

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

RS3608 · RS · Publiée

L'essentiel

Code(s) NSF	326
Type d'enregistrement	Enregistrement sur demande
Date d'échéance	31/12/2021

Certificateur(s)

MICROSOFT FRANCE · SIRET : 32773318400516

Partenaires habilités

2 organismes habilités, d'après la liste publiée par France compétences : 2 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
EDITIONS ENI	40330342300038	Former et organiser l'évaluation
GLOBAL KNOWLEDGE NETWORK FRANCE	40394420000142	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

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).

COMPÉTENCES ATTESTÉES

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

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
- 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 œuvre 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)

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION

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.

Base légale

Date d'échéance de l'enregistrement 31/12/2021

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

Présentation des certifications Microsoft disponible sur

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rs/3608/>

Demande CPF — formations engagées

Dossiers CPF engagés	3
Montant total engagé	2 856 €
Coût moyen par dossier	952 €
Durée moyenne	12 h
Période	04/2020 – 12/2020
France compétences	100 %

Formations engagées via le CPF — Caisse des Dépôts (open data), tous organismes confondus.