Ping Identity PAP-001 Practice Questions

Shared by Keller on 21-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An administrator needs to configure a signed JWT identity mapping for an application that expects to be able to validate the signature. Which endpoint does the application need to access to validate the signature?

Options:

A- /pa/authtoken/JWKS
B- /pa-admin-api/v3/identityMappinga/descriptora/jwtidentitymapping
C- /pa/aidc/cb
D- /pa-admin-api/v3/authTokenManagement

Answer:

A

Explanation:

Applications consuming signed JWTs need the JSON Web Key Set (JWKS) endpoint to retrieve the public keys used for validating JWT signatures. PingAccess exposes this at /pa/authtoken/JWKS.

Exact Extract:

''When using JWT identity mapping, applications can obtain the signing keys from the /pa/authtoken/JWKS endpoint to validate the JWT signature.''

Option A is correct --- /pa/authtoken/JWKS provides the key set for signature validation.

Option B is incorrect --- that's an administrative API for configuring identity mappings, not a runtime validation endpoint.

Option C is incorrect --- /pa/aidc/cb is the OIDC callback endpoint.

Option D is incorrect --- /pa-admin-api/v3/authTokenManagement is for admin token management, not JWT validation.

Question 2

Question Type: MultipleChoice

Which two variables should be set in order for the PingAccess service script to start? (Choose 2 answers.)

Options:

A- J2EE_HOME
B- JAVA_HOME
C- PA_PATH
D- PA_HOME
E- JAVA_PATH

Answer:

B, D

Explanation:

PingAccess service scripts depend on knowing:

Where the Java runtime is installed (JAVA_HOME)

Where PingAccess itself is installed (PA_HOME)

Exact Extract:

''The PingAccess startup scripts require the JAVA_HOME environment variable to locate the JDK/JRE and the PA_HOME variable to locate the PingAccess installation directory.''

Option A (J2EE_HOME) is irrelevant to PingAccess.

Option B (JAVA_HOME) is correct --- needed for Java execution.

Option C (PA_PATH) is not a standard variable.

Option D (PA_HOME) is correct --- required to point to the PingAccess installation root.

Option E (JAVA_PATH) is not valid; PATH can include Java, but JAVA_HOME is the correct environment variable.

Question 3

Question Type: MultipleChoice

An administrator is integrating a new PingAccess Proxied Application. The application will use an SSL certificate issued by a publicly trusted Certificate Authority. PingAccess is terminating SSL and is responsible for loading the SSL certificate for that application. What initial action must the administrator take in PingAccess in this situation?

Options:

A- Import the SSL public key with the full certificate chain into the Certificates.
B- Import the PKCS#12 file with the full certificate chain into the Certificates.
C- Import the SSL public key with the full certificate chain into the Key Pairs.
D- Import the PKCS#12 file with the full certificate chain into the Key Pairs.

Answer:

D

Explanation:

For PingAccess to terminate SSL for a proxied application, it requires access to the private key and certificate chain. These are stored as Key Pairs.

Exact Extract:

''For SSL termination, you must import the server certificate and its private key as a PKCS#12 file into Key Pairs.''

Option A is incorrect --- a public key alone cannot terminate SSL.

Option B is incorrect --- PKCS#12 files must go into Key Pairs, not Certificates.

Option C is incorrect --- public keys alone are insufficient; PingAccess must have the private key.

Option D is correct --- the PKCS#12 file with full chain and private key is imported into Key Pairs.

Question 4

Question Type: MultipleChoice

A PingAccess administrator needs to configure PingAccess to validate tokens. Which two options can the administrator use? (Choose 2 answers)

Options:

A- PingFederate
B- Kerberos
C- Common SAML provider
D- Common OIDC provider
E- PingAuthorize

Answer:

A, D

Explanation:

PingAccess validates access tokens using Access Token Managers, which are typically backed by PingFederate or a generic OIDC provider.

Exact Extract:

''PingAccess validates tokens through Access Token Managers, which can be configured against PingFederate or a common OIDC provider.''

Option A (PingFederate) is correct --- the most common token provider.

Option B (Kerberos) is not supported for token validation.

Option C (SAML provider) is incorrect --- PingAccess does not natively consume SAML assertions.

Option D (Common OIDC provider) is correct --- tokens can be validated against any OIDC-compliant IdP.

Option E (PingAuthorize) is an authorization engine, not a token provider.

Question 5

Question Type: MultipleChoice

All style sheets should be accessible to all users without authentication across all applications. Which configuration option should the administrator use?

Options:

A- Define a Protocol Source for the resource.

B- Define Authentication Challenge Policy of none for the resource.
C- Define Global Unprotected Resources for the resource.
D- Define a Default Availability Profile of on-demand for the resource.

Answer:

C

Explanation:

The correct way to ensure resources such as CSS files, images, or JavaScript are accessible without authentication across all applications is to configure Global Unprotected Resources.

Exact Extract:

''Global unprotected resources define resources that do not require authentication and are accessible to all clients across applications.''

Option A is incorrect; Protocol Sources define back-end host connections, not authentication.

Option B would apply only per-resource, not across all applications.

Option C is correct --- Global Unprotected Resources are designed for this exact purpose.

Option D (Availability Profile) is related to application health checks and availability, not authentication.

Question 6

Question Type: MultipleChoice

An administrator is setting up PingAccess to terminate SSL for a proxied application. What action must the administrator take to configure an existing certificate for that application?

Options:

A- Assign the Key Pair to the Virtual Host
B- Enable Require HTTPS in the Application configuration
C- Assign the Key Pair to the Agent Listener
D- Set the secure flag to Yes in the Site configuration

Answer:

A

Explanation:

PingAccess terminates SSL at the Virtual Host level. To configure an existing certificate, the administrator must assign the appropriate Key Pair (which contains the certificate and private key) to the Virtual Host.

Exact Extract:

''SSL termination occurs on the engine listener through virtual hosts. Assign the certificate's key pair to the virtual host to secure proxied applications.''

Option A is correct --- assign the key pair to the Virtual Host for SSL termination.

Option B is incorrect --- Require HTTPS enforces secure access but does not configure SSL termination.

Option C is incorrect --- Agent Listener is for PingAccess Agents, not proxied apps.

Option D is incorrect --- secure flag affects cookie settings, not SSL certificates.

Question 7

Question Type: MultipleChoice

An administrator needs to use attributes that are not currently available in the Identity Mapping Attribute Name dropdown. Which action should the administrator take?

Options:

A- Request that the additional attributes be added by the token provider administrator
B- Create a Rewrite Content rule for the additional attributes
C- Request that the additional attributes be added by the web developer
D- Create a Web Session Attribute rule for the additional attributes

Answer:

A

Explanation:

Identity Mapping in PingAccess relies on attributes provided by the token provider (e.g., PingFederate, OIDC provider). If the desired attributes are not present in the dropdown, it means they are not being provided in the token or userinfo response.

Exact Extract:

''Attributes available in identity mappings are those provided in the web session by the token provider. If attributes are missing, they must be added to the token by the identity provider.''

Option A is correct --- the token provider administrator must configure the IdP to include the additional attributes.

Option B is incorrect --- rewrite rules modify content but do not supply new identity attributes.

Option C is incorrect --- developers cannot directly add identity attributes; they must come from the IdP.

Option D is incorrect --- Web Session Attribute rules only evaluate available attributes; they don't create new ones.

Question 8

Question Type: MultipleChoice

What is the purpose of the Mutual TLS Site Authenticator?

Options:

A- Allows the backend server to authenticate to PingAccess
B- Allows the user to authenticate to the backend server
C- Allows PingAccess to authenticate to the backend server
D- Allows PingAccess to authenticate to the token provider

Answer:

C

Explanation:

Mutual TLS (mTLS) is used to establish two-way authentication where both the client and the server present certificates to prove their identity. In the case of PingAccess, a Mutual TLS Site Authenticator is configured when PingAccess acts as a reverse proxy making requests to a backend (target) server.

Exact Extract from PingAccess documentation:

''Mutual TLS site authenticators provide client certificate authentication when PingAccess connects to a backend site. This allows PingAccess to present its certificate to the target server during the TLS handshake.''

This means the purpose is for PingAccess (client) to authenticate itself to the backend server (target resource) when establishing a secure connection.

Why other options are wrong:

A . Allows the backend server to authenticate to PingAccess

Incorrect. That's normal server-side TLS authentication (the server presents a cert to the client), not mutual TLS initiated by PingAccess.

B . Allows the user to authenticate to the backend server

Incorrect. End users do not directly use this setting; this is between PingAccess and the backend application server.

C . Allows PingAccess to authenticate to the backend server

Correct. This is exactly the definition of a Mutual TLS Site Authenticator in PingAccess.

D . Allows PingAccess to authenticate to the token provider

Incorrect. That would involve OIDC/OAuth token exchange and possibly TLS trust, but it's not the role of the Site Authenticator.

Thus, the correct answer is C. Allows PingAccess to authenticate to the backend server.

Question 9

Question Type: MultipleChoice

Any user who accesses an application must be in sales unless the user is a manager in the marketing department. The administrator creates the following web session rules:

(A) Look for department = sales

(B) Look for department = marketing

(C) Look for job_title = manager

Which additional actions should be taken to properly enforce this requirement?

Options:

A- Create a Rule Set (D) to accept ALL (A) (B AND C) Add Rule Set (D) to the resource
B- Create a Rule Set (D) to accept ANY (A) (B) (C) Add Rule Set (D) to the resource
C- Create a Rule Set (D) to accept ALL (A) Create a Rule Set (E) to accept ANY (B) (C) Create a Rule Set Group (F) to accept ALL (D) (E) Add Rule Set Group (F) to the resource
D- Create a Rule Set (D) to accept ANY (A) Create a Rule Set (E) to accept ALL (B) (C) Create a Rule Set Group (F) to accept ANY (D) (E) Add Rule Set Group (F) to the resource

Answer:

D

Explanation:

The requirement is:

Allow access if user is in sales

OR if user is in marketing AND is a manager

This is logically represented as:

(A) OR (B AND C)

To configure this in PingAccess:

Rule Set (D) = ANY (A)

Rule Set (E) = ALL (B, C)

Rule Set Group (F) = ANY (D, E)

Assign Group (F) to the resource

This exactly matches Option D.

Option A is incorrect --- requires both A and (B AND C), which is stricter than the requirement.

Option B is incorrect --- ANY(A, B, C) would allow users in marketing or managers without requiring both.

Option C is incorrect --- it uses ALL(D, E), which would require both conditions instead of OR.

Option D is correct --- it models (A OR (B AND C)).