IBM

C1000-120
IBM Security Verify SaaS v1 Administrator

Questions And Answers PDF Format:

For More Information – Visit link below:
https://www.certsgrade.com/

Version = **Product**

Latest Version: 6.0

Question: 1

Which three methods can be used to authenticate to the provisioning endpoint when Account lifecycle is enabled for a custom application?
Response:

A. SAML
B. OAuth Bearer
C. Kerberos Token
D. JSON Web Token
E. Client Certificate
F. Basic Authentication

Answer: B,D,F

Question: 2

What are two types of application access policies that can be authored in IBM Security Verify?
Response:

A. Native custom app policy
B. Kerberos based policy
C. Form login based policy
D. HTTP header based policy
E. Federated sign-on policy

Answer: A,E

Question: 3

An administrator tries to onboard an application to IBM Security Verify but the application isn't in the catalog. What action should the user take to continue to onboard the application?
Response:

A. Open a support ticket.
B. Connect an identity agent.
C. Create a custom application.
D. Use Add app in the Launchpad.

Answer: C

Question: 4

If an account on a target system shows as compliant, which statement was true at the time of the account synchronization?
Response:

A. The account was marked as active in IBM Security Verify.
B. The remediation policy was set to Do not remediate non-compliant accounts automatically.
C. All attributes set in attribute mapping matched between the account and the IBM Security Verify user.
D. All attributes set in reverse attribute mapping configuration matched between the account and the IBM Security Verify user.

Answer: D

Question: 5

Which use case describes the IBM Security Verify integration with IBM QRadar?
Response:

A. Automates user lifecycle events.
B. Enhances user registration capabilities.
C. Provides a way to archive and analyze events.
D. Protects application access through conditional constraints.

Answer: C

Question: 6

How can an OpenID Connect 1.0 application definition be added in the IBM Security Verify administrator interface?
Response:

A. Add a custom application with OIDC 1.0 as the sign-on method.
B. Add an OAuth application definition and add OIDC as a permitted scope.
C. Add a Generic OpenID Connect application in the application type selector.
D. Add an OAuth application definition and select the Enable OIDC 1.0 checkbox.

Answer: A

Question: 7

Where can the IBM Security Verify Directory Sync Agent be downloaded?
Response:

A. GitHub
B. Dockerhub
C. IBM App Exchange
D. IBM Passport Advantage

Answer: C

Question: 8

An administrator has been asked to configure an application, so that users in the sales group are automatically provisioned with an account. Which option should be used to configure this under Application Entitlements?
Response:

A. Automatic access for all users and groups.
B. Approval required for all users and groups.
C. Select users and groups, and assign individual access.
D. This can only be configured using Roles and Permissions.

Answer: C

Question: 9

What functionality is covered by the Authentication Activity Report?
Response:

A. multi-factor authentication activity by method
B. all sign-in attempts, application access requests, and API calls
C. all sign-in attempts to IBM Security Verify for a given time range
D. management events performed by administrator users and application owners

Answer: C

Question: 10

What are two actions available in the IBM Resilient integration with IBM Security Verify?
Response:

A. Add User
B. Add User to Role
C. Add User as Admin
D. Add User to Group
E. Add User Entitlement

Answer: D,E

For More Information – Visit link below:

https://www.certsgrade.com/

PRODUCT FEATURES

- 100% Money Back Guarantee
- 90 Days Free updates
- Special Discounts on Bulk Orders
- Guaranteed Success
- 50,000 Satisfied Customers
- 100% Secure Shopping
- Privacy Policy
- Refund Policy

16 USD Discount Coupon Code: NB4XKTMZ