

C1000-153 IBM Cloud Pak for Security V1.10 Administrator

Objectifs

- Ces administrateurs auront des connaissances et de l'expérience dans l'installation, la configuration, l'administration et la maintenance d'IBM Cloud Pak for Security dans un environnement cloud, sur site et dans un environnement SaaS. Ces administrateurs sont capables d'effectuer des tâches avancées liées à la gestion et au fonctionnement quotidiens de l'environnement Cloud Pak for Security, y compris les services de base IBM Cloud Pak et Red Hat OpenShift Container Platform. L'administrateur Cloud Pak for Security est responsable de la configuration et de l'administration de Data Explorer, Threat Intelligence Insights, Threat Investigator et Cases.

Prérequis

- Connaissance de l'architecture cloud
- Connaissance de l'administration des utilisateurs de Cloud Pak for Security
- Familiarité avec le déploiement isolé de Cloud Pak for Security
- Connaissance de la façon d'effectuer des mises à niveau de version de Cloud Pak for Security
- Connaissance des flux de menaces et de sécurité basés sur STIX/TAXII
- Connaissance pratique des techniques de dépannage de base
- Connaissance des concepts de gestion des menaces XDR Connect
- Possibilité de connecter des sources de données et des actifs IBM et tiers
- Connaissance de Red Hat OpenShift Container Platform [CLI et UI]
- Connaissance des fonctionnalités, des cas d'utilisation et des applications du produit CP4S
- Comprendre les exigences pour installer la plateforme Cloud Pak for Security dans un environnement cloud
- Familiarité avec les systèmes SIEM afin de configurer les sources de données associées et/ou QRadar Proxy
- Possibilité d'utiliser les composants des services de base d'IBM Cloud Pak (tels que la journalisation) pour gérer CP4S

Programme

- Section 1 : Installation
 1. Vérifier les exigences de Cloud Pak pour la sécurité
 2. Configurer le cluster OpenShift
 3. Installer Cloud Pak pour la sécurité
- Section 2 : Configuration
 1. Configurer les fournisseurs d'identité dans Cloud Pak for Security
 2. Configurer les comptes dans Cloud Pak for Security
 3. Configurer les licences et l'utilisation de Cloud Pak for Security
 4. Configurer les applications
 5. Connecter les sources de données
- Section 3 : Administration
 1. Administrer les utilisateurs

2. Gérer les paramètres spécifiques à l'application
 3. Créer des clés API Cloud Pak pour la sécurité
 4. Gérer les dossiers
 5. Créer des tableaux de bord administratifs
- Section 4 : Maintenir l'environnement
 1. Évaluer et maintenir les licences Cloud Pak for Security
 2. Maintenir Cloud Pak pour la sécurité
 3. Maintenir la plateforme de cluster Red Hat OpenShift
 4. Sauvegarder et restaurer Cloud Pak pour la sécurité
 5. Mettre à niveau Cloud Pak pour la sécurité
 - Section 5 : Dépannage
 1. Dépanner Cloud Pak pour la sécurité
 2. Dépanner Red Hat OpenShift Container Platform
 -