Smartfuture
Certifications | Training | Technology solutions

Formation & Certification • ITS Cloud Computing

IT Specialist – Cloud Computing

Formation préparant à la certification IT Specialist – Cloud Computing, couvrant les concepts fondamentaux, la conception d'architectures et la gestion des environnements cloud.

Distributeur officiel Certiport | Centre d'examen Certiport

Learn • Practice • Certify

Durée	Examen
20,5 h (selon modalité)	ITS – Cloud Computing
Modalité	**Niveau**
Distanciel	Fondamental / Intermédiaire

INSCRIPTION / RÉSERVATION

Je m'inscris maintenant

- **Learn** : accès à un parcours pédagogique complet couvrant l'ensemble des objectifs officiels ITS Cloud Computing.
- **Practice** : accès à un simulateur d'examen interactif pour s'entraîner dans des conditions proches de l'examen.
- **Certify** : obtention d'un voucher de certification ITS – Cloud Computing pour passer l'examen dans un centre Certiport.

OBJECTIFS PÉDAGOGIQUES

- Comprendre les concepts du cloud et les modèles de services.
- Évaluer la pertinence d'une solution cloud pour un besoin métier.
- Concevoir une architecture performante, fiable et scalable.
- Maîtriser le déploiement, l'exploitation et les notions de gouvernance et sécurité dans le cloud.

PUBLIC CIBLE

- Pour étudiants et personnes en reconversion souhaitant se spécialiser dans le cloud.
- Pour techniciens et développeurs visant une première certification cloud.
- Pour professionnels IT impliqués dans des projets de migration ou de gestion cloud.

PRÉREQUIS

- Connaissances de base en informatique (systèmes, réseaux, applications).
- Une expérience pratique sur un environnement cloud public est un plus mais n'est pas obligatoire.

PROGRAMME DE LA FORMATION – DÉTAILLÉ

Déterminer si une solution cloud est appropriée

Expliquer les avantages du cloud aux parties prenantes

- Décrire l'infrastructure cloud et ses principaux composants.
- Faire la distinction entre IaaS, PaaS et SaaS et préciser les cas d'usage typiques.
- Montrer comment le cloud permet de construire des applications à moindre coût par rapport aux modèles traditionnels.
- Montrer comment le cloud permet de délivrer des applications plus rapidement que les modèles traditionnels.

Expliquer les coûts aux parties prenantes

- Identifier le cas d'usage : nouveau développement ou migration d'un produit/service existant.
- Identifier les ressources nécessaires pour construire le service ou produit avec des composants hébergés dans le cloud (calcul, données, réseau).
- Identifier le plan de support nécessaire pour respecter les critères de performance, disponibilité, scalabilité et fiabilité (PASR).
- Prendre en compte les facteurs entrant dans le calcul du retour sur investissement (ROI).

Expliquer la performance aux parties prenantes

- Identifier les critères de performance à respecter.
- Considérer les solutions susceptibles de répondre à ces critères.
- Évaluer le coût et la disponibilité de l'expertise technique requise.

Expliquer la fiabilité aux parties prenantes

- Identifier les critères de fiabilité, y compris les exigences en termes de débit et de latence réseau.
- Considérer les solutions qui satisfont ces critères.
- Comprendre les engagements de service (SLA) du fournisseur cloud.
- Prendre en compte les stratégies de reprise après sinistre et de sauvegarde (incluant la redondance ou le facteur de réplication).

Expliquer la disponibilité aux parties prenantes

- Identifier le cas d'usage : nouveau développement ou migration.
- Identifier les SLA amont et aval qui gouvernent les exigences de disponibilité.

- Définir les métriques de disponibilité.
- Évaluer le SLA proposé par la solution hébergée dans le cloud.

Expliquer la scalabilité aux parties prenantes

- Identifier le cas d'usage (nouveau développement ou migration).
- Comprendre que des règles peuvent être définies pour adapter dynamiquement les ressources en fonction de la demande.

Recommander des solutions sur étagère (OTS) ou sur mesure

- Identifier le cas d'usage (nouveau développement ou transition d'un produit/service existant).
- Évaluer si une solution sur étagère existante répond aux besoins en termes de performance, disponibilité, scalabilité et fiabilité.
- Évaluer l'effort technique nécessaire pour une solution sur mesure.
- Évaluer si une solution sur mesure peut dépasser l'offre OTS sur les critères PASR.

Développer l'architecture cloud

Choisir entre cloud public, privé et hybride

- Identifier les exigences de sécurité et de confidentialité pour la solution (en insistant sur les options réseau de chaque modèle).
- Prendre en compte les limites imposées par la mutualisation (tenancy) dans chaque type de mise en œuvre cloud.

Créer un schéma d'architecture et flux de données

- Décomposer la solution proposée en composants de calcul, de données et de réseau.
- Produire des groupements logiques pour ces composants.
- Tracer les flux de données entre les composants (y compris les protocoles utilisés).
- Identifier les limites du système et des composants (y compris le modèle de responsabilité).

Définir les exigences techniques

- Décider s'il faut virtualiser les serveurs, le réseau, le stockage et les postes de travail.
- Connaître les modèles de conception modernes comme les micro-services et le serverless.

- Prendre en compte l'infrastructure réseau, les dispositifs de stockage, la mémoire et les terminaux utilisateurs nécessaires.

Identifier la communication par API

- Identifier les services avec lesquels l'application doit s'intégrer.
- Comprendre comment interagir avec ces services via des API.

Créer des machines virtuelles

- Déterminer le système d'exploitation des machines virtuelles.
- Choisir la taille appropriée des machines virtuelles.
- Décider de la région géographique (latence, contraintes légales).
- Configurer les options (limites temporelles, mise à l'échelle, sauvegardes) des machines virtuelles.

Identifier les exigences de stockage de données

- Différencier les données structurées et non structurées.
- Déterminer la quantité de stockage nécessaire.
- Prendre en compte l'emplacement du stockage.
- Prendre en compte la sécurité du stockage.

Mettre en œuvre le cycle de développement cloud

Créer du contenu dans des environnements virtuels

- Comprendre la nécessité de mettre en place un système de gestion de code source.
- Installer et configurer les composants prérequis dans l'environnement virtuel.
- Enregistrer les changements et suivre les versions du code dans un gestionnaire de sources (par ex. GitHub).

Effectuer les tests

Définir des cas de test, des scénarios de test et des scripts de test.

Exécuter les tests et remonter les anomalies de manière itérative.

Structurer la solution cloud globale

Intégrer les systèmes et applications dans l'environnement cloud choisi.

Intégrer les systèmes et applications avec des systèmes existants (legacy).

Intégrer les systèmes et applications avec des applications tierces.

- Faire la distinction entre conteneurs et machines virtuelles.
- Savoir quand choisir les conteneurs plutôt que les machines virtuelles.

Déployer une application sur un serveur

- Définir la stratégie de déploiement d'une nouvelle application en remplacement d'une application existante.
- Comprendre les principes du contrôle de version.
- Identifier les solutions cloud pour créer des pipelines de code et de données (offres CI/CD cloud natives, automatisation de workflow comme GitHub Actions).
- Identifier les pratiques CI/CD existantes et les intégrer à la chaîne de déploiement.

Gérer les opérations cloud

Gérer les coûts opérationnels

- Comprendre la tarification basée sur l'usage (pay-as-you-go).
- Mettre en place des stratégies de mise à l'échelle pour répondre à la demande au meilleur coût.

Développer une politique de continuité d'activité et de reprise après sinistre

- Identifier les risques et les scénarios de sinistre.
- Établir une stratégie de sauvegarde sur site et hors site.

Fournir du support aux utilisateurs

- Identifier les politiques de protection et de sécurité pour les utilisateurs internes et externes.
- Fournir un support applicatif et matériel aux utilisateurs internes.
- Proposer des outils et ressources de formation pour les utilisateurs internes et externes.

Surveiller les systèmes cloud

- Journaliser les événements et actions majeures.
- Superviser le matériel et les logiciels (par exemple via graphiques et tableaux de bord).
- Comprendre les notifications ou alertes liées à la mise à disposition de ressources et aux sauvegardes.

PROGRAMME DE LA FORMATION – DÉTAILLÉ

Comprendre la gouvernance du cloud

Se conformer aux exigences de confidentialité et réglementaires

- Identifier les exigences de confidentialité pertinentes selon la géographie, le domaine d'activité et les politiques de l'organisation (BIPA, HIPAA, PDP, FERPA, COPPA, GDPR, CCPA, etc.).
- Identifier les engagements de conformité du fournisseur cloud vis-à-vis de ces réglementations.
- Identifier les types de données gérées dans l'environnement.
- Identifier l'emplacement et les modalités de stockage de ces données.
- Avoir connaissance des cadres et normes NIST et ISO.

Se conformer aux lignes directrices éthiques

- Prendre en compte l'impact des biais, du manque de transparence et de responsabilité dans les systèmes cloud.
- Expliquer les risques de biais et les enjeux de transparence dans l'usage de services préconfigurés.

Gérer la sécurité dans le cloud

- Comprendre les options et concepts de vérification et d'authentification de l'identité, y compris l'identité numérique et l'authentification multi facteur.
- Comprendre les politiques d'accès et les autorisations (options d'accès, rôles fournis par le fournisseur, rôles et autorisations personnalisés, hygiène des accès, principe du moindre privilège, suppression des accès inutiles, désactivation des comptes).
- Comprendre l'importance de la sécurité des données et du chiffrage.
- Comprendre les options de protection contre les accès non autorisés dans les environnements cloud (détection/prévention d'intrusion, pare-feu, etc.).