

IBM Certified Associate Administrator - Security Guardium Data Protection

RS3353 · RS · Publiée

L'essentiel

Code(s) NSF	326
Formacode(s)	31054
Type d'enregistrement	Enregistrement sur demande
Date d'échéance	31/12/2021

Certificateur(s)

CIE IBM FRANCE · SIRET : 55211846503644

Partenaires habilités

5 organismes habilités, d'après la liste publiée par France compétences : 4 à former et organiser l'évaluation et 1 à organiser l'évaluation.

Organisme	SIRET	Habilitation
ARROW ECS	38416992600027	Former et organiser l'évaluation
GLOBAL KNOWLEDGE NETWORK FRANCE	40394420000142	Former et organiser l'évaluation
LEARNQUEST FRANCE SAS	80073704100015	Former et organiser l'évaluation
PEARSON FRANCE	68201927800055	Organiser l'évaluation
TECH DATA FRANCE	72206563800065	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

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

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.

COMPÉTENCES ATTESTÉES

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

Caractéristiques produit :

- Exposer les fonctionnalités de base de Data Activity Monitoring (DAM) et de File Activity Monitoring (FAM)
- Détecter 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 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)

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION

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

Base légale

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

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

Lien de la certification :

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rs/3353/>