

IBM Certified Administrator - Security Guardium

RS3242 · 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 Administrator - Security Guardium, de niveau intermédiaire, s'adresse aux administrateurs de la solution Guardium, et en particulier aux professionnels de la sécurité des données et du déploiement.

Elle concerne les produits : IBM Security Guardium Data Activity Monitor, IBM Security Guardium File Activity Monitor et IBM Security Guardium Vulnerability Assessment, et a pour objectif de former des professionnels chargés d'administrer les règles de sécurité des bases de données.

Ceux-ci sont en mesure de configurer la solution Guardium afin de repérer, classer, analyser, protéger les données sensibles et d'en contrôler l'accès.

Par ailleurs, ils évaluent la vulnérabilité et surveillent les données et l'activité des fichiers.

Enfin, ils créent des rapports, des audits, des alertes et mettent en place des processus de conformité.

COMPÉTENCES ATTESTÉES

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

- Exécuter des tâches de planification
- Installer et configurer Security Guardium
- Surveiller les données et faire fonctionner l'analyse automatique incluse dans Guardium
- Définir les règles de sécurité des données
- Etablir des rapports
- Assurer la maintenance du produit et apporter un soutien technique

Caractéristiques produit et capacités techniques :

- Faire fonctionner les composants de haut niveau de la solution Guardium
- Actionner les fonctionnalités spécifiques de Data Activity Monitoring (DAM) et de File Activity Monitoring (FAM)
- Utiliser les fonctions 'Classification', 'Admissibilité' et 'Evaluation de la Vulnérabilité'
- Se servir du 'contrôle d'accès du niveau des données' (SGATE et Rédaction)
- Recourir aux agents et modules inclus dans la solution, tels que GIM (Guardium Installation Manager), S-TAP et CAS

Planification, dimensionnement et capacité :

- Isoler les principaux facteurs qui affectent le volume des données gérées par Guardium, en prenant en compte les sauvegardes et les archives
- Planifier l'architecture de l'emplacement des dispositifs
- Maîtriser les spécificités des structures à surveiller, tels que systèmes d'exploitation, bases de données, type de données, volumes de données et effets produits
- Elaborer une stratégie pour atteindre une haute disponibilité
- Evaluer le nombre et le type de dispositifs nécessaires en fonction de la charge PVU (Processor Value Unit)
- Mettre en évidence les exigences système des dispositifs Guardium

Installation et configuration :

- Localiser et télécharger les programmes d'installation les mieux adaptés aux dispositifs Guardium et à l'agent
- Créer de nouveaux dispositifs pour collecter les données et les regrouper
- Effectuer l'installation et la configuration initiales des appareils
- Configurer les processus de gestion des données des appareils et sa programmation
- Configurer l'appareil de manière à établir une interface avec les systèmes standards (mail, SNMP, LDAP, SIEM).
- Gérer l'accès des utilisateurs à Guardium
- Installer GIM (gestionnaire d'installation de Guardium) et l'utiliser pour mettre à jour les agents et les modules
- Installer S-TAP (Software Tap) à partir de la ligne de commande
- Configurer l'agent et faire fonctionner le moteur d'évaluation en examinant chacun des paramètres

Surveillance des données, règles et politiques, rapports :

- Réaliser un test d'évaluation de la vulnérabilité
- Etablir une distinction entre les effets des règles établies et les actions associées
- Utiliser les fonctions de contrôle, telles que les requêtes, les rapports, les procédures d'audit et les alertes
- Utiliser les outils de recherche

Surveillance automatique et performance :

- Utiliser les rapports et les alertes de surveillance automatique inclus dans Guardium
- Analyser les erreurs et les exceptions et prendre les mesures rectificatives
- Déceler et résoudre les problèmes liés à la performance des appareils
- Optimiser les tables de bases de données internes afin de soutenir la performance
- Contrôler l'activité des utilisateurs Guardium et établir des rapports
- Assurer la gestion continue de l'environnement

Maintenance et support technique :

- Utiliser les ressources et les services de dépannage IBM à disposition, tels que Knowledge Center, les notes techniques et le service de support technique d'IBM
- Planifier puis installer des correctifs sur les appareils et des mises à jour sur l'agent
- Recueillir les informations des diagnostics et résoudre les problèmes
- Utiliser les commandes classiques CLI (interface de ligne de commande) et GrdAPI, y compris les commandes de support
- Restaurer les données et les configurations à partir des sauvegardes et des archives

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION

Les connaissances suivantes sont requises pour réussir la certification :

- Systèmes d'exploitation et bases de données
- Matériels informatiques ou machines virtuelles
- Réseaux et protocoles
- Audits et mise en conformité
- Principes de la sécurité de l'information

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/3242/>