Durée :	5 jours soit 35 heures	Référence :	AZ-802T00

Public visé :

Profils concernés

- Administrateurs systèmes Windows.
- Administrateurs systèmes et réseaux.
- Ingénieurs systèmes Microsoft.
- Administrateurs infrastructures hybrides.
- Techniciens systèmes confirmés souhaitant évoluer vers des fonctions d'administration avancée.
- Consultants infrastructures Microsoft.

Métiers visés

- Administrateur Windows Server.
- Administrateur systèmes et réseaux.
- Ingénieur systèmes Microsoft.
- Administrateur infrastructures hybrides Azure.
- Ingénieur exploitation.
- Consultant Microsoft Infrastructure.
- Responsable technique infrastructures Windows.

Niveau attendu

Intermédiaire à avancé.

Cette formation s'adresse à des professionnels disposant déjà d'une expérience de l'administration Windows Server et souhaitant approfondir leurs compétences sur les environnements hybrides Microsoft, Active Directory, Azure et les services d'infrastructure associés.

Pré-requis :

Prérequis indispensables

- Maîtriser les fondamentaux de l'administration des systèmes Windows Server.
- Posséder une expérience pratique de l'administration d'un environnement Windows d'entreprise.
- Comprendre les concepts de base des réseaux TCP/IP (adressage IP, DNS, DHCP, routage).
- Connaître les principes fondamentaux d'Active Directory (utilisateurs, groupes, domaines, contrôleurs de domaine).
- Disposer de notions d'administration via PowerShell.
- Posséder une connaissance de base des services Microsoft Azure et de la virtualisation.

Prérequis recommandés (sans être obligatoires)

- Expérience dans l'administration d'environnements hybrides Windows Server et Azure.
- Connaissances préalables de Microsoft Entra ID (Azure AD).
- Première expérience de l'administration d'Hyper-V ou de machines virtuelles Azure.

Objectifs pédagogiques :

À l'issue de la formation, le participant sera capable de :

- Déployer et administrer les services de domaine Active Directory dans des environnements locaux et Azure.
- Mettre en œuvre une infrastructure d'identité hybride entre Active Directory et Microsoft Entra ID.
- Configurer et gérer les stratégies de groupe afin d'appliquer les paramètres de sécurité et d'administration des postes et serveurs.
- Administrer et sécuriser les infrastructures Windows Server à l'aide des outils Microsoft de gestion locale, distante et automatisée.
- Déployer et exploiter des machines virtuelles Windows Server dans Azure en intégrant les exigences de sécurité, de disponibilité et de continuité de service.
- Mettre en œuvre les services réseau Windows Server et Azure tels que DNS, DHCP, IPAM et les services d'adressage IP.
- Déployer et administrer les solutions de stockage, de partage de fichiers et de réplication dans des environnements hybrides.

- Configurer et gérer les infrastructures Hyper-V, les workloads virtualisés et les conteneurs Windows Server.

Compétences acquises à l'issue de la formation :

- Être capable de déployer, administrer et maintenir une infrastructure Active Directory Domain Services (AD DS) incluant les contrôleurs de domaine, les rôles FSMO, la réplication, les relations d'approbation et les services d'identité associés.
- Savoir gérer et sécuriser les objets Active Directory et les stratégies de groupe (GPO) afin d'administrer les utilisateurs, groupes, unités organisationnelles, comptes de service et politiques de sécurité dans un environnement d'entreprise.
- Être en mesure de mettre en œuvre et administrer une architecture d'identité hybride Microsoft Entra ID et Windows Server, incluant la synchronisation des identités, Microsoft Entra Connect, l'authentification hybride et Microsoft Entra Domain Services.
- Maîtriser l'administration, l'automatisation et la sécurisation des environnements Windows Server hybrides et Azure à l'aide des outils d'administration à distance, PowerShell, JEA, Azure Arc, Azure Automation, Azure Update Manager et Azure Machine Configuration.
- Être capable de déployer, configurer et administrer des infrastructures réseau Windows Server et Azure comprenant DNS, DHCP, IPAM, le routage IP, l'adressage réseau, les réseaux virtuels Azure et les mécanismes de sécurisation des communications.
- Savoir déployer, gérer et sécuriser des machines virtuelles Windows Server dans Azure en intégrant les mécanismes de haute disponibilité, de montée en charge, de reprise d'activité, d'administration sécurisée et de protection réseau.
- Être capable de mettre en œuvre et administrer les services de stockage et de fichiers Windows Server en environnement hybride, notamment Azure Files, Azure File Sync, SMB, FSRM, Storage Spaces, Storage Spaces Direct, la déduplication, iSCSI et Storage Replica.
- Maîtriser le déploiement, l'administration et la sécurisation des infrastructures de virtualisation Hyper-V et des conteneurs Windows Server, y compris les fonctionnalités de haute disponibilité et de protection des workloads.

Modalités pédagogiques :

Session dispensée en présentiel ou téléprésentiel, selon la modalité inter-entreprises ou intra-entreprises sur mesure. 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.

Note relative au programme : Les ateliers, démonstrations, travaux pratiques et scénarios présentés dans ce programme sont fournis à titre d'exemples illustratifs et ne sont pas exhaustifs. Afin de garantir une adéquation permanente avec les évolutions technologiques, le contenu pédagogique ainsi que les environnements de travaux pratiques (TP) sont susceptibles d'être adaptés, ajustés ou mis à jour au cours du temps.

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
- 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

Modalités d'évaluation et de suivi :

Avant

Afin de valider le choix d'un programme de formation, une évaluation des prérequis est réalisée à l'aide d'un questionnaire en ligne ou lors d'un échange avec le formateur(trice), qui valide la base de connaissances nécessaires.

Les stagiaires disposent également, depuis leur extranet, d'un **outil d'auto-positionnement** leur permettant d'évaluer leur niveau de maîtrise des compétences visées par la formation. Cette auto-évaluation est réalisée avant le démarrage de la formation à l'aide d'un curseur de positionnement allant du niveau le plus faible au niveau le plus élevé.

Pendant

Après chaque module théorique, un ou plusieurs ateliers pratiques permettent de valider progressivement l'acquisition des connaissances. Un quiz peut accompagner les ateliers pratiques afin de mesurer la compréhension des notions abordées.

Après

À l'issue de la formation, les stagiaires réalisent une nouvelle **auto-évaluation** sur les mêmes compétences que celles évaluées avant la formation. Cette comparaison permet de mesurer leur perception de la progression réalisée et de visualiser les compétences développées au cours de la formation.

Lorsque le programme de formation le prévoit, un examen de certification est organisé conformément aux modalités définies par l'éditeur ou le centre de certification (TOSA, Pearson VUE, ENI, PeopleCert…).

Le formateur réalise également une **évaluation individuelle des compétences** de chaque stagiaire sur l'ensemble des compétences visées par la formation. Pour chacune d'elles, il indique si la compétence est :

- Acquise ;
- En cours d'acquisition ;
- Non acquise.

Lorsque la compétence est évaluée comme **en cours d'acquisition** ou **non acquise**, le formateur formule des observations précisant les difficultés rencontrées ainsi que les actions ou recommandations permettant au stagiaire de poursuivre sa montée en compétences.

Enfin

Un questionnaire de satisfaction permet au participant d'évaluer la qualité de la prestation de formation.

Informations sur l'accessibilité :

Nos formations sont, dans la mesure du possible, conçues pour être accessibles à toutes et à tous. Afin de garantir les meilleures conditions d'accueil et d'apprentissage pour les personnes en situation de handicap, nous vous invitons à contacter notre référente handicap certifiée :
Céline SOLATGES – 05 61 34 39 80 – csolatges@iform.fr
Nous vous remercions de bien vouloir nous communiquer toute information utile à ce sujet en amont de la formation, afin de mettre en place les adaptations nécessaires et d'assurer un accompagnement optimal.

Pour en savoir plus sur les dispositifs d'accompagnement existants, vous pouvez consulter les sites suivants :

- AGEFIPH
- FIPHFP
- MDPH de votre département

Description / Contenu

Module 1 : Déployer et gérer les contrôleurs de domaine des services de domaine Active Directory

Ce module vous présente la topologie des contrôleurs de domaine au sein d'un environnement Active Directory. Il vous initie également au déploiement, à la gestion et à la migration d'un contrôleur de domaine d'un serveur vers un autre.

- Définir les services de domaine Active Directory
- Définir les forêts et les domaines des services de domaine Active Directory
- Déployer les contrôleurs de domaine des services de domaine Active Directory
- Migrer un contrôleur de domaine vers un nouveau site
- Gérer les maîtres d'opérations des services de domaine Active Directory

Module 2 : Déployer et gérer des contrôleurs de domaine Active Directory IaaS Azure dans Azure

Ce module présente la mise en œuvre de contrôleurs de domaine des services de domaine Active Directory (AD DS) sur des machines virtuelles Azure. Vous apprenez à choisir entre le déploiement d'une forêt Azure autonome et l'extension d'un environnement local dans Azure, à configurer la connectivité entre les environnements à l'aide d'un VPN site à site ou d'ExpressRoute, et à planifier les sites AD DS, les relations d'approbation, les contrôleurs de domaine en lecture seule (RODC), le placement des rôles FSMO et les serveurs de catalogue global. Vous parcourez également les étapes permettant d'installer un contrôleur de domaine répliqué et de créer une nouvelle forêt AD DS dans Azure.

- Choisir une option pour mettre en œuvre les services d'annuaire et d'identité à l'aide des services de domaine Active Directory dans Azure
- Déployer et configurer des contrôleurs de domaine des services de domaine Active Directory sur des machines virtuelles Azure
- Installer un contrôleur de domaine Active Directory répliqué sur une machine virtuelle Azure
- Installer une nouvelle forêt Active Directory sur un réseau virtuel Azure

Module 3 : Gérer les contrôleurs de domaine AD DS et les rôles FSMO

Ce module présente le déploiement et la gestion des contrôleurs de domaine AD DS et des rôles FSMO. Vous apprenez à déployer des contrôleurs de domaine dans des environnements locaux à l'aide de Server Manager et de l'Assistant Configuration des services de domaine Active Directory, à maintenir la disponibilité des contrôleurs de domaine grâce à des procédures de sauvegarde et de récupération, à gérer le rôle de catalogue global et son placement entre les différents sites, à comprendre et gérer les cinq rôles FSMO (maître de schéma, maître d'attribution de noms de domaine, maître RID, maître d'infrastructure et émulateur PDC), à transférer les rôles FSMO entre les contrôleurs de domaine et à reprendre ces rôles dans des situations d'urgence, ainsi qu'à gérer et étendre le schéma AD DS.

- Déployer des contrôleurs de domaine AD DS
- Maintenir les contrôleurs de domaine AD DS
- Gérer le rôle de catalogue global AD DS
- Gérer les maîtres d'opérations AD DS
- Gérer le schéma AD DS

Module 4 : Créer et gérer des objets Active Directory

Ce module présente la création et la gestion des principaux objets des services de domaine Active Directory (AD DS). Vous apprenez à créer et configurer des comptes d'utilisateurs, des groupes de sécurité, des unités organisationnelles (OU) et des comptes de service gérés, notamment les comptes de service gérés de groupe (gMSA). Vous effectuez également des tâches de gestion en masse, telles que le déplacement de comptes et le forçage des réinitialisations de mots de passe, et vous maintenez la disponibilité des contrôleurs de domaine grâce à la réplication multimaître, à la Corbeille Active Directory et aux opérations de restauration faisant ou non autorité.

- Définir les utilisateurs, les groupes et les ordinateurs
- Définir les unités organisationnelles
- Gérer les objets et leurs propriétés dans Active Directory
- Créer des objets dans Active Directory
- Configurer des objets dans Active Directory
- Effectuer des tâches de gestion en masse pour les comptes d'utilisateurs
- Maintenir les contrôleurs de domaine des services de domaine Active Directory

Module 5 : Mettre en œuvre une identité hybride avec Windows Server

Ce module présente la mise en œuvre d'une identité hybride en intégrant les services de domaine Active Directory (AD DS) locaux à Microsoft Entra ID. Vous apprenez à choisir parmi les modèles d'intégration Microsoft Entra, notamment l'extension d'AD DS à Azure, la synchronisation d'annuaire, la synchronisation des hachages de mots de passe et la fédération avec AD FS, à planifier et préparer AD DS local pour la synchronisation avec Microsoft Entra Connect, à configurer l'authentification unique (SSO) transparente et l'authentification directe, à activer la connexion Microsoft Entra ID pour les machines virtuelles Azure et à mettre en œuvre Microsoft Entra Domain Services pour l'authentification Kerberos, LDAP et les stratégies de groupe dans le cloud, sans déployer de contrôleurs de domaine.

- Choisir un modèle d'intégration Microsoft Entra
- Planifier l'intégration de Microsoft Entra
- Préparer Active Directory local pour la synchronisation d'annuaire
- Installer et configurer la synchronisation d'annuaire avec Microsoft Entra Connect
- Mettre en œuvre l'authentification unique (SSO) transparente
- Activer la connexion Microsoft Entra pour une machine virtuelle Windows dans Azure
- Vérification des connaissances 1
- Décrire Microsoft Entra Domain Services

- Mettre en œuvre et configurer Microsoft Entra Domain Services
- Gérer Windows Server dans un environnement Microsoft Entra Domain Services
- Créer et configurer une instance Microsoft Entra Domain Services
- Joindre une machine virtuelle Windows Server à un domaine géré

Module 6 : Créer et configurer des objets de stratégie de groupe dans Active Directory

Ce module porte sur les objets de stratégie de groupe, notamment sur leur utilisation pour appliquer une stratégie de mot de passe à l'échelle du domaine ainsi que des stratégies de mot de passe avec un niveau de granularité plus précis.

- Définir les objets de stratégie de groupe
- Mettre en œuvre la portée et l'héritage des objets de stratégie de groupe
- Définir les objets de stratégie de groupe basés sur le domaine
- Créer et configurer un objet de stratégie de groupe basé sur le domaine
- Configurer une stratégie de mot de passe au niveau du domaine
- Configurer et appliquer une stratégie de mot de passe avec un niveau de granularité précis

Module 7 : Mettre en œuvre les objets de stratégie de groupe

Apprendre à mettre en œuvre les objets de stratégie de groupe (GPO) dans les services de domaine Active Directory (AD DS).

- Définir les GPO
- Mettre en œuvre la portée et l'héritage des GPO
- Définir les GPO basées sur le domaine
- Créer et configurer un GPO basé sur le domaine
- Définir le stockage des GPO
- Définir les modèles d'administration

Module 8 : Gérer les fonctionnalités avancées d'AD DS

Ce module présente les tâches d'administration avancées des services de domaine Active Directory (AD DS). Vous apprenez à créer et gérer des relations d'approbation, notamment les approbations externes, entre forêts et entre domaines Kerberos, à mettre en œuvre des forêts ESAE (Enhanced Security Administrative Environment) pour protéger les comptes privilégiés en appliquant le principe de la source propre, à surveiller et résoudre les problèmes de réplication AD DS à l'aide de Performance Monitor, Repadmin.exe et Dcdiag.exe, et à créer des partitions d'application AD DS personnalisées à l'aide de NtdsUtil.exe.

- Créer des relations d'approbation
- Mettre en œuvre des forêts ESAE
- Surveiller et résoudre les problèmes liés à AD DS
- Créer des partitions AD DS personnalisées

Module 9 : Administrer et gérer à distance des machines virtuelles IaaS Windows Server

Ce module présente l'administration et la gestion à distance des machines virtuelles IaaS Windows Server dans Azure. Vous apprenez à sélectionner l'outil d'administration à distance approprié parmi le portail Azure, Windows Admin Center, Azure PowerShell, Azure CLI et Azure Cloud Shell, à vous connecter de manière sécurisée aux machines virtuelles Azure à l'aide d'Azure Bastion sans exposer d'adresses IP publiques, et à configurer l'accès aux machines virtuelles juste-à-temps (JIT) via Microsoft Defender for Cloud afin de restreindre les ports de gestion entrants et de réduire la surface d'attaque.

- Sélectionner l'outil d'administration à distance approprié
- Gérer les machines virtuelles Windows avec Azure Bastion
- Créer un hôte Azure Bastion
- Configurer l'administration juste-à-temps

Module 10 : Décrire les outils d'administration de Windows Server

Ce module présente les outils disponibles pour administrer Windows Server dans des environnements locaux et à distance. Vous apprenez à installer et utiliser Windows Admin Center pour gérer les serveurs via une interface web, à utiliser Server Manager pour gérer les rôles et les fonctionnalités, à installer et configurer les outils d'administration de serveur distant (RSAT) sur les systèmes d'exploitation clients Windows, et à utiliser la communication à distance Windows PowerShell avec WinRM pour exécuter des commandes et des scripts sur des serveurs distants.

- Découvrir Windows Admin Center
- Utiliser Server Manager
- Répertorier les outils d'administration de serveur distant
- Utiliser Windows PowerShell
- Utiliser Windows PowerShell pour administrer un serveur à distance

Module 11 : Administration juste suffisante dans Windows Server

Ce module présente la configuration et l'utilisation de Just Enough Administration (JEA) pour restreindre les accès administratifs dans Windows Server. Vous apprenez comment JEA utilise la communication à distance PowerShell avec des comptes virtuels pour limiter les utilisateurs à des applets de commande, des paramètres et des valeurs spécifiques, à définir des fonctionnalités de rôle et des fichiers de configuration de session pour contrôler les actions disponibles dans une session JEA, et à créer et utiliser des points de terminaison JEA pour des tâches d'administration restreintes, telles que le redémarrage de services ou le déploiement de conteneurs.

- Expliquer le concept de Just Enough Administration (JEA)
- Définir les fonctionnalités de rôle pour un point de terminaison JEA
- Créer un fichier de configuration de session pour enregistrer un point de terminaison JEA
- Décrire le fonctionnement des points de terminaison JEA pour limiter l'accès à une session PowerShell
- Créer et se connecter à un point de terminaison JEA
- Démonstration : Se connecter à un point de terminaison JEA

Module 12 : Effectuer une administration sécurisée de Windows Server

Ce module présente la mise en œuvre de pratiques d'administration sécurisée dans les environnements Windows Server. Vous apprenez à appliquer le principe du moindre privilège en identifiant et en restreignant l'appartenance aux groupes privilégiés intégrés, tels que Enterprise Admins et Domain Admins, à déléguer le contrôle administratif à l'aide de l'Assistant Délégation de contrôle et des groupes restreints, à déployer des stations de travail à accès privilégié (PAW) avec Windows Defender Application Control, Credential Guard et Device Guard, et à configurer des serveurs de rebond pour contrôler l'accès à distance aux infrastructures sensibles.

- Définir l'administration selon le principe du moindre privilège
- Mettre en œuvre les privilèges délégués
- Utiliser des stations de travail à accès privilégié
- Utiliser des serveurs de rebond

Module 13 : Utiliser des techniques avancées de communication à distance avec Windows PowerShell

Ce module présente des techniques avancées utiles permettant de surmonter les limitations de la communication à distance Windows PowerShell de base.

- Examiner les techniques courantes de communication à distance avec Windows PowerShell
- Envoyer des paramètres à des ordinateurs distants avec Windows PowerShell
- Définir la protection d'accès aux variables, aux alias et aux fonctions à l'aide du modificateur de portée
- Activer la communication à distance multibond avec Windows PowerShell

Module 14 : Gérer un ou plusieurs ordinateurs à l'aide de la communication à distance avec Windows PowerShell

Ce module explique comment utiliser la communication à distance pour effectuer des tâches d'administration sur des ordinateurs distants.

- Examiner la fonctionnalité de communication à distance de Windows PowerShell
- Comparer la communication à distance et la connectivité à distance
- Examiner les fonctionnalités de sécurité liées à la communication à distance de Windows PowerShell
- Activer la communication à distance à l'aide de Windows PowerShell
- Utiliser la communication à distance un-à-un à l'aide de Windows PowerShell
- Utiliser la communication à distance un-à-plusieurs à l'aide de Windows PowerShell
- Comparer les résultats obtenus à distance et localement

Module 15 : Gérer les workloads hybrides avec Azure Arc

Ce module présente la gestion des workloads hybrides à l'aide d'Azure Arc. Vous apprenez à décrire les fonctionnalités d'Azure Arc pour gérer Windows Server, Linux, les clusters Kubernetes et SQL Server dans des environnements hybrides et multicloud, à intégrer des instances de serveurs locaux à Azure Arc à l'aide de l'agent Azure Connected Machine, à connecter des machines hybrides à Azure depuis le portail Azure à l'aide de scripts interactifs ou de déploiements de principaux de service à grande échelle, à gérer les extensions et à surveiller les serveurs compatibles avec Arc via Azure Resource Manager, et à restreindre l'accès aux ressources compatibles avec Arc à l'aide du contrôle d'accès en fonction du rôle (RBAC).

- Décrire Azure Arc
- Intégrer des instances Windows Server
- Connecter des machines hybrides à Azure depuis le portail Azure

- Utiliser Azure Arc pour gérer des instances Windows Server
- Restreindre l'accès avec le contrôle d'accès en fonction du rôle (RBAC)

Module 16 : Gérer les mises à jour Azure
Gérer les mises à jour du système d'exploitation des machines virtuelles Azure et des serveurs compatibles avec Azure Arc à l'aide d'Azure Update Manager.

- Décrire Azure Update Manager
- Préparer les machines pour Azure Update Manager
- Déployer les mises à jour
- Évaluer les mises à jour
- Gérer les mises à jour à grande échelle

Module 17 : Automatiser la configuration des machines virtuelles IaaS Windows Server
Apprendre à déployer des extensions Desired State Configuration (DSC), à utiliser ces extensions pour remédier aux problèmes de conformité des serveurs et à utiliser l'extension de script personnalisé.

- Décrire Azure Automation
- Mettre en œuvre Azure Automation avec DSC
- Remédier aux problèmes de conformité des serveurs
- Décrire les extensions de script personnalisé
- Configurer une machine virtuelle à l'aide de DSC

Module 18 : Appliquer la configuration de sécurité des machines virtuelles avec Azure Machine Configuration
Auditer et appliquer la configuration de sécurité du système d'exploitation sur les machines virtuelles Azure et les serveurs compatibles avec Azure Arc à l'aide d'Azure Machine Configuration. Appliquer les stratégies intégrées de référence de sécurité pour Windows et Linux, configurer les modes d'audit et d'application, et créer des configurations de machine personnalisées répondant aux exigences de sécurité propres à l'organisation.

- Découvrir les fonctionnalités et les modes de l'extension Azure Machine Configuration
- Appliquer les stratégies de référence de sécurité intégrées
- Créer et attribuer des configurations de machine personnalisées

Module 19 : Découvrir Azure Automation avec DevOps
Apprendre à mettre en œuvre Azure Automation avec DevOps à l'aide de runbooks, de webhooks et de workflows PowerShell. Comprendre comment créer des comptes Automation, gérer les ressources partagées, intégrer des systèmes de contrôle de code source et planifier la gestion du cloud hybride dans les environnements Azure et locaux.

- Créer des comptes Automation
- Qu'est-ce qu'un runbook ?
- Comprendre les ressources partagées d'Automation
- Découvrir la galerie de runbooks
- Examiner les webhooks
- Découvrir l'intégration au contrôle de code source
- Découvrir les workflows PowerShell
- Créer un workflow
- Découvrir la gestion hybride
- Examiner les points de contrôle et le traitement parallèle

Module 20 : Configurer et gérer les machines virtuelles Hyper-V
Ce module présente la configuration et la gestion des machines virtuelles Hyper-V dans Windows Server. Vous apprenez à choisir entre les machines virtuelles de génération 1 et de génération 2, à utiliser les formats de disque dur virtuel VHD et VHDX, à configurer les paramètres matériels des machines virtuelles, notamment les processeurs, la mémoire, la topologie NUMA et le TPM virtuel, à sélectionner les options de stockage telles que les disques locaux, les SAN Fibre Channel et les partages de fichiers SMB 3.0, et à mettre en œuvre des disques VHD partagés et des jeux de fichiers VHD (VHD Sets) pour les clusters de basculement invités.

- Répertorier les versions de configuration des machines virtuelles
- Répertorier les générations de machines virtuelles
- Répertorier les formats et types de VHD disponibles
- Créer et configurer des machines virtuelles
- Déterminer les options de stockage pour les machines virtuelles
- Définir les VHD partagés et les jeux de fichiers VHD (VHD Sets)
- Mettre en œuvre des clusters invités à l'aide de VHDX partagés

Module 21 : Configurer et gérer Hyper-V
Ce module présente l'installation et la configuration du rôle Hyper-V dans Windows Server. Vous apprenez à préparer les hôtes Hyper-V conformément aux bonnes pratiques, à utiliser le Gestionnaire Hyper-V pour gérer les machines virtuelles et les hôtes, à créer et configurer des commutateurs virtuels (externes, internes et privés) prenant en charge les VLAN, à mettre en œuvre des fonctionnalités réseau avancées, notamment NIC Teaming, SR-IOV, la gestion de la bande passante, DHCP Guard, la mise en miroir des ports et Switch Embedded Teaming (SET), et à configurer la virtualisation

imbriquée pour exécuter Hyper-V au sein d'une machine virtuelle.

- Définir Hyper-V
- Définir le Gestionnaire Hyper-V
- Configurer les hôtes Hyper-V conformément aux bonnes pratiques
- Configurer la mise en réseau Hyper-V
- Évaluer les fonctionnalités réseau avancées d'Hyper-V
- Définir la virtualisation imbriquée

Module 22 : Sécuriser les workloads Hyper-V

Ce module présente la sécurisation des workloads Hyper-V dans Windows Server à l'aide d'une infrastructure protégée (guarded fabric). Vous apprenez à déployer et configurer le Host Guardian Service (HGS) avec les modes d'attestation basés sur un TPM approuvé et sur une clé d'hôte, à utiliser le Key Protection Service (KPS) pour contrôler l'accès aux clés de chiffrement des machines virtuelles protégées, à distinguer les machines virtuelles standard, les machines virtuelles prenant en charge le chiffrement et les machines virtuelles protégées, et à créer et déployer des machines virtuelles protégées à l'aide de disques modèles signés avec le chiffrement BitLocker et des fichiers de données de provisionnement.

- Définir une infrastructure protégée (guarded fabric)
- Définir le Host Guardian Service
- Découvrir l'attestation basée sur un TPM approuvé
- Définir le KPS
- Déterminer les principales fonctionnalités des machines virtuelles protégées
- Comparer les machines virtuelles prenant en charge le chiffrement et les machines virtuelles protégées dans une infrastructure protégée (guarded fabric)
- Mettre en œuvre une machine virtuelle protégée

Module 23 : Mettre en œuvre la haute disponibilité des machines virtuelles Windows Server

Ce module présente la mise en œuvre de la haute disponibilité des machines virtuelles Hyper-V dans Windows Server. Vous apprenez à choisir entre la mise en cluster des hôtes, la mise en cluster des invités et l'équilibrage de charge réseau (NLB) selon les différents types de workloads, à configurer et effectuer une migration dynamique pour déplacer des machines virtuelles en cours d'exécution entre des hôtes Hyper-V à l'aide de l'authentification CredSSP ou Kerberos, et à effectuer une migration du stockage pour déplacer les fichiers de disque dur virtuel des machines virtuelles sans interruption de service.

- Sélectionner les options de haute disponibilité pour Hyper-V
- Envisager l'équilibrage de charge réseau pour les machines virtuelles Hyper-V
- Mettre en œuvre la migration dynamique des machines virtuelles Hyper-V
- Mettre en œuvre la migration du stockage des machines virtuelles Hyper-V

Module 24 : Exécuter des conteneurs sur Windows Server

Ce module présente l'exécution et la gestion des conteneurs sur Windows Server. Vous apprenez en quoi les conteneurs diffèrent des machines virtuelles, à choisir entre les modes d'isolation des processus et d'isolation Hyper-V, à préparer un hôte Windows Server pour les workloads de conteneurs à l'aide de Docker, à extraire des images de base de conteneurs (Server Core, Nano Server, Windows) depuis Microsoft Container Registry, et à gérer les conteneurs à l'aide des commandes Docker et de Windows Admin Center.

- Définir les conteneurs
- Identifier les différences entre les conteneurs et les machines virtuelles
- Définir les conteneurs Windows Server, les conteneurs Hyper-V et les modes d'isolation
- Explorer Docker
- Préparer un hôte Windows Server 2019 au déploiement de conteneurs
- Sécurité, stockage et mise en réseau avec les conteneurs Windows

Module 25 : Planifier et déployer des machines virtuelles IaaS Windows Server

Ce module explique comment planifier et déployer des machines virtuelles IaaS Windows Server dans Azure. Vous apprendrez à décrire les ressources de calcul Azure, notamment les tailles et les séries de VM, ainsi que les niveaux Basic et Standard, à choisir les options de stockage sur disque appropriées, notamment les disques managés Standard HDD, Standard SSD et Premium SSD, à déployer des VM Azure à l'aide du portail Azure, d'Azure CLI et des modèles Azure Resource Manager (ARM), et à configurer des options supplémentaires, notamment Azure Automanage, afin d'appliquer les bonnes pratiques de gestion automatisée des VM.

- Décrire les ressources de calcul Azure
- Décrire le stockage des machines virtuelles
- Déployer des machines virtuelles Azure
- Créer une machine virtuelle Windows à l'aide du portail Azure

- Créer une machine virtuelle Windows à l'aide d'Azure CLI
- Déployer des machines virtuelles Azure à l'aide de modèles
- Décrire les options supplémentaires d'optimisation de la gestion des VM

Module 26 : Mettre en œuvre la montée en charge et la haute disponibilité avec les VM Windows Server

Ce module explique comment mettre en œuvre la montée en charge et la haute disponibilité des machines virtuelles Windows Server dans Azure. Vous apprendrez à décrire les groupes identiques de machines virtuelles (Virtual Machine Scale Sets) et leurs cas d'usage pour les charges de travail variables, à mettre en œuvre la mise à l'échelle horizontale (ajout et suppression de VM) et la mise à l'échelle verticale (augmentation des ressources des VM) à l'aide de règles automatisées basées sur des métriques, à configurer des machines virtuelles avec équilibrage de charge à l'aide d'Azure Load Balancer et de configurations IP front-end, à décrire les fonctionnalités d'Azure Site Recovery pour la reprise d'activité après sinistre et la continuité des activités, et à mettre en œuvre Azure Site Recovery afin de répliquer et de protéger les VM Azure.

- Décrire les groupes identiques de machines virtuelles (Virtual Machine Scale Sets)
- Mettre en œuvre la mise à l'échelle
- Mettre en œuvre l'équilibrage de charge des VM
- Créer un groupe identique de machines virtuelles dans le portail Azure
- Décrire Azure Site Recovery
- Mettre en œuvre Azure Site Recovery

Module 27 : Mettre en œuvre l'adressage IP et le routage des VM IaaS Windows Server

Ce module explique comment mettre en œuvre l'adressage IP et le routage pour les machines virtuelles IaaS Windows Server dans Azure. Vous apprendrez à mettre en œuvre des réseaux virtuels Azure (VNet) avec des sous-réseaux et des espaces d'adressage IP privés, à configurer des adresses IP privées et publiques à l'aide de méthodes d'allocation dynamique et statique, à gérer les interfaces réseau et à attribuer des configurations IP lors de la création des VM, à comprendre les routes système et à mettre en œuvre des routes définies par l'utilisateur afin de personnaliser les flux de trafic entre les sous-réseaux et les réseaux, ainsi qu'à mettre en œuvre IPv6 pour Azure VNet afin de prendre en charge une connectivité réseau double pile.

- Mettre en œuvre un réseau virtuel
- Mettre en œuvre l'adressage IP des VM IaaS
- Attribuer et gérer les adresses IP
- Configurer une adresse IP privée pour une machine virtuelle à l'aide du portail Azure
- Créer une machine virtuelle avec une adresse IP publique statique à l'aide du portail Azure
- Mettre en œuvre le routage IP des VM IaaS
- Mettre en œuvre IPv6 pour les machines virtuelles IaaS Windows Server

Module 28 : Mettre en œuvre la sécurité réseau des VM IaaS Windows Server

Ce module explique comment mettre en œuvre la sécurité réseau des machines virtuelles IaaS Windows Server dans Azure. Vous apprendrez à configurer des groupes de sécurité réseau (NSG) avec des règles de sécurité entrantes et sortantes, un traitement basé sur les priorités et des règles par défaut, à déployer et configurer Azure Firewall pour le filtrage centralisé du trafic réseau, à configurer Pare-feu Microsoft Defender avec fonctions avancées de sécurité pour assurer la protection au niveau de l'hôte, à choisir la solution de filtrage la plus appropriée parmi les NSG, Azure Firewall et Pare-feu Microsoft Defender, et à utiliser Azure Network Watcher pour capturer le trafic réseau et journaliser les flux réseau à des fins de diagnostic.

- Mettre en œuvre les groupes de sécurité réseau et les VM IaaS Windows
- Mettre en œuvre Azure Firewall avec les VM IaaS Windows
- Mettre en œuvre le Pare-feu Windows avec les VM IaaS Windows Server
- Choisir la solution de filtrage appropriée
- Déployer et configurer Azure Firewall à l'aide du portail Azure
- Capturer le trafic réseau avec Azure Network Watcher
- Journaliser le trafic réseau entrant et sortant d'une VM à l'aide du portail Azure

Module 29 : Administrer et gérer à distance une machine virtuelle IaaS Windows Server

Ce module explique comment administrer et gérer à distance des VM IaaS Windows Server dans Azure. Vous apprendrez à sélectionner l'outil d'administration à distance le plus adapté parmi le portail Azure, Windows Admin Center, Azure PowerShell, Azure CLI et Azure Cloud Shell, à vous connecter de manière sécurisée aux VM Azure à l'aide d'Azure Bastion sans exposer d'adresses IP publiques, et à configurer l'accès Just-In-Time (JIT) aux VM via Microsoft Defender for Cloud afin de verrouiller les ports d'administration entrants et de réduire la surface d'attaque.

- Sélectionner l'outil d'administration à distance approprié
- Gérer les machines virtuelles Windows avec Azure Bastion
- Créer un hôte Azure Bastion
- Configurer l'administration Just-In-Time (JIT)

Module 30 : Mettre en œuvre le DNS sous Windows Server
Ce module explique comment déployer et configurer le rôle Serveur DNS dans Windows Server. Vous apprendrez le fonctionnement de la résolution de noms DNS, à créer et gérer des zones de recherche directe et inverse à l'aide d'un stockage standard basé sur des fichiers ou intégré à Active Directory, à configurer les étendues de réplication des zones et les transferts de zone entre serveurs principal et secondaire, ainsi qu'à mettre en œuvre des stratégies de transfert, notamment les redirecteurs, les redirecteurs conditionnels et les zones de stub, afin de résoudre les noms au-delà des limites de domaine.

- Explorer l'architecture DNS
- Travailler avec les zones et les enregistrements DNS
- Installer et configurer le rôle DNS
- Mettre en œuvre le transfert DNS

Module 31 : Mettre en œuvre DNS pour les VM IaaS Windows Server
Ce module explique comment mettre en œuvre DNS pour les VM IaaS Windows Server dans Azure. Vous apprendrez à décrire Azure DNS, notamment son réseau anycast, son intégration avec le contrôle d'accès en fonction du rôle (RBAC) et ses limitations actuelles, telles que l'absence de prise en charge de DNSSEC, à configurer des zones DNS publiques Azure avec délégation et jeux d'enregistrements, à mettre en œuvre des zones DNS privées Azure avec liaison aux VNet et enregistrement automatique des enregistrements d'hôtes des VM, à déployer Windows Server DNS sur des VM IaaS Azure pour des scénarios intégrés à AD DS, à mettre en œuvre le DNS à horizon partagé (split-horizon DNS) afin de fournir des enregistrements différents aux clients internes et externes, et à résoudre les problèmes DNS dans les environnements Azure.

- Comprendre Azure DNS
- Mettre en œuvre Azure DNS
- Créer une zone DNS Azure et un enregistrement à l'aide du portail Azure
- Mettre en œuvre DNS avec des machines virtuelles IaaS Azure
- Mettre en œuvre le DNS à horizon partagé (split-horizon DNS) dans Azure
- Résoudre les problèmes DNS

Module 32 : Sécuriser le DNS sous Windows Server
Ce module explique comment sécuriser le DNS sous Windows Server afin de protéger votre infrastructure de résolution de noms. Vous apprendrez à mettre en œuvre le DNS à horizon partagé (split-horizon DNS) pour séparer le DNS interne intégré à Active Directory des serveurs DNS exposés à Internet, à créer des stratégies DNS pour des scénarios tels que la gestion du trafic, le routage basé sur la géolocalisation, l'équilibrage de charge des applications et le DNS split-brain, à mettre en œuvre et gérer des stratégies DNS à l'aide de cmdlets PowerShell afin d'assurer un contrôle granulaire des requêtes et des transferts de zone, à appliquer des fonctionnalités de sécurité DNS telles que le verrouillage du cache, le pool de sockets DNS et la limitation du débit des réponses, ainsi qu'à mettre en œuvre DNSSEC pour signer cryptographiquement les zones DNS et se protéger contre l'usurpation et l'altération du cache DNS.

- Mettre en œuvre le DNS à horizon partagé (split-horizon DNS)
- Créer des stratégies DNS
- Mettre en œuvre des stratégies DNS
- Sécuriser le DNS sous Windows Server
- Mettre en œuvre DNSSEC

Module 33 : Déployer et gérer DHCP
Ce module explique comment déployer et gérer le protocole DHCP (Dynamic Host Configuration Protocol) dans Windows Server. Vous apprendrez comment DHCP automatise la configuration IP à l'aide du processus d'attribution de bail en quatre étapes (DISCOVER, OFFER, REQUEST, ACK) et du renouvellement des baux, à installer et configurer le rôle Serveur DHCP, y compris l'autorisation du serveur dans AD DS, à configurer les options DHCP au niveau du serveur, de l'étendue et des réservations pour les serveurs DNS, les passerelles par défaut et d'autres paramètres, à créer et gérer des étendues DHCP avec des plages d'adresses, des exclusions et des réservations, à sélectionner des options de haute disponibilité, notamment le basculement DHCP (DHCP Failover) en mode veille à chaud (hot standby) et en mode équilibrage de charge, ainsi qu'à mettre en œuvre DHCP Failover pour assurer la tolérance aux pannes sur plusieurs serveurs DHCP.

- Utiliser DHCP pour simplifier la configuration IP
- Installer et configurer le rôle DHCP
- Configurer les options DHCP
- Configurer les étendues DHCP
- Sélectionner les options de haute disponibilité DHCP
- Mettre en œuvre DHCP Failover

Module 34 : Mettre en œuvre IP Address Management (IPAM)

Ce module explique comment déployer et utiliser IP Address Management (IPAM) dans Windows Server. Vous apprendrez à installer IPAM sur un serveur membre dédié avec un stockage WID ou SQL Server, à configurer l'approvisionnement basé sur des GPO pour la découverte des serveurs DHCP, DNS et des contrôleurs de domaine, à gérer les zones et les enregistrements DNS, les étendues DHCP et DHCP Failover, ainsi que les blocs et plages d'adresses IP à partir d'une console unique, et à contrôler les accès à l'aide des rôles RBAC intégrés et des étendues d'accès.

- Définir IP Address Management (IPAM)
- Déployer IP Address Management (IPAM)
- Administrer IP Address Management (IPAM)
- Configurer les options d'IP Address Management (IPAM)
- Gérer les zones DNS avec IP Address Management (IPAM)
- Gérer les serveurs DHCP avec IP Address Management (IPAM)
- Utiliser IP Address Management (IPAM) pour gérer l'adressage IP

Module 35 : Mettre en œuvre l'adressage IP et le routage des VM IaaS Windows Server

Ce module explique comment mettre en œuvre l'adressage IP et le routage pour les machines virtuelles IaaS Windows Server dans Azure. Vous apprendrez à mettre en œuvre des réseaux virtuels Azure (VNet) avec des sous-réseaux et des espaces d'adressage IP privés, à configurer des adresses IP privées et publiques à l'aide de méthodes d'allocation dynamique et statique, à gérer les interfaces réseau et à attribuer des configurations IP lors de la création des VM, à comprendre les routes système et à mettre en œuvre des routes définies par l'utilisateur afin de personnaliser les flux de trafic entre les sous-réseaux et les réseaux, ainsi qu'à mettre en œuvre IPv6 pour Azure VNet afin de prendre en charge une connectivité réseau double pile.

- Mettre en œuvre un réseau virtuel
- Mettre en œuvre l'adressage IP des VM IaaS
- Attribuer et gérer les adresses IP
- Configurer une adresse IP privée pour une machine virtuelle à l'aide du portail Azure
- Créer une machine virtuelle avec une adresse IP publique statique à l'aide du portail Azure
- Mettre en œuvre le routage IP des VM IaaS
- Mettre en œuvre IPv6 pour les machines virtuelles IaaS Windows Server

Module 36 : Mettre en œuvre une infrastructure de serveurs de fichiers hybride

Ce module explique comment mettre en œuvre une infrastructure de serveurs de fichiers hybride à l'aide d'Azure Files et d'Azure File Sync. Vous apprendrez à créer et configurer des partages de fichiers Azure avec une authentification basée sur l'identité et des autorisations NTFS, à déployer Azure File Sync avec Storage Sync Service, des groupes de synchronisation et des points de terminaison serveur, à configurer des stratégies de hiérarchisation vers le cloud afin de conserver en cache localement les fichiers fréquemment utilisés tout en plaçant les fichiers moins utilisés dans Azure, et à migrer de DFS Replication vers Azure File Sync.

- Décrire les services Azure Files
- Configurer Azure Files
- Configurer la connectivité à Azure Files
- Décrire Azure File Sync
- Mettre en œuvre Azure File Sync
- Déployer Azure File Sync
- Déployer Azure File Sync (2)
- Gérer la hiérarchisation vers le cloud
- Migrer de DFS Replication (DFSR) vers Azure File Sync

Module 37 : Gérer les serveurs de fichiers Windows Server

Ce module explique comment configurer et gérer le rôle Serveur de fichiers dans Windows Server. Vous apprendrez à utiliser les systèmes de fichiers NTFS et ReFS, à configurer File Server Resource Manager (FSRM) pour la gestion des quotas, le filtrage des fichiers, les rapports de stockage et la classification, à configurer les fonctionnalités SMB 3.x, notamment le chiffrement, SMB Multichannel et SMB Direct pour un accès haute performance aux fichiers, à désactiver SMB 1.0 afin de corriger les vulnérabilités de sécurité, et à utiliser le service Volume Shadow Copy Service (VSS) pour les opérations de sauvegarde et de capture instantanée.

- Définir le système de fichiers Windows Server
- Identifier les avantages et les cas d'usage de File Server Resource Manager (FSRM)
- Définir SMB et ses considérations de sécurité
- Configurer le protocole SMB
- Définir le service Volume Shadow Copy Service (VSS)

Module 38 : Mettre en œuvre Storage Spaces et Storage Spaces Direct

Ce module explique comment mettre en œuvre Storage Spaces et Storage Spaces Direct dans Windows Server. Vous apprendrez à créer des pools de stockage à partir de disques

physiques et à configurer des disques virtuels avec une résilience de type simple, miroir ou parité, à utiliser des niveaux de stockage pour combiner des SSD et des HDD, à choisir entre un provisionnement fixe et un provisionnement dynamique (thin provisioning), et à déployer Storage Spaces Direct pour un stockage hyperconvergé à l'aide des Cluster Shared Volumes (CSV), du Software Storage Bus et de ReFS, configurés via Windows Admin Center ou PowerShell.

- Définir l'architecture de Storage Spaces et ses composants
- Identifier les fonctionnalités, les avantages et les cas d'usage de Storage Spaces
- Mettre en œuvre Storage Spaces
- Identifier les fonctionnalités, les composants, les avantages et les cas d'usage de Storage Spaces Direct
- Mettre en œuvre Storage Spaces Direct

Module 39 : Mettre en œuvre la déduplication des données dans Windows Server

Ce module explique comment mettre en œuvre la déduplication des données dans Windows Server. Vous apprendrez comment la déduplication remplace les blocs de données dupliqués par des références vers un magasin de blocs (chunk store), à identifier les candidats idéaux tels que les documents utilisateurs, les bibliothèques VDI, les partages de déploiement logiciel et les volumes de sauvegarde, à installer et activer la déduplication à l'aide de Windows Admin Center, du Gestionnaire de serveur ou de PowerShell, à configurer les types d'utilisation et les planifications d'optimisation, ainsi qu'à exécuter des tâches d'optimisation, de collecte des déchets (garbage collection) et de vérification de l'intégrité des données (scrubbing).

- Définir l'architecture, les composants et le fonctionnement de la déduplication des données
- Définir les cas d'usage et l'interopérabilité de la déduplication des données
- Mettre en œuvre la déduplication des données
- Gérer et maintenir la déduplication des données

Module 40 : Mettre en œuvre iSCSI dans Windows Server

Ce module explique comment mettre en œuvre le stockage en mode bloc iSCSI dans Windows Server. Vous apprendrez comment iSCSI utilise des réseaux TCP/IP standard pour fournir des fonctionnalités SAN sans nécessiter de câblage spécialisé, à installer et configurer le service de rôle iSCSI Target Server et à créer des disques virtuels à l'aide de PowerShell, à connecter des initiateurs iSCSI à des cibles, ainsi qu'à configurer la redondance réseau à l'aide de Multiple Connections per Session (MCS) et de Multipath I/O (MPIO) avec des stratégies d'équilibrage de charge.

- Identifier les fonctionnalités, les composants et les cas d'usage d'iSCSI
- Identifier les considérations relatives à la mise en œuvre d'iSCSI
- Mettre en œuvre iSCSI
- Configurer la haute disponibilité pour iSCSI

Module 41 : Mettre en œuvre Storage Replica dans Windows Server

Ce module explique comment mettre en œuvre Storage Replica dans Windows Server afin d'assurer la reprise d'activité après sinistre et la haute disponibilité. Vous apprendrez comment Storage Replica effectue une réplication au niveau des blocs entre des volumes à l'aide de groupes et de partenariats de réplication, à choisir entre les modes de réplication synchrone et asynchrone, à configurer des clusters de basculement étendus (stretch failover clusters) répartis sur deux sites physiques, à valider les prérequis avec Test-SRTopology, et à déployer la réplication à l'aide de Windows Admin Center ou de PowerShell avec la cmdlet New-SRPartnership.

- Identifier les fonctionnalités et les composants de Storage Replica
- Examiner les prérequis pour la mise en œuvre de Storage Replica
- Mettre en œuvre Storage Replica à l'aide de Windows Admin Center
- Mettre en œuvre Storage Replica à l'aide de Windows PowerShell