



Administrateur(rice) d'Infrastructures Sécurisées

Titre Professionnel du Ministère du Travail du Plein Emploi et de l'Insertion inscrit au Répertoire National des Certifications Professionnelles (RNCP)

Bac +3/4 : Niveau 6

Code CPF : 242501

Code RNCP : RNCP37680

Code Certif Info : 114912

AIS



Le métier d'Administrateur(rice) d'Infrastructures Sécurisées

L'Administrateur(rice) d'Infrastructures Sécurisées administre les infrastructures informatiques dont il(elle) assure l'installation, le paramétrage, la sécurisation ainsi que le maintien en condition opérationnelle et en condition de sécurité. Il(Elle) est l'interlocuteur(rice) des clients, internes et externes, des responsables métiers et des décideurs (maîtrise d'ouvrage), ainsi que des partenaires externes, prestataires et fournisseurs.

Il(elle) propose et met en œuvre des solutions permettant de faire évoluer les infrastructures et contribue à la gestion des risques et à la politique de sécurité de l'entreprise.

Il(elle) installe, sécurise et met en exploitation les composants de l'infrastructure (serveurs, réseaux, hyperviseurs).

Enfin il(elle) met en œuvre et administre les moyens techniques permettant aux utilisateurs d'accéder aux données et aux applications pouvant être hébergées sur différentes infrastructures (internes, externalisés, Clouds privés ou publics), en assurant la sécurité des accès et la protection des données.

Le dispositif de formation

Public concerné



Toute personne en reconversion professionnelle ou souhaitant monter en compétences.
Niveau Bac+2 conseillé.

Toutes nos formations sont accessibles aux personnes en situation de handicap.

Métier visés / Passerelles et poursuite d'études



Métiers accessibles*

- + Administrateur(rice) Réseaux/Télécom
- + Administrateur(rice) Systèmes
- + Administrateur(rice) Infrastructure
- + Technicien(ne) Supérieur(e) Technique (télécoms et réseaux)



Passerelles et poursuite d'études possibles**

Formations accessibles à partir d'un diplôme de niveau Bac +3
Expert Réseaux infrastructure et sécurité
Master Réseaux et Télécommunication parcours sécurité des systèmes d'information et des réseaux

* Liste non-exhaustive

** La formation vise l'insertion directe en emploi. Une poursuite de parcours peut néanmoins être envisageable avec des exemples indiqués.

Prérequis et modalités d'accès



Avoir suivi une formation en informatique système et réseaux ou expérience professionnelle en assistance et maintenance en informatique.

Entrée en formation soumise à :

- + Entretien(s) avec un(e) Conseiller(e) Formation visant à démontrer la cohérence du projet professionnel en adéquation avec la formation visée
- + Positionnement via une plateforme de test
- + Validation du financement du parcours (délai d'accès variable selon le calendrier de la formation et le dispositif de financement mobilisé, entre 15 jours et 5 mois)

Méthodes mobilisées



Formation en présentiel à distance

- + 35 heures/semaine, du lundi au vendredi de 9h00 à 17h00
- + Formation synchrone avec une équipe pédagogique dédiée tout au long du parcours, comme en présentiel
- + Modalités : théorie, pratique, travaux de groupes, individuels, réalisation de projets



Prérequis techniques fortement conseillés pour suivre cette formation en présentiel à distance

- + Connexion internet « Haut débit », 15 mégabits par seconde minimum
- + Fibre non obligatoire
- + Relier sa box à son ordinateur via un câble réseau
- + Résider en France Métropolitaine
- + Être muni d'un casque audio/micro
- + PC/MAC i7, SSD, 32 Go de RAM
- + Configuration nécessaire pour travailler sur des environnements virtualisés



Pédagogie

Un apprentissage métier proactif basé sur le faire avec l'accompagnement des formateurs tout au long du parcours. Accès individuel aux ressources de formation et progression personnalisée si besoin. Outils de suivi collectif et individuels (espaces d'échanges et de partage en ligne, salles virtuelles, supports de cours, TP, exercices).

Le dispositif de formation

(suite)

Modalités d'évaluation



- + Evaluation des acquis : tout au long du parcours, tests d'acquisition des savoirs et mesures des savoir-faire lors de situations de mise en application pratique (TPs, exercices, projets), ECF
- + Fin de formation : attestation de fin de formation
- + Validation : titre professionnel du Ministère du Travail du Plein Emploi et de l'Insertion (reconnu par l'Etat et inscrit au répertoire national des certifications professionnelles (RNCP). Possibilité de validation du titre complet ou de validation partielle (CCP)
- + Modalités d'examen : modalités conformes au référentiel de certification du titre visé avec présentation d'un projet réalisé en amont de la session, un entretien technique, un questionnaire professionnel, un entretien final (y compris le temps d'échange avec le livret ECF et le Dossier Professionnel). Le jury vérifie la capacité du candidat à appréhender la globalité d'une solution technique d'infrastructure et des services qu'elle supporte, en portant une attention particulière à la prise en compte des problématiques de sécurité. Présentation détaillée des modalités de certification lors de l'entretien de candidature et en cours de parcours de formation

Que la formation se déroule en présentiel ou en présentiel à distance, l'examen final permettant de valider le titre professionnel ou la certification professionnelle se fera sur l'un de nos 3 sites (Paris, Lille, Lyon) en présence physique du candidat et des jurys habilités.

TARIF & FINANCEMENT



Tarif

Taux horaire de 16€ TTC.

Demandeurs d'emploi ou financement personnel :

Tarifs spécifiques à consulter auprès du centre concerné pour un accompagnement personnalisé.



Financement

Quel que soit votre statut (salarié du secteur privé ou public, demandeur d'emploi...), des [dispositifs de financement](#) vous aident à réaliser votre projet de formation.

Toutes nos formations sont éligibles au CPF.

Objectifs de formation

Le titre professionnel Administrateur d'infrastructures sécurisées (titre créé par arrêté de spécialité du 6 avril 2018 et modifié au JO du 13 mai 2023), niveau 6 (code NSF : 326) se compose de trois activités types, chaque activité type comportant les compétences nécessaires à sa réalisation. A chaque activité type correspond un certificat de compétences professionnelles (CCP).

A l'issue de cette formation, vous serez capable de :

Administrer et sécuriser les infrastructures

- + Appliquer les bonnes pratiques dans l'administration des infrastructures
- + Administrer et sécuriser les infrastructures réseaux
- + Administrer et sécuriser les infrastructures systèmes
- + Administrer et sécuriser les infrastructures virtualisées

Participer à la gestion de la cybersécurité

- + Participer à la mesure et à l'analyse du niveau de sécurité de l'infrastructure
- + Participer à l'élaboration et à la mise en œuvre de la politique de sécurité
- + Participer à la détection et au traitement des incidents de sécurité

Concevoir et mettre en œuvre une solution en réponse à un besoin d'évolution

- + Concevoir une solution technique répondant à des besoins d'évolution de l'infrastructure
- + Mettre en production des évolutions de l'infrastructure
- + Mettre en œuvre et optimiser la supervision des infrastructures



Parchemin et livret de certification

- + Un parchemin est attribué au candidat ayant obtenu le titre complet
- + Un livret de certification est remis au candidat en réussite partielle

Ces deux documents sont délivrés par le représentant territorial compétent du Ministère du Travail du Plein Emploi et de l'Insertion.

Le système de certification du Ministère du Travail du Plein Emploi et de l'Insertion est régi par les textes suivants :

- Code de l'éducation notamment les articles L. 335-5, L 335-6, R 335-7, R. 335-13 et R. 338-1 et suivants ;

- Arrêté du 22 décembre 2015 relatif aux conditions de délivrance du titre professionnel du Ministère du Travail du Plein Emploi et de l'Insertion ;

- Arrêté du 21 juillet 2016 (JO du 28 juillet 2016 modifié par l'arrêté du 15 septembre 2016) portant règlement général des sessions d'examen pour l'obtention du titre professionnel du Ministère du Travail du Plein Emploi et de l'Insertion.



1. Comprendre et mettre en œuvre des services réseaux

- + Révision des Notions fondamentales des réseaux
- + Protocoles réseaux / Modèle OSI
- + Protocoles TCPI/IP et adressage IPv4 et IPv6
- + Routage statique / Routage dynamique
- + Services réseaux : DNS, DHCP en environnement Windows et Linux
- + Qualité de service

2. Implémenter et Administrer des environnements Windows

- + Rappels des fondamentaux
- + Installation et configuration de Contrôleurs de domaine
- + Gestion des objets dans AD DS
- + Implémentation et administration d'une infrastructure Windows distribuée multi-sites
- + Gestion de configuration (GPO)
- + Gestion des accès et des identités
- + Mise en œuvre de DFS-R + DFS-N
- + Respect des Best Practices

3. Implémenter et Administrer des environnements Linux

- + Rappels des fondamentaux
- + Administration des services réseaux : routage, BIND, DHCP...)
- + Implémenter et administrer des serveurs Linux
- + Mise en place d'un serveur KickStart
- + Implémentation Interopérabilité Linux / Windows : Samba, NFS
- + Intégration de services Linux dans un environnement mixte

4. Sécuriser un SI

- + Gestion des identités : PKI, Kerberos, RADIUS, LDAP
- + Gestion des Certificats et des clés, SSH/TLS
- + Sécuriser une infrastructure Windows server : identité, risques, protection, audit et surveillance.
- + Introduction à la sécurisation de systèmes Linux
- + Mise en place et gestion d'une DMZ, firewall, proxy
- + Installation d'équipement PFsense ou équivalent
- + Implémentation d'un VPN
- + Sécurisation Wifi et Filaire

5. La Virtualisation

- + Configurer et administrer VMware vSphere, Hyper-V
- + Gérer des Bibliothèques et modèles
- + Gérer les VMs, les modèles, les clones et les snapshots
- + Migrer les VMs à chaud avec VMware vSphere vMotion
- + Connaître les acteurs majeurs et les usages actuels

6. Gérer des projets et communiquer

- + Gestion de projets opérationnelle, méthodes Agile
- + Gestion budgétaire
- + Préparer et animer une réunion avec des outils collaboratifs

7. Étendre un SI dans le Cloud Azure

- + Les principes du Cloud
- + Les piliers du Cloud
- + Mettre en œuvre et gérer les réseaux virtuels
- + Mettre en œuvre et gérer les machines virtuelles
- + Mise en œuvre du stockage
- + Mettre en œuvre Azure Active Directory
- + Gérer Azure Active Directory dans un environnement hybride

8. Étendre un SI dans le Cloud Amazon

- + Plateforme AWS et accès
- + Amazon VPC
- + Amazon Identity and Access Management (IAM)
- + Amazon EC2
- + Amazon S3
- + Amazon Elastic Beanstalk

9. Déployer et administrer des postes de travail pour les utilisateurs

- + Outils de gestion de mobilité, de parc et de flotte
- + EMM, BYOD, Licensing... Les défis de la mobilité et des devices
- + Déploiement de postes : WDS/MDT
- + Maintien en conformité (WSUS/GLPI OCS)
- + Gestion de configuration et de données : MDM/DLP - Microsoft 365 DLP et Intune
- + Mise en œuvre de solutions de mobilité

10. Implémenter de la haute disponibilité

- + Les fondamentaux de la haute disponibilité : redondance et scalability
- + Prévoir un PCI/PRI, comprendre son imbrication dans un PCA/PRA
- + Mise en Œuvre : SAN, Cluster, NLB, Backup en environnement Windows
- + Politique de sauvegarde et restauration RTO/RPO
- + L'intérêt du cloud dans la mise en œuvre d'une politique de disponibilité

11. Automatiser et Orchestrer

- + Automatiser l'administration (PowerShell / Bash) avec PowerShell et PowerShell Core
- + Programmation Shell Bash
- + Python pour l'administration système
- + Comprendre les apports des solutions d'orchestration et d'automatisation
- + Automatisation avec Ansible
- + Orchestration avec Kubernetes
- + AWS CloudFormation
- + Introduction à l'orchestration cloud-agnostic avec Terraform



Modalités d'obtention du titre

1. Pour un candidat issu d'un parcours continu de formation

À l'issue d'un parcours continu de formation correspondant au titre visé, le candidat est évalué par un jury composé de professionnels, sur la base des éléments suivants :

- + une mise en situation professionnelle écrite en français, reconstituée sous forme d'étude d'un cas d'entreprise, complétée par un entretien technique,
- + les résultats des évaluations passées en cours de formation;
- + un dossier professionnel dans lequel le candidat a consigné les preuves de sa pratique professionnelle, complété d'annexes si prévues au RC ;
- + un entretien final avec le jury.

2. Pour un candidat à la VAE

Le candidat constitue un dossier de demande de validation des acquis de son expérience professionnelle d'un an en rapport avec le titre visé.

Il reçoit, de l'unité départementale de la Direction Régionale de l'Economie, de l'Emploi, du Travail et des Solidarités (DREETS), une notification de recevabilité lui permettant de s'inscrire à une session titre.

Lors de cette session, le candidat est évalué par un jury de professionnels, sur la base des éléments suivants :

- + une mise en situation professionnelle ou une présentation d'un projet réalisé en amont de la session, complétée par un entretien technique
- + un dossier professionnel dans lequel le candidat a consigné les preuves de sa pratique professionnelle, complété d'annexes si prévues au RC ;
- + un entretien final avec le jury.

Pour ces deux catégories de candidats (§ 1 et 2 ci-dessus), le jury, au vu des éléments spécifiques à chaque parcours, décide ou non de l'attribution du titre. En cas de non-obtention du titre, le jury peut attribuer un ou plusieurs certificat(s) de compétences professionnelles (CCP) composant le titre. Le candidat peut se présenter aux CCP manquants dans la limite de la durée de validité du titre.

Afin d'attribuer le titre, un entretien final se déroule en fin de session du dernier CCP, et au vu du livret de certification. En cas de révision du titre, l'arrêté de spécialité fixe les correspondances entre les CCP de l'ancien titre et ceux du titre révisé. Le candidat se présente aux CCP manquants du nouveau titre.

En cas de clôture du titre, le candidat ayant antérieurement obtenu des CCP dispose d'un an à compter de la date de la fin de validité du titre pour obtenir le titre initialement visé.

3. Pour un candidat issu d'un parcours discontinu de formation ou ayant réussi partiellement le titre (formation ou VAE)

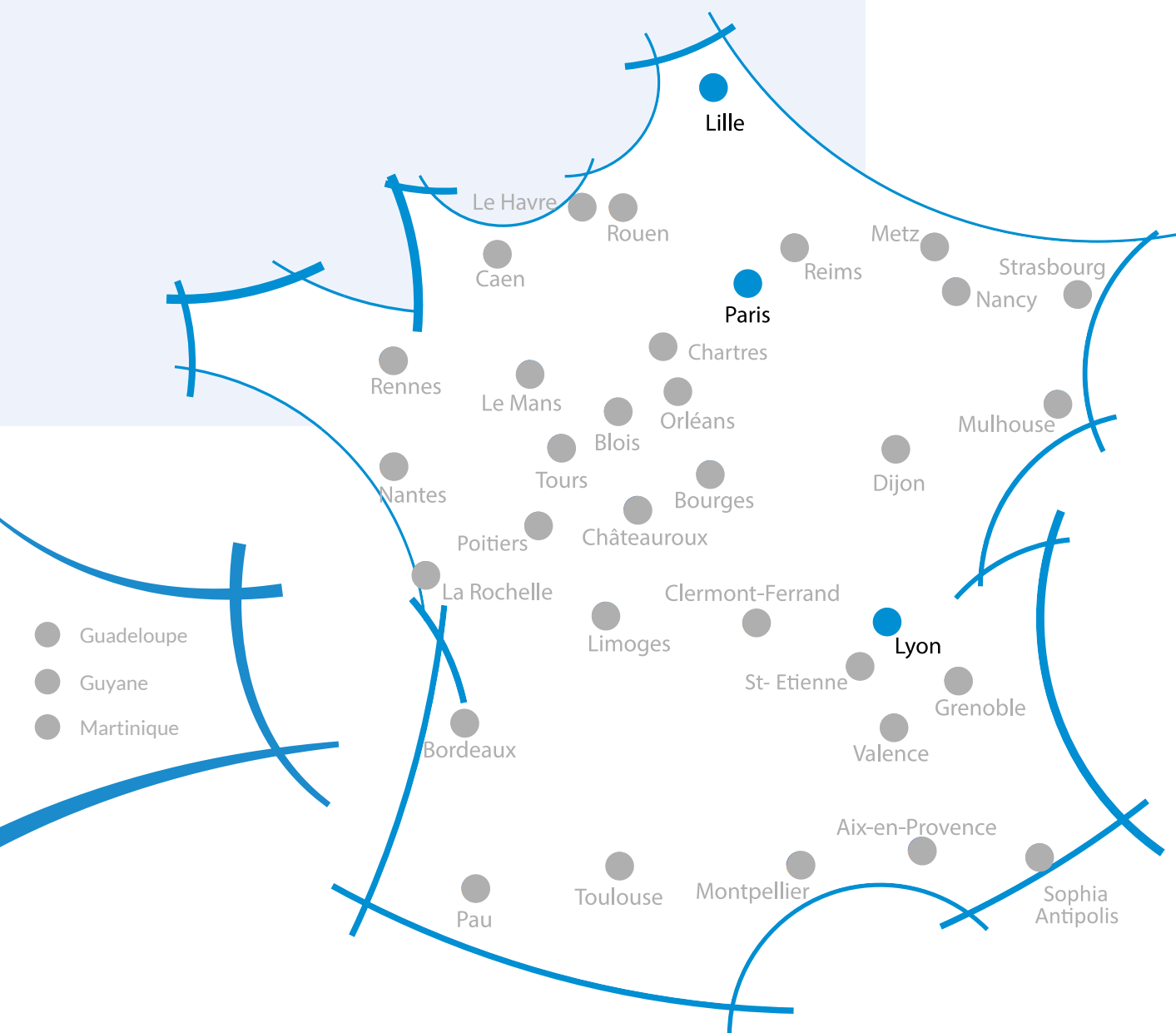
Le candidat issu d'un parcours composé de différentes périodes de formation ou ayant réussi partiellement le titre peut obtenir le titre par capitalisation des CCP constitutifs du titre.

Pour l'obtention de chaque CCP, le candidat est évalué par un jury composé de professionnels. L'évaluation est réalisée sur la base des éléments suivants :

- + Une mise en situation professionnelle ou une présentation d'un projet réalisé en amont de la session, complétée par un entretien technique;
- + Un dossier professionnel dans lequel le candidat a consigné les preuves de sa pratique professionnelle, complété d'annexes si prévues au RC.

Afin d'attribuer le titre, un entretien final se déroule en fin de session du dernier CCP, et au vu du livret de certification.

M2i, LEADER DE LA FORMATION IT, DIGITAL ET MANAGEMENT EN FRANCE



Retrouvez tous les détails de notre offre
sur diplome.m2iformation.fr

Tél. Paris : 01 44 53 36 30 - Tél. Lyon : 04 78 02 38 90 - Tél. Lille : 03 20 19 07 19

