SailPoint

SailPoint-Certified-IdentityNow-Professional
SailPoint Certified IdentityNow Professional Certification Exam

Questions and Answers (PDF)

For More Information - Visit:
https://www.certkillers.net

Total Questions: 208
Latest Version: 6.0

Question: 1

Pass-through Authentication
Give this one a try later!

A. The highest level role, which allows for complete control over the IdentityNow tenant.
B. Separation of Duties Policy
C. Any system of interest where you want to manage user access.
D. For authentication that uses another system like AD or LDAP to manage authentication.

Answer: D

Question: 2

All tenants have access to a set of shared services.
Give this one a try later!

A. True
B. False

Answer: A

Question: 3

Which of the following is not an option for handling the provisioning of passwords for new accounts?
Give this one a try later!

A. Using a static password for everyone.
B. Emailing a generated password to the user.
C. Setting an initial password based on identity data the user will know.
D. Setting a random password and having the user reset it before logging in.

Answer: B

Question: 4

All non-authoritative sources need a separate source of entitlement (group) data that can be aggregated to provide information like display names and descriptions.
Give this one a try later!

A. True
B. False

Answer: B

Question: 5

What is the Certification Email?
Give this one a try later!

A. 1. Entitlement Matching
2. Attribute Matching
3. Identity List
B. Sent to certifiers at the beginning of a campaign.
C. A create profile is applied anytime IdentityNow creates an account for a user on a source.
D. 1. Source Metadata
2. Account Schema
3. Manager Correlation

Answer: B

Question: 6

Can any attribute from a source create profile be used for attribute syncing?
Give this one a try later!

A. Yes
B. No

Answer: B

Question: 7

What does the Identity Profile encompass?
Give this one a try later!

A. 1. Authoritative Settings

2. Identity Attribute Mappings
3. Lifecycle States (optional)
B. 1. With every aggregation/identity refresh
2. In a daily refresh job
3. On manual update
C. 1. Static Passwords
2. Dynamic Known Passwords
3. Dynamic Unknown Passwords
D. 1. Data-driven/automated
2. Request-driven/user-initiated

Answer: A

Question: 8

Governance groups require that all members sign off on an access request before it can be approved.
Give this one a try later!

A. True
B. False

Answer: B

Question: 9

Every identity is required to login to IdentityNow.
Give this one a try later!

A. True
B. False

Answer: B

Question: 10

All entitlements that are aggregated into IdentityNow are automatically visible and requestable in the Request Center.
Give this one a try later!

A. True
B. False