



Objectifs	Cette formation enseigne aux Architectes de solutions les exigences des entreprises en solutions sécurisées, évolutives et fiables. Les modules comprennent l'infrastructure de virtualisation, d'automatisation, de la mise en réseau, du stockage, de l'identité, de la sécurité, de la plateforme de données, et des applications. Cette formation souligne la manière dont les décisions prises, dans chacun de ces domaines, affectent une solution globale.
Participants	Professionnels de l'informatique possédant de l'expérience dans la conception et la mise en œuvre de solutions exécutées sur Microsoft Azure - Toutes personnes possédant des connaissances approfondies des opérations informatiques, notamment la mise en réseau, la virtualisation, l'identité, la sécurité, la continuité des activités, la reprise après sinistre, la plateforme de données, la budgétisation et la gouvernance - Toutes personnes ayant des compétences de niveau expert dans l'administration Azure et une expérience dans les procédés de développement Azure et les procédés DevOps - Les Architectes de solutions Azure utilisent le portail Azure et en se familiarisant davantage, ils utiliseront le Command Line Interface
Prérequis	Avoir une compréhension des technologies de virtualisation sur site, y compris : les machines virtuelles, la mise en réseau virtuelle, et les disques durs virtuels. - Avoir une compréhension de la configuration du réseau, ce qui inclut TCP/IP, le système de nom de domaine (DNS), les réseaux privés virtuels (VPN), les pare-feux et les technologies de cryptage - Avoir une compréhension des concepts d'Active Directory, ce qui inclut les domaines, les forêts, les contrôleurs de domaine, la réplication, le protocole Kerberos et le Lightweight Directory Access Protocol (LDAP) -Avoir une compréhension de la résilience et la récupération après sinistre, ce qui inclut les opérations de sauvegarde et de récupération.
Moyens pédagogiques	1 poste par participant - 1 Vidéo projecteur - Support de cours fourni à chaque participant - Ateliers individuels
Méthodes pédagogiques	Approche participative et interactive - Alternance d'apports théoriques et de mises en situation - Accompagnement personnalisé du formateur.
Durée	5 jour(s) - 35 heure(s)

Code : NCI_3E5F6G7H8I

Programme :

Mise en Réseau Virtuelle

Virtual Network Peering
Mise en œuvre de VNet Peering

Mise en œuvre des machines virtuelles pour Windows et Linux

Sélectionner la taille de la machine virtuelle
Configurer la haute disponibilité
Mise en œuvre d' Azure Dedicated Hosts
Déployer et configurer des ensembles d'échelle
Configurer Azure Disk Encryption

Automatiser le Déploiement et la Configuration des Ressources

Créer des Modèles Azure Resource Manager
Enregistrer un Modèle pour une Machine Virtuelle
Évaluer l'emplacement des nouvelles ressources
Configurer un modèle de disque dur virtuel
Déployer à partir d'un modèle
Créer et exécuter un Runbook d'automatisation

Mise en œuvre de l'équilibrage de charges et la sécurité réseau

Mise en œuvre de l'équilibreur de charges Azure
Mise en œuvre d'une passerelle de données
Comprendre le pare-feu des applications Web
Mise en œuvre du pare-feu Azure
Mise en œuvre d'une porte d'entrée Azure
Mise en œuvre d'Azure Traffic Manager
Mise en œuvre des groupes de sécurité réseau et les groupes de sécurité applications
Mise en œuvre d'Azure Bastion

Mise en œuvre des comptes de stockage

Comptes de stockage
Stockage des blobs
Sécurité du stockage
Gestion du stockage
Accéder à des Blobs et des files d'attente à l'aide d'Azure Active Directory (AAD)
Configurer les pare-feux du stockage Azure et les réseaux virtuels

Mettre en œuvre Azure Active Directory

Présentation d'Azure Active Directory
Utilisateurs et groupes
Domaines et domaines personnalisés
Protection de l'identité Azure AD
Mise en œuvre d'un accès conditionnel
Configurer des alertes de fraude pour l'authentification multifactor (MFA)
Mise en œuvre des options de contournement
Configurer des adresses IP approuvées
Configurer les utilisateurs invités dans Azure AD
Gérer plusieurs répertoires

Mise en œuvre et gestion de la gouvernance Azure

Créer des groupes de gestion, des abonnements et des groupes de ressources
Présentation du contrôle d'accès en fonction du rôle (RBAC)
Rôles du contrôle d'accès en fonction du rôle (RBAC)
Commentaires sur l'accès à Azure AD
Mise en œuvre et configuration d'une stratégie Azure
Azure Blueprints

Mise en œuvre et gestion les identités hybrides

Installer et configurer Azure AD Connect
Configurer la synchronisation et l'écriture des mots de passe
Configurer Azure AD Connect Health

Gérer les charges de travail dans Azure

Migrer des charges de travail à l'aide d'Azure Migrate
Migration sans agent des machines virtuelles VMware
Migration basée sur l'agent des machines virtuelles VMware
Mise en œuvre de la sauvegarde Azure
Récupération d'urgence Azure à Azure
Mise en œuvre de la gestion de l'actualisation Azure

Mise en œuvre de la surveillance de l'infrastructure cloud

Surveillance de la sécurité de l'infrastructure Azure
Azure Monitor
Classeurs Azure

