

Formation Windows Server 2022/2025 Sécurité

Durée de la formation : 4 jour(s)

OBJECTIFS

A l'issue de la formation le participant sera capable de :

Définir les risques et les vulnérabilités

Apprendre à implémenter et configurer une PKI

Comprendre comment sécuriser Active Directory et les authentifications

Pouvoir sécuriser les services réseaux et les connexions

Savoir sécuriser les données

Savoir durcir les serveurs IIS

Comprendre comment implémenter et configurer WSUS

Normaliser les systèmes pour mieux les connaître et mieux les gérer

Apprendre à implémenter des restrictions logicielles

Disposer des connaissances nécessaires pour sécuriser Hyper-V et les machines virtuelles

Savoir surveiller et auditer les systèmes

PREREQUIS

Avoir de bonnes connaissances des systèmes Windows et de PowerShell.

Un entretien en amont avec notre expert permet de prendre en compte le profil de chaque participant (niveau, objectifs et résultats attendus, contexte professionnel, enjeux...) et d'adapter le contenu de la formation si besoin.

Cette formation ne peut être financée que dans le cadre d'un projet d'entreprise (prise en charge entreprise ou OPCO). Les dossiers à financement personnel et CPF ne sont pas pris en compte.

PUBLIC

RSSI, administrateurs Windows, architectes d'infrastructure et de système, ingénieurs systèmes

Formation Windows Server 2022/2025 Sécurité

Durée de la formation : 4 jour(s)

PROGRAMME

Introduction à la sécurité

État des vulnérabilités et mauvaises pratiques
Les risques
Principaux types et vecteurs d'attaques

Mettre en place une infrastructure de clé publique (PKI)

Vue d'ensemble d'une PKI
Déployer et configurer une PKI (autorité de certification, CRL, répondeur en ligne, ...)
Définir et gérer les modèles de certificats
Gérer, surveiller et révoquer les certificats
Audit et surveillance d'une PKI

Sécuriser les authentifications et Active Directory

Vues d'ensemble des méthodes d'authentification
Réorganisation de la structure Active Directory et bonnes pratiques d'administration
Mettre en oeuvre des hôtes d'administration sécurisés
Durcissement des authentifications (bloquer les protocoles à risques et la négociation d'authentification, ...), stratégies et silos d'authentification
Usage et configuration des RODC
Autorisations et délégations dans l'annuaire
Stratégies de mots de passe
Gestion de l'accès privilégié
Mettre en oeuvre LAPS pour les mots de passe
Administrateurs locaux et points d'attention liés à LAPS
Les stratégies de groupe pour la sécurité des systèmes et stratégies de sécurité
Bonnes et mauvaises pratiques liées aux stratégies de groupe
Administration sécurisée avec PowerShell JEA
Auditer et surveiller les authentifications, les tickets Kerberos et Active Directory

Sécuriser les services réseau et les connexions

Sécuriser les serveurs DNS
Mettre en oeuvre DNSSec
Définir des stratégies DNS
Désactiver NetBIOS par DHCP ou par GPO
Configurer le pare-feu
Mettre en oeuvre IPSec

Sécuriser les serveurs de fichiers et les données

Rappels sur les autorisations NTFS
Rappels sur le gestionnaire de ressources du serveur de fichiers (FSRM) et filtrages
Inexploité mais précieux contrôle d'accès dynamique
Présentation d'AD RMS
Sécuriser le trafic SMB

Formation Windows Server 2022/2025 Sécurité

Durée de la formation : 4 jour(s)

Utiliser le chiffrement EFS, avantages, inconvénients et récupération
Mettre en oeuvre BitLocker et options avancées (déverrouillage réseau, ...), de la nécessité de chiffrer aussi les serveurs
Gérer la récupération BitLocker

Sécuriser les serveurs IIS

Déplacer les dossiers de site sur une partition dédiée
Configurer les authentifications et authentifications basées sur un serveur RADIUS
Définir des restrictions IP dynamiques des requêtes
Restreindre les requêtes autorisées sur le serveur
Configurer ou forcer HTTPS
Choisir la réécriture des requêtes HTTP en HTTPS et HSTS, avantages et inconvénients
Isoler les sites avec un pool d'application dédié
Limiter les accès anonymes au pool d'application
Sécurisation NTFS des dossiers physiques des sites

Mettre à jour les systèmes

Configurer un serveur WSUS
Paramétrages avancés et sécurisation
Rapports WSUS et limites
Gérer les mises à jour applicatives non Microsoft

Normaliser les systèmes

Installer et gérer un serveur en installation minimale
Mettre en oeuvre la sécurité basée sur la virtualisation (Credential Guard, Device Guard)
Utiliser PowerShell DSC pour unifier les configurations et sécuriser les systèmes
Exploiter le Security Compliance Toolkit
Audit et surveillance générale des systèmes

Restreindre les applications autorisées

Restrictions logicielles ou AppLocker ?
Mettre en oeuvre AppLocker et les restrictions logicielles
Exploiter des stratégies d'intégrité de code avec PowerShell
Surveiller les applications

Sécuriser la virtualisation Hyper-V

Sécuriser Hyper-V
Sécuriser l'infrastructure virtuelle avec des hôtes gardés (Guarded Fabric)
Mettre en oeuvre des machines virtuelles blindées (Shielded VM)

Introduction à Microsoft Defender Advanced Threat Protection

Présentation de Microsoft Defender ATP
Implémenter et gérer Microsoft Defender ATP
Utiliser les recommandations de sécurité fournies par Microsoft Defender ATP

Formation Windows Server 2022/2025 Sécurité

Durée de la formation : 4 jour(s)

Surveiller et auditer les systèmes

- Configurer les audits selon les types de serveurs
- Configurer les journaux et leur archivage, durée de conservation
- Centraliser les journaux, solution Microsoft ou tierce
- Mise en oeuvre de la solution Microsoft
- Analyser les accès
- Les événements à prioriser

Formation Windows Server 2022/2025 Sécurité

Durée de la formation : 4 jour(s)

Prise en compte du handicap

Pour les personnes en situation de handicap, afin de nous permettre d'organiser le déroulement de la formation dans les meilleures conditions possibles, contactez-nous via notre formulaire de contact ou par mail (formation@access-it.fr) ou par téléphone (0320619506). Un entretien avec notre référente handicap pourra être programmé afin d'identifier les besoins et aménagements nécessaires.

Modalités et moyens Pédagogiques, techniques et d'encadrement mis en œuvre

Répartition théorie/pratique : 45%/55%. Cette formation se compose d'une alternance d'apports théoriques, de travaux pratiques s'articulant autour d'une application fil rouge, de démonstrations, de phases d'échanges entre participants et de synthèses de la part du formateur.

Formation accessible à distance de n'importe où et n'importe quand, via un ordinateur type PC disposant d'une connexion à Internet à haut débit (ADSL ou plus).

Pour assurer un démarrage dans les meilleures conditions au premier jour de la formation, notre service logistique se met systématiquement en relation, en amont, avec vous afin de réaliser un test de validation technique et de vous présenter l'environnement de formation.

Pendant toute la durée de la formation, le stagiaire dispose d'une assistance technique et pédagogique illimitée, par e-mail, avec un délai de prise en compte et de traitement qui n'excède pas 24h. En complément, le stagiaire peut planifier un rendez-vous pédagogique avec un formateur expert afin d'échanger sur des éléments de la formation.

La durée de la formation affichée sur cette page est une durée estimée qui peut varier en fonction du profil du stagiaire et de ses objectifs (notamment s'il souhaite valider sa formation par le passage d'un examen de certification).

Durant la formation, le formateur prévoit :

Des démonstrations organisées en modules et en séquences découpées le plus finement possible, en suivant le programme pédagogique détaillé sur cette page ;

Des énoncés et corrigés de travaux pratiques à réaliser tout au long de la formation ;

Des travaux pratiques sont proposés ; la plateforme prévoit l'environnement technique nécessaire à la réalisation de l'ensemble des travaux pratiques ;

Le formateur valide les connaissances acquises après chaque TP ;

Il est proposé un ou plusieurs livres numériques faisant office d'ouvrage(s) de référence sur le thème de la formation.

Validation et sanction de la formation

Une attestation mentionnant les objectifs, la nature et la durée de l'action et les résultats de l'évaluation des acquis de la formation sera remise au stagiaire à l'issue de sa formation par courrier électronique.

A la demande, il sera délivré un certificat de réalisation.

Type de formation

Professionalisante ayant pour objectif le perfectionnement, l'élargissement des compétences

Moyens permettant de suivre l'exécution de l'action

Le contrôle de la présence des stagiaires sera assuré par la vérification de l'assiduité des participants. Le stagiaire signera une feuille de présence par demi-journée de formation. Celle-ci sera également signée par le formateur.

Modalité d'évaluation des acquis

Durant la formation, le participant est amené à mettre en pratique les éléments du cours par la réalisation de travaux pratiques réalisés sur PC.

La validation des acquis du stagiaire est faite par le formateur à la fin de chaque atelier. Cette validation individuelle est possible du fait du faible nombre de participants par session de formation (6 personnes maximum).

A la fin de la formation, le stagiaire a donc atteint les objectifs fixés par la formation.

En complément, pour les stagiaires qui le souhaitent, certaines formations peuvent être validées officiellement par l'éditeur en passant un examen de certification.

Access it étant centre d'examen ENI, les examens peuvent être réalisés sur demande à distance ou dans nos locaux de Villeneuve d'Ascq.

Les candidats à la certification doivent produire un travail personnel important en vue de se présenter au passage de l'examen, le seul suivi de la formation ne constitue pas un élément suffisant pour garantir un bon résultat et/ou l'obtention de la certification

Assistance Post-Formation

Toute personne ayant suivi une formation avec Access it bénéficie d'une assistance post-formation d'une durée de 1 mois. Ce nouveau service d'accompagnement permet aux stagiaires rencontrant des difficultés dans la mise en œuvre des connaissances acquises de solliciter l'aide de nos formateurs sur des aspects relatifs aux programmes de formation suivis. Pour en bénéficier, il suffit de se rendre sur la page contact de notre site web et de remplir le formulaire. Une réponse est apportée par mail ou par téléphone dans un délai de 48 heures.

Centre d'Examen

Notre centre de formation agréé Qualiopi bénéficie de l'agrément d'ENI et ICDL pour les certifications informatiques. C'est pour nos clients la garantie de pouvoir suivre des formations préparant à des certifications professionnelles.

Aide à l'orientation

Pour chacune des grandes thématiques couvertes par notre offre de formation, nous proposons via nos spécialistes un rendez-vous physique ou téléphonique qui via un diagnostic permettra aux personnes souhaitant être accompagnées dans le choix d'un programme ou dans la définition d'un parcours de formation une orientation vers les programmes les plus adaptés à leurs besoins et à leur niveau.

Aspects Pratiques

Dès leur inscription, les participants sont contactés par nos services qui s'assurent que les débits internet constatés sur le lieu depuis lequel ils souhaitent se former sont suffisants pour suivre la formation dans des conditions optimales.

À l'occasion de cet appel, nos experts s'assurent également qu'ils disposent du matériel nécessaire pour suivre la formation (PC Portable, webcam, Micro-casque..).

Avant le début de la formation, les participants reçoivent un lien leur permettant d'accéder à la classe virtuelle et leurs identifiants personnels de connexion. Un aide à l'utilisation de la solution de visioconférence utilisée leur est également proposée.

Le jour de la formation, ils se connectent à la classe virtuelle depuis leur navigateur internet. Ils voient et entendent le formateur ainsi que les autres participants et peuvent à tout moment communiquer avec eux.

Ils participent aux échanges et réalisent les ateliers dans les mêmes conditions que s'ils étaient en salle. Grâce à nos outils de prise en main à distance, les formateurs peuvent à tout moment prendre la main sur leurs postes pour les aider ou vérifier leurs TP.

Tout au long de la formation, les participants peuvent bénéficier de l'assistance immédiate de nos experts en composant le numéro qui leur a été communiqué avant la formation.

Des bilans intermédiaires ont lieu en présence des participants du formateur et du référent pédagogique d'Access it afin de vérifier l'état d'avancement de la session, les difficultés rencontrées et permettre d'éventuels actions correctives.

Bénéfices pour les participants

Se former depuis leur lieu de travail ou leur domicile,

Accéder sans se déplacer à la qualité d'une formation interentreprise par un formateur consultant ayant une expérience probante sur le sujet animé.

Bénéficier à distance de la richesse d'une formation interentreprises : échanges avec le formateur et les autres participants, partages d'expériences, ateliers pratiques...

Pouvoir se former en toutes circonstances et notamment en cas d'imprévus.

Bénéfices pour l'entreprise

Optimiser ses budgets en limitant les frais de déplacement et d'hébergement.

Proposer à tous ses collaborateurs, quelle que soit leur situation géographique, des formations de qualité (en Inter comme en Intra).

Limiter les temps de déplacement.

Proposer davantage de choix dans les formations à des collaborateurs peu mobiles.

Assurer la montée en compétences de ses collaborateurs quelles que soient les circonstances