C1000-120IBM Security Verify SaaS v1 Administrator

Objectifs

- Gérer l'intégration des applications
- Gérer l'intégration des sources d'identité
- Gérer les contrôles de sécurité

Prérequis

- Connaissance pratique de SAML 2.0, OAuth 2.0 et OIDC 1.0
- Connaissance pratique des méthodes d'authentification à premier et deuxième facteurs
- Connaissance pratique des fonctionnalités d'intégration IBM Security Verify disponibles.
- Connaissance pratique des concepts et des processus de gestion des identités et des accès

Programme

- Section 1 : Rapports et analyses
    1. Décrire les différents rapports pris en charge
    2. Analyser les événements d'audit
- Section 2 : Administration générale
    1. Identifiez les différents rôles d'administrateur par défaut
    2. Créer de nouveaux rôles d'administrateur
    3. Gérer les certificats
    4. Personnaliser l'apparence d'IBM Security Verify
- Section 3 : Support aux développeurs
    1. Ajouter le portail des développeurs à IBM Security Verify
    2. Ajouter et configurer un client API
- Section 4 : Intégration
    1. Décrire les fonctionnalités d'intégration de configuration avec IBM Resilient
    2. Décrire l'intégration MaaS360 pour Verify
    3. Décrire l'intégration IBM Security QRadar pour IBM Security Verify
    4. Décrire les scénarios hybrides avec IBM Verify Access
    5. Décrire l'intégration du gestionnaire de périphériques avec des solutions de gestion unifiée des points de terminaison tierces.
- Section 5 : Consentement et confidentialité
    1. Gérer un contrat de licence utilisateur final
    2. Gérer les objectifs de confidentialité
    3. Créer des règles de confidentialité
    4. Décrire les types de consentement
    5. Attribuer des règles à la stratégie
- Section 6 : Accès utilisateur, cycle de vie et gouvernance
    1. Forcer la justification métier pour l'accès aux applications
    2. Provisionner les utilisateurs dans l'application cible
    3. Exécuter la synchronisation des comptes
    4. Gérer les campagnes de recertification

- Section 7 : Gestion des utilisateurs
    1. Gérer les utilisateurs
    2. Ajouter un nouvel attribut
    3. Décrire les méthodes d'importation/création d'utilisateurs dans le répertoire cloud
    4. Décrire l'objectif du protocole SCIM et son application
    5. Décrire et gérer des groupes
    6. Ajouter une source d'identité fédérée
    7. Ajouter une source d'identité sociale
    8. Décrire le provisionnement juste à temps dans une source d'identité ?
    9. Connecter une source d'identité sur site avec un agent d'identité
    10. Configurer la liaison d'identité
    11. Configurer la politique de mot de passe
- Section 8 : Contrôles de sécurité
    1. Activer l'inscription à l'authentification multifacteur en ligne
    2. Appliquer des politiques d'accès à la console d'administration et à la page d'accueil
    3. Créer et modifier une politique d'accès de sécurité pour SSO
    4. Décrire la capacité d'accès adaptatif
    5. Sélectionnez le type de politique d'accès
    6. Configurer les méthodes d'authentification à deuxième facteur
    7. Décrire les méthodes d'authentification prises en charge dans IBM Verify
    8. Décrire le processus d'inscription dans l'application Verify
    9. Configurer l'authentification sans mot de passe
    10. Décrire la manière dont IBM Security Verify protège l'accès aux systèmes d'exploitation
    11. Décrire la manière dont IBM Security Verify protège l'accès VPN RADIUS
- Section 9 : Gestion des applications
    1. Ajouter une application SAML 2.0 à IBM Security Verfiy
    2. Ajouter une application OIDC 1.0
    3. Décrire les types d'applications
    4. Identifiez le bon composant pour l'authentification unique pour les applications existantes
    5. Distinguer les applications natives et fédérées
    6. Déterminer le bon type de subvention
    7. Sélectionnez le protocole d'authentification avec le jeton JWT
    8. Décrire l'utilisation d'une politique d'accès pour le SSO
    9. Configurer le cycle de vie du compte pour une application cible
    10. Créer et attribuer des rôles d'application
    11. Attribuer des droits aux utilisateurs et aux groupes
    12. Attribuer des objectifs aux applications
    13. Créer un profil d'application personnalisé
    14. Effectuer un dépannage SSO
-