IBM Certified Associate Administrator - Security Guardium Data Protection

CATEGORIE : B

Vue d'ensemble

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

Transverse : ■ **Transverse et tout secteur d'activités**

Tout type d'entreprise ou association ayant plusieurs postes informatisés, et entreprises du secteur informatique à partir d'une personne

Code(s) NAF : **62.02A**

Code(s) NSF : **326**

Code(s) ROME : **M1801**, **M1802**, **M1810**, **I1401**

Formacode : **31054**

Date de création de la certification : **13/04/2017**

Mots clés : **Données sensibles**, **Protection des données**, **Sécurité informatique**, **IBM Security Guardium**

Identification

Identifiant : **3353**

Version du : **19/02/2018**

Références

Consensus, reconnaissance ou recommandation :

Formalisé :

- [Détails sur les sites :](#)
- [*](#)
- [, rubrique certification IBM](#)
- [La recherche s'effectuera ensuite par mot-clé ou n° de test ou de certification sur le site en anglais des certifications IBM.](#)

Non formalisé :

- **N/A**

Norme(s) associée(s) :

—

Descriptif

Objectifs de l'habilitation/certification

IBM Security Guardium est une plateforme complète de sécurité des données qui offre une large gamme de fonctionnalités : détection et classification des données sensibles, évaluation des vulnérabilités, surveillance de l'activité des données et des fichiers, masquage, chiffrement, blocage, émission d'alertes et mise en quarantaine afin de protéger les données sensibles.

La certification IBM Certified Associate Administrator - Security Guardium Data Protection, de niveau débutant, s'adresse aux administrateurs spécialisés dans la sécurité des données et le déploiement.

Ils sont en mesure de faire fonctionner IBM Security Guardium Data Protection dans ses principes fondamentaux et d'assurer l'implémentation, la gestion et le support technique de base de cette solution.

La certification concerne les produits IBM Security Guardium Data Activity Monitor, IBM Security Guardium File Activity Monitor et IBM Security Guardium Vulnerability Assessment.

L'objectif est de familiariser ces administrateurs avec les fonctionnalités du produit et tous les composants du logiciel (agents et dispositifs).

De prime abord, cette certification n'est pas liée à une plateforme spécifique. Cependant, il existe quelques exceptions pour Linux, Unix, et Windows. Ces questions spécifiques sont traitées dans une documentation figurant sur la liste des ressources conseillées pour la formation.

Lien avec les certifications professionnelles ou les CQP enregistrés au RNCP

- 11554
- 7440

Descriptif général des compétences constituant la certification

La certification **IBM Certified Associate Administrator - Security Guardium Data Protection**, permettra au professionnel de se spécialiser dans l'administration de Security Guardium et d'acquérir les compétences suivantes autour de cette solution :

Installer et configurer Security Guardium
Déployer la solution
Gérer le logiciel
Apporter un soutien technique

Modalités générales

Pour la préparation de cette certification, deux présentations, une documentation produit, un guide de déploiement de la solution sous forme de Redbook, ainsi que de multiples ressources sont proposés et disponibles en ligne.

Un module de formation officielle de 3 jours est disponible.

La mise en place d'une formation sur-mesure assurée par un instructeur est également possible.

Liens avec le développement durable

Aucun

Public visé par la certification

- multiples : salariés, demandeurs d'emploi

Valeur ajoutée pour la mobilité professionnelle et l'emploi

Pour l'individu

Le professionnel certifié **IBM Certified Associate Administrator - Security Guardium Data Protection** met ses connaissances et ses compétences acquises dans le domaine de la protection des données au service de son entreprise.

Il prend en charge l'administration de la solution IBM Security Guardium Data Protection, son installation, sa configuration, son déploiement et assure par ailleurs son support technique.

Il implémente et gère IBM Security Guardium Data Protection, met en place les outils adaptés au contrôle de l'activité des données et des fichiers, ainsi que les produits spécifiques d'évaluation de la vulnérabilité.

Il valide à la fois des compétences techniques et une compréhension des enjeux business de l'entreprise.

Pour l'entité utilisatrice

Les produits IBM Security Guardium offrent l'avantage pour les entreprises de garantir la sécurité, la confidentialité et l'intégrité des informations de leur centre de données. Ces produits de sécurité des données prennent en charge les environnements hétérogènes, y compris les bases de données, les entrepôts de données, les partages de fichiers et les systèmes Hadoop pour les applications personnalisées et intégrées sur toutes les principales plateformes.

IBM Security Guardium aide les clients à prendre en charge une gamme complète de cas d'utilisation : initiatives de conformité et de confidentialité, sécurité du Big Data, lutte contre les menaces internes, et protection complète des données.

Avec l'aide d'un professionnel certifié **IBM Certified Associate Administrator - Security Guardium Data Protection**, l'entreprise pourra sauvegarder ses données sensibles grâce à IBM Security Guardium, solution fiable et simple d'utilisation qui

Dans un monde où les organisations se trouvent confrontées aux menaces croissantes qui pèsent sur leurs données stratégiques, se spécialiser dans Security Guardium constitue pour le professionnel un gage d'employabilité, ce produit phare lui offrant à la fois de larges opportunités de carrière, ainsi que des possibilités d'évolution dans tous les métiers de la sécurité informatique. Ces profils sont aujourd'hui très recherchés par les entreprises.

l'accompagnera de bout en bout dans la mise en place de la sécurité, analysant et ciblant de façon automatique ses données stratégiques, révélant les risques, assurant une protection complète de ses données les plus sensibles, s'adaptant tout en souplesse aux changements intervenant dans son environnement IT, qu'il s'agisse d'ajout de nouveaux utilisateurs, d'évolutivité ou d'intégration de nouvelles technologies.

Les sociétés de services partenaires d'IBM employant un spécialiste sécurité sur IBM Security Guardium Data Protection seront en mesure d'accompagner leurs clients dans la mise en œuvre de cette solution au sein de leur infrastructure.

Evaluation / certification

Pré-requis

Les connaissances de base suivantes sont requises pour réussir la certification :

Systèmes d'exploitation et bases de données
Réseaux et protocoles
Les principes fondamentaux du SQL
Les plateformes Linux, Unix et Windows

Compétences évaluées

Caractéristiques produit :

Exposer les fonctionnalités de base de Data Activity Monitoring (DAM) et de File Activity Monitoring (FAM)
Détecer les types de sources de données susceptibles d'être surveillés par Guardium
Présenter les caractéristiques de la fonction évaluation de la vulnérabilité et celles d'un rapport des droits d'accès aux bases de données
Souligner les différences entre classification des objets sensibles, découverte de bases de données, découverte de cas, et découverte à partir de File Activity Monitoring
Fournir des exemples de cas d'usage relatifs au contrôle d'accès du niveau des données, tels que blocage, mise en quarantaine, rédaction, réécriture de requêtes, en précisant leurs spécificités techniques
Révéler les fonctionnalités d'investigation étendues, telles que Outlier Detection (système de détection des données aberrantes), les tableaux de bord d'investigation et d'optimisation des droits, Eagle Eye (scan des menaces) et Quick Search

Architecture de la solution :

Recenser les principales exigences systèmes requises pour les dispositifs Guardium
Décrire les options de déploiement des dispositifs Guardium
Faire fonctionner un gestionnaire central, un agrégateur et un

Certificateur(s)

- IBM

Centre(s) de passage/certification

- De nombreux centres Pearson Vue France entière.

collecteur (y compris Deployment Health Topology)
Utiliser les agents de Guardium (par ex. S-TAP, File Activity Monitoring)
Mettre en évidence la flexibilité de Guardium
Démontrer la capacité de la solution Guardium à s'intégrer à d'autres produits

Installation et configuration :

Désigner les prérequis pour l'installation de l'agent
Désigner les prérequis pour les options sans agent (par ex. évaluation de la vulnérabilité, découverte)
Installer et procéder à la configuration initiale des dispositifs de Guardium, tels que collecteur, agrégateur, gestionnaire central
Installer et configurer les agents de Guardium, tels que S-TAP, GIM (Guardium Installation Manager)
Faire fonctionner les commandes de configuration CLI et grdapi pour installer les dispositifs Guardium (entre autres Syslog, SMTP, NTP)

Administration :

Maintenir en bon état de fonctionnement tous les composants de Guardium (à partir, entre autres, de Health Views, de rapports GUI)
Exécuter les diverses tâches de gestion des données : archiver, sauvegarder, importer, exporter, restaurer
Gérer les accès, créer des utilisateurs, gérer les privilèges, séparer les tâches
Mettre à niveau et corriger les composants de Guardium
Configurer les fonctions haute disponibilité et basculement
Configurer les mécanismes d'équilibrage de charge de Guardium

Surveillance de l'activité et rapports :

Exposer les types de politiques et les mesures
Instaurer des règles et des procédures en accord avec les objectifs de surveillance des données
Utiliser des groupes pour contrôler les règles et les rapports
Détailler les différents types de rapports (personnalisés et intégrés)
Générer des requêtes et des rapports personnalisés
Mettre en œuvre un processus d'audit automatisé
Configurer l'évaluation de la vulnérabilité

Résolution des problèmes techniques :

Utiliser les outils, les rapports et les tableaux de bord spécifiques aux diagnostics
Présenter les capacités d'auto-surveillance et d'alertes de Guardium
Récapituler les étapes d'un dépannage de l'agent
Contrôler les charges de travail des dispositifs
Réduire la charge de travail des dispositifs en adaptant les règles
Recueillir pour le support technique les informations des fichiers journaux utiles au dépannage de Guardium
Créer un rapport de gestion des problèmes (PMR)

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

N/A

La validité est Permanente

Possibilité de certification partielle : non

Matérialisation officielle de la certification :

Un Certificat électronique est envoyé par IBM aux candidats ayant réussi, ainsi qu'une carte professionnelle lors du 1er examen réussi. Le candidat accède à son transcript à tout moment sur un portail sécurisé dédié.

Plus d'informations

Statistiques

Le programme de certification professionnelle IBM existe depuis plus de 15 ans et compte, sur le territoire national, entre 1000 et 2000 nouveaux certifiés par an, toutes certifications confondues.

En France, sur les 2 dernières années, une centaine de personnes ont obtenu une certification IBM dans le domaine de la **Sécurité informatique**. IBM Security Guardium constitue un produit phare en la matière.

La protection des données constitue aujourd'hui un enjeu capital dans le cadre du nouveau règlement européen **RGPD** (Règlement Général sur la Protection des Données) ou **GDPR** (General Data Protection Regulation), et les formations qui y sont rattachées conduisent incontestablement vers des métiers porteurs.

Autres sources d'information

<http://home.pearsonvue.com/IBM>

<http://www-03.ibm.com/certify/>

Lien de la certification :

<https://www-03.ibm.com/certify/cert.html?id=38008401>