de sécurité de l'infrastructure informatique
- Évolution de la politique et des solutions de sécurité de l'infrastructure informatique

Piloter l'équipe du projet d'architecture informatique / Management de l'équipe du projet d'architecture informatique

- Définition des besoins en compétences de l'équipe du projet d'architecture informatique
- Création de l'équipe du projet d'architecture informatique
- Gestion opérationnelle de l'équipe du projet d'architecture informatique
- Animation de l'équipe du projet d'architecture informatique
- Plan de formation de l'équipe du projet d'architecture informatique
- Suivi de la performance de l'équipe du projet d'architecture informatique

Préparation, passage et obtention du titre RNCP 38823 Expert en architectures systèmes, réseaux et sécurité informatique
Préparation, passage et obtention de 3 certifications officielles : AZ-305, AZ-500 et Terraform

Compétences acquises à l'issue de la formation :

- Maitriser l'affectation de ressources,
- Gérer les ressources partagées en contexte multi-projet,
- Analyser les projets à travers les différents affichages et formatage,
- Maîtriser les techniques de suivi de projet.
- Ingérer, nettoyer et transformer les données
- Modélisation des données pour la performance et l'évolutivité
- Conception et création de rapports pour l'analyse des données
- Appliquer et réaliser des analyses de rapports avancées
- Gérer et partager les ressources des rapports
- Déployer et configurer une architecture avancée de Zabbix, incluant les serveurs, proxies, bases de données et optimisations de performance.
- Créer et gérer des modèles avancés, en exploitant les macros, les checks actifs et passifs, ainsi que l'import/export de modèles.
- Automatiser la surveillance et la gestion avec l'API Zabbix, en intégrant des outils comme Ansible pour optimiser les tâches récurrentes.
- Mettre en place une surveillance avancée des données et des applications, en utilisant des scripts personnalisés et des indicateurs de performance clés (KPI).
- Optimiser la sécurité et l'authentification de Zabbix, en configurant SSL/TLS, en gérant les permissions et en sécurisant les communications.
- Analyser et visualiser efficacement les données de surveillance, en créant des tableaux de bord avancés, des rapports et des prévisions pour le capacity planning.
- Maîtrise de la suite Elastic pour la gestion et l'analyse de données.
- Transfert de données brutes vers Elasticsearch depuis diverses sources (fichiers, brokers).
- Création et production de tableaux de bord pour la visualisation des données dans Elasticsearch.
- Concevoir une solution de gouvernance.
- Concevoir une solution de calcul.
- Concevoir une architecture d'application.
- Concevoir le stockage, non relationnel et relationnel.
- Concevoir des solutions d'intégration de données.
- Concevoir des solutions d'authentification, d'autorisation et d'identité.
- Concevoir des solutions réseau.
- Concevoir des solutions de sauvegarde et de reprise d'activité après sinistre.
- Concevoir des solutions de monitoring.
- Concevoir des solutions de migration
- Être capable d'installer, de configurer et de mettre à jour un serveur ESXi ainsi que ses accès aux réseaux et au stockage
- Savoir configurer et gérer une infrastructure vSphere à l'aide des différents clients d'administration
- Être en mesure de déployer et gérer des machines virtuelles, de les déplacer et d'utiliser les snapshots
- Comprendre comment paramétrer vSphere pour optimiser la gestion des ressources et surveiller les consommations de ressources
- Savoir utiliser les outils de haute disponibilité de vSphere pour protéger les machines virtuelles
- Disposer des compétences nécessaires pour assurer le dépannage des hôtes ESXi, des machines virtuelles hébergées et vCenter Server$
- Comprendre le principe de Docker et Kubernetes
- Mettre en œuvre Docker et ses produits associés
- Maîtriser les concepts d'orchestration avec Kubernetes
- Gérer des conteneurs et déployer des applications dans un environnement orchestré
- Utiliser Helm pour le déploiement d'applications packagées
- Gérer les droits d'accès et la sécurité des déploiements
- Connaitre les bases, les concepts, les principales librairies du langage Python.
- Être capable de développer sa propre application en utilisant les classes et les objets.
- Comprendre l'intérêt et le fonctionnement des outils d'automatisation de gestion de l'infrastructure
- Pouvoir écrire des playboooks pour gérer son infrastructure et déployer ses applications
- Savoir créer des Rôles réutilisables
- Comprendre l'évolution et les tendances des modèles de langage et de l'IA générative.
- Maîtriser les bases du deep learning et les architectures neuronales sous-jacentes aux LLM.
- Utiliser des modèles pré-entraînés et appliquer des techniques avancées d'optimisation (fine-tuning, prompting).
- Développer des pipelines RAG en intégrant des bases de données vectorielles pour améliorer les performances des LLM.
- Mettre en œuvre des agents conversationnels et des workflows de génération de texte avec LangChain et LlamaIndex.

- Expérimenter la génération d'images avec des modèles de diffusion et Stable Diffusion.
- Implémenter des solutions IA adaptées à des besoins spécifiques en entreprise.
- Analyser et anticiper les défis éthiques et les implications légales des systèmes IA génératifs.
- Mettre en œuvre les principes de l'Infrastructure as Code (IaC) pour automatiser le cycle de vie des ressources.
- Configurer les fournisseurs (providers) pour interagir avec différentes API Cloud ou services tiers.
- Piloter le flux de travail principal (Workflow) incluant l'initialisation, la planification et l'application des changements.
- Développer des fichiers de configuration HCL (HashiCorp Configuration Language) utilisant des variables, des types complexes et des fonctions dynamiques.
- Modulariser le code Terraform pour créer des composants d'infrastructure réutilisables et versionnés.
- Sécuriser la gestion de l'état (State) et des données sensibles via des backends distants et des outils de gestion de secrets.
- Maintenir une infrastructure existante en utilisant l'importation de ressources et l'inspection de l'état en ligne de commande.
- Collaborer sur des projets d'infrastructure via l'interface et les fonctionnalités de gouvernance de HCP Terraform (Cloud).
- Concevoir une stratégie et une architecture Confiance zéro
- Évaluer les stratégies techniques et les stratégies d'opérations de sécurité des Risques conformité en matière de gouvernance (GRC)
- Concevoir la sécurité pour l'infrastructure
- Concevoir une stratégie de données et d'applications
- Mettre en œuvre des stratégies de gouvernance d'entreprise
- Mettre en œuvre une infrastructure Azure AD
- Mettre en œuvre une protection de l'identité Azure AD
- Mettre en œuvre la gestion de l'identité privilégiée Azure AD
- Mettre en œuvre Azure AD Connect
- Mettre en œuvre des stratégies de sécurité du périmètre
- Mettre en œuvre des stratégies de sécurité de réseau
- Mettre en œuvre des stratégies de sécurité de l'hôte
- Mettre en œuvre des stratégies de sécurité de conteneurs
- Mettre en œuvre Azure Key Vault
- Mettre en œuvre des stratégies de sécurité d'applications
- Mettre en œuvre des stratégies de sécurité de stockage
- Mettre en œuvre des stratégies de sécurité de bases de données
- Mettre en œuvre Azure Monitor
- Mettre en œuvre Azure Security Center
- Mettre en œuvre Azure Sentinel, notamment les classeurs, les incidents et les playbooks.
- Identifier et comprendre les techniques d'analyse et de détection
- Acquérir les connaissances pour déployer différents outils de détection d'intrusion
- Mettre en œuvre les solutions de prévention et de détection d'intrusions
- Gérer un incident d'intrusion
- Connaître le cadre juridique
- Comprendre les techniques des pirates informatiques et pouvoir contrer leurs attaques
- Mesurer le niveau de sécurité de votre Système d'Information
- Réaliser un test de pénétration
- Définir l'impact et la portée d'une vulnérabilité
- Se préparer au passage de la certification Microsoft SC-500
- Mettre en pratique les compétences liées au rôle de chef de projets
- Animer une équipe projets
- Conduire les réunions projets
- Etablir un plan d'action (organigramme des tâches, ressources...)
- Piloter les projets
- Manager les équipes
- Suivre et communiquer l'avancement
- Tenir les budgets
- Gérer les risques.
- Être capable de structurer un discours professionnel clair et cohérent
- Savoir adapter sa communication à différents types d'interlocuteurs
- Maîtriser les techniques de prise de parole en public
- Être en mesure de concevoir un support de présentation pertinent et lisible
- Savoir gérer son stress lors d'une prise de parole
- Être capable d'animer une réunion en respectant un cadre et des objectifs
- Savoir conduire des échanges constructifs (écoute active, reformulation, gestion des objections)
- Préparer le titre RNCP 36061

Modalités pédagogiques :

Session dispensée en présentiel ou téléprésentiel, selon la modalité inter-entreprises.
La formation est animée par un(e) formateur(trice) durant toute la durée de la session et présentant une suite de modules théoriques clôturés par des ateliers pratiques validant l'acquisition des connaissances. Les ateliers peuvent être accompagnés de Quizz.
L'animateur(trice) présente la partie théorique à l'aide de support de présentation, d'animation réalisée sur un environnement de démonstration.
En présentiel comme en téléprésentiel, l'animateur(trice) accompagne les participants durant la réalisation des ateliers.

Moyens et supports pédagogiques :

Cadre présentiel

Salles de formation équipées et accessibles aux personnes à mobilité réduite.

- Un poste de travail par participant
- Un support de cours numérique ou papier (au choix)
- Un bloc-notes + stylo
- Vidéoprojection sur tableau blanc
- Connexion Internet
- Accès extranet pour partage de documents et émargement électronique

Cadre téléprésentiel

Session dispensée via notre solution iClassroom s'appuyant sur Microsoft Teams.

- Un compte Office 365 par participant
- Un poste virtuel par participant
- Un support numérique (PDF ou Web)
- Accès extranet pour partage de documents et émargement électronique

Informations sur l'accessibilité :

Description / Contenu

Formation en alternance d'une durée de 24 mois. Rythme de l'alternance : 1 semaine de formation et 3 semaines en entreprises.

Module 1 : Conduite de projet avec MS PROJECT
Module 2 : Elaborer un schéma d'architecture avec Visio
Module 3 : Les différents outils de monitoring et de collecte de données d'évènements
Module 4 : PL-300T00 : Analyste de données Microsoft Power BI
Module 5 : Déployer et superviser des services Cloud (rappel AZ-104)
Module 6 : Maîtrise de Zabbix : Architecture, Optimisation et Automatisation
Module 7 : La suite Elastic
Module 8 : AZ-305T00 : Conception de solutions d'infrastructure Microsoft Azure - Certifiante
Module 9 : Green IT - Créer des services responsables
Module 10 : Faire de la veille : Collecter, traiter, analyser et diffuser l'information
Module 11 : Préparation à la certification AZ-305 : Microsoft Certified : Azure Solutions Architect Expert
Module 12 : Projet fil rouge N°1 et évaluations
Module 13 : VmWare vSphere - Installation, configuration et administration
Module 14 : Déployer et orchestrer des microservices avec Docker et Kubernetes
Module 15 : Initiation au langage Python
Module 16 : Ansible - Automatiser la gestion des serveurs
Module 17 : IA Générative en Python
Module 18 : Cartographie et modélisation du SI
Module 19 : Terraform Associate - Certifiant
Module 20 : Projet fil rouge N°2 et évaluations
Module 21 : SC-100T00 : Architecte en cybersécurité Microsoft
Module 22 : AZ-500T00 : Microsoft Azure Security Technologies - Certifiante
Module 23 : Détection d'intrusions & IOT sécurité des objets connectés
Module 24 : Avoir une expertise du hacking et de la sécurité
Module 25 : Préparation à la certification AZ-500 : Microsoft Certified: Azure Security Engineer Associate
Module 26 : Projet fil rouge N°3 et évaluations
Module 27 : Urbanisation et architecture des systèmes d'information
Module 28 : Devenir Chef de projet informatique
Module 29 : Gestion de projets informatiques
Module 30 : Développer sa capacité rédactionnelle sans l'IA !
Module 31 : Première préparation au titre RNCP 38823
Module 32 : Projet fil rouge 4 et évaluations
Module 33 : Préparation au titre RNCP 38823
Module 34 : Passage du titre RNCP 38823