

Certification Microsoft - Securing Windows Server 2016 (70-744)

CATEGORIE : B

Vue d'ensemble

Domaine(s) d'activité professionnel dans lequel(s) est utilisé la certification :

Transverse : ■ **Entreprises de tout secteur d'activité qui utilise des serveurs Microsoft Windows**

Code(s) NAF : —

Code(s) NSF : **326**

Code(s) ROME : **M1810**, **M1802**, **M1801**, **M1401**

Formacode : —

Date de création de la certification : **15/12/2016**

Mots clés : **sécurité serveurs**, **windows server**, **SECURITE DE L'INFORMATION**, **microsoft**

Identification

Identifiant : **3608**

Version du : **16/10/2018**

Références

Consensus, reconnaissance ou recommandation :

Formalisé :

- [Détail sur le programme de certification Microsoft sur le site de l'éditeur](#)

Non formalisé :

- [Témoignages sur la certification Microsoft](#)
- [Pourquoi passer la certification sur les produits et les technologies Microsoft ?](#)

Norme(s) associée(s) :

—

Descriptif

Objectifs de l'habilitation/certification

L'examen de certification Microsoft « Securing Windows Server 2016 (70-744) » s'adresse aux professionnels réseaux et valide une compétence complémentaire essentielle en sécurité.

Les candidats à cet examen ont pour mission de sécuriser les environnements Windows Server 2016. Ils connaissent les méthodes et les technologies utilisées pour renforcer les environnements de serveurs et sécuriser les infrastructures de machines virtuelles..

En réussissant la certification *Securing Windows Server 2016*, les candidats démontrent qu'ils sont en mesure d'utiliser des solutions de détection des menaces telles que l'audit d'accès, la mise en œuvre d'Advanced Threat Analytics (ATA), le déploiement de solutions Operations Management Suite (OMS) et l'identification de solutions pour des charges de travail spécifiques. L'examen évalue également leurs capacités à gérer la protection des infrastructures Active Directory et Identity, à gérer les identités privilégiées en utilisant les approches Just in Time (JIT) et Just Enough Administration (JEA), ainsi que les PAW (Privileged Access Workstation) et les serveurs sécurisés utilisant la solution Local Administrator Password (LAPS).

Lien avec les certifications professionnelles ou les CQP enregistrés au RNCP

- 17840
- 7440

■ 4245

Descriptif général des compétences constituant la certification

Les compétences visées et évaluées par la certification se répartissent en plusieurs grands champs d'intervention qui constituent tout ou partie des missions de l'expert en sécurité des serveurs d'administration Windows, toutes ayant pour but de protéger les données de l'entreprise :

- Mettre en œuvre des solutions qui renforcent la protection du serveur réseau de l'entreprise
- Sécuriser une infrastructure de Virtualisation et une infrastructure réseau pour empêcher toute attaque de l'extérieur
- Gérer les identités privilégiées et les accès utilisateurs, en fonction des droits de chaque service pour garantir l'intégrité des données de l'entreprise
- Mettre en œuvre des solutions de détection des menaces (attaques), pour anticiper les actions défensives
- Implémenter la sécurité spécifique à la charge de travail, afin d'optimiser les opérations exécutées par tout service dans l'entreprise sans perturbation

Modalités générales

La préparation à cet examen se base sur le suivi d'une formation officielle de 35 Heures (incluant support de cours et labs) ainsi qu'un travail personnel. Il est conseillé de respecter un temps de révision après la formation avant de passer l'examen.

De nombreux outils de préparation existent en complément, comme le MOC-On demand (formation au format vidéo, incluant des labs), le Practice test (test d'entraînement au passage de la certification), et autres ressources en ligne sur les sites de l'éditeur.

La certification Microsoft « Securing Windows Server 2016 (70-744) » est ouverte à tout public. Le suivi de la formation officielle n'est pas obligatoire pour la validation du titre de certification, mais elle est toutefois recommandée puisqu'elle met en pratique les connaissances à acquérir.

Liens avec le développement durable

Aucun

Public visé par la certification

Tous publics

Valeur ajoutée pour la mobilité professionnelle et l'emploi

Pour l'individu

L'ANSSI (l'autorité nationale française de sécurité des systèmes d'information) écrit sur son site : La formation et le recrutement d'experts en cybersécurité est un enjeu majeur pour le développement de notre société connectée. Former les nouvelles générations de professionnels n'est pas le seul défi à relever. Intégrer des connaissances de base (...) dans les circuits de formation en entreprise est l'une des conditions d'une transition numérique réussie. C'est pourquoi le professionnel certifié en sécurité sur les serveurs

Pour l'entité utilisatrice

Les entités utilisatrices disposant de professionnels certifiés en sécurité sur Windows Server sont assurées de garantir à leurs utilisateurs la disponibilité du système d'information et la protection des données.

Pour les entités dont l'activité commerciale est de revendre, intégrer ou préconiser des solutions réseaux Microsoft Windows Server, l'intégration d'un professionnel certifié en sécurité Windows lui permet de satisfaire les pré-requis techniques du

Windows 2016 peut rassurer l'entreprise qui l'emploie en garantissant un haut niveau de protection de son système d'informations.

Grâce à la création par l'éditeur de badges numériques, chaque professionnel certifié peut afficher son expertise via son CV, son blog ou ses réseaux professionnels. L'affichage des compétences via ce badge est un vecteur de recrutement grâce à l'octroi de services supplémentaires.

programme de partenariat Microsoft, d'assurer aux clients utilisateurs une expertise technique et un savoir-faire, et d'acquérir ainsi un réel avantage concurrentiel.

Evaluation / certification

Pré-requis

Aucun en termes de niveau scolaire.

Au préalable de sa préparation au passage de l'examen, le candidat devra être en mesure de comprendre les fondamentaux du réseau tels que TCP/IP, UDP, DNS, des principes de AD DS et les fondamentaux de la virtualisation avec Hyper-V.

Compétences évaluées

Les compétences visées et évaluées par la certification se répartissent en plusieurs grands champs d'intervention qui constituent tout ou partie des missions de l'expert en sécurité des serveurs d'administration Windows. Le pourcentage indiqué pour chaque compétence représente la proportion des questions permettant de valider cette compétence :

Mettre en œuvre des solutions qui renforcent la protection du serveur (25-30%)

Configurer le chiffrement de disques et de fichiers à partir des exigences matérielles et logicielles pour la fonctionnalité de démarrage sécurisé et de clé de chiffrement; implémenter le processus de récupération BitLocker en utilisant des solutions de récupération de mot de passe

Mettre en place une protection contre les logiciels malveillants avec Windows Defender

Protéger les informations d'identification

Créer des lignes de base de sécurité

Sécuriser une infrastructure de Virtualisation (5-10%)

Configurer le service de protection des clés et migrer les machines virtuelles blindées vers d'autres hôtes protégés, les dépanner les hôtes protégés le cas échéant

Certificateur(s)

- MICROSOFT

Centre(s) de passage/certification

- Centres Pearson VUE - accessibles depuis <http://www.pearsonvue.com/microsoft/locate/>

Déterminer les exigences et les scénarios pour l'implémentation de machines virtuelles blindées, incluant le chiffrement des disques de données, dépanner les machines virtuelles protégées et cryptées

Sécuriser une infrastructure réseau (10-15%)

Configurer le pare-feu Windows pour la sécurité avancée, dont les règles de sécurité de connexion, de la console de gestion de l'interface graphique ou de Windows PowerShell, pour autoriser ou refuser les applications, les étendues, les ports et les utilisateurs.

Implémenter un pare-feu de Datacenter Software Defined en déterminant les exigences et les scénarios d'utilisation

Configurer les options d'authentification IPsec et les règles de sécurité de connexion

Gérer les identités privilégiées et les accès utilisateurs en fonction des droits de chaque service pour garantir l'intégrité des données de l'entreprise (25-30%)

Implémenter l'administration « juste-à-temps » (JIT)

Implémenter le « Just-Enough-Administration » (JEA)

Implémenter les postes de travail avec accès privilégié (PAW) et les attributions de droits utilisateur

Configurer les stratégies de groupe pour affectation des droits utilisateur, configurer les paramètres des options de sécurité dans la stratégie de groupe, activer et configurer l'accès au bureau à distance

Mettre en oeuvre la solution LAPS pour gérer les paramètres et les propriétés du mot de passe

Mettre en oeuvre des solutions de détection des menaces pour anticiper les actions défensives (15-20%)

Configurer des stratégies d'audit avancées

Installer et configurer Microsoft Advanced Threat Analytics (ATA) pour créer des alertes lorsqu'une activité suspecte est détectée; examiner et modifier les activités suspectes sur la ligne de temps d'attaque

Déterminer les solutions de détection des menaces à l'aide d'Operations Management Suite (OMS)

Implémenter la sécurité spécifique à la charge de travail, afin d'optimiser les opérations exécutées par tout service dans l'entreprise sans perturbation (5-10%)

Sécuriser le développement des applications sécurisées et une infrastructure de charge de travail serveur

Implémenter une infrastructure de services de fichiers sécurisée et un contrôle d'accès dynamique (DAC)

Niveaux délivrés le cas échéant (hors nomenclature des niveaux de formation de 1969)

Non Applicable

La validité est Permanente

Possibilité de certification partielle : non

Matérialisation officielle de la certification :

Les candidats reçoivent la notification de réussite/échec quelques minutes après la fin de l'examen et accède à un relevé de notes détaillé : son transcript est disponible à tout moment sur un portail sécurisé dédié.

Plus d'informations

Statistiques

Chaque année ce sont près de 10 000 personnes qui passent les Certifications Microsoft. Concernant l'examen de sécurité Windows Server, nous comptabilisons 1185 professionnels certifiés à fin janvier 2018.

Autres sources d'information

Présentation des certifications Microsoft disponible sur <https://www.microsoft.com/learning/fr-fr/certification-overview.aspx>