TESTPASSPORT

ÜBUNGSFRAGEN

HOCHWERTIGE LERNRESSOURCEN

Exam : **PAP-001**

Title : Certified Professional - PingAccess

Version : DEMO

1.Which two variables should be set in order for the PingAccess service script to start? (Choose 2 answers.)
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.
Reference: PingAccess Installation Guide – Environment Variables

2.An administrator needs to add a set of rules to an application protected by a PingAccess agent. Which rule will be unavailable to add to the application?
A. Rewrite Cookie Domain
B. Network Range
C. Rate Limiting
D. Cross-Origin Request
Answer: A
Explanation:
PingAccess distinguishes between gateway rules and agent rules. Some processing rules, such as Rewrite Cookie Domain, only apply when PingAccess is acting as a reverse proxy (gateway), not when protecting applications via agents.
Exact Extract:
“Rewrite Cookie Domain rules are not supported for agent applications. They are only available for proxied (gateway) applications.”
Option A (Rewrite Cookie Domain) is correct — unavailable with agent applications.
Option B (Network Range) is available for both agents and gateways.
Option C (Rate Limiting) is supported on both application types.
Option D (Cross-Origin Request) is also supported in both.
Reference: PingAccess Administration Guide – Agent vs. Gateway Rules

3.An administrator is configuring a resource in PingAccess that has no authentication requirements but

must still apply identity mappings for users who are already authenticated. The resource must be accessible without requiring authentication while allowing access-control and processing rules to be applied.
How should the administrator configure the resource?
A. Select Standard for Authentication.
B. Apply a custom Authentication Policy.
C. Select Unprotected for Authentication.
D. Select Anonymous for Authentication.
Answer: D
Explanation:
Anonymous is correct because it removes the requirement to authenticate before accessing the resource while preserving policy processing. PingAccess documentation states that, for an Anonymous resource, identity mappings still run when the requester is already authenticated, and applicable access-control and processing rules remain active. Unprotected also removes authentication, but it bypasses the application and resource access-control policy, so it would not satisfy the stated requirement. Standard inherits the root application's authentication behavior and could still trigger authentication. A custom authentication policy is unnecessary and does not represent the required resource authentication type. Therefore, the administrator should select Anonymous, option D. Ping Identity: Adding application resources

4.For a Web Application, the id_token must be transmitted through a back channel with the OIDC standards-based approach.
Which action should the administrator perform in the Web Session to meet this requirement?
A. Set the login type to code
B. Set the request preservation to POST
C. Set the login type to POST
D. Set the request preservation to None
Answer: A
Explanation:
To transmit the id_token via a back channel according to OIDC best practices, the application must use the Authorization Code Flow (login type = code). This ensures tokens are retrieved securely via the back channel instead of being exposed in the browser.
Exact Extract:
"For back-channel transmission of ID tokens, configure the OIDC login type as Authorization Code."
Option A is correct — setting login type to code ensures back-channel delivery.
Option B is incorrect — request preservation concerns request method persistence, not OIDC flow.
Option C is incorrect — POST is not a valid login type; only Code, Implicit, or Hybrid.
Option D is incorrect — request preservation has no bearing on token delivery.
Reference: PingAccess Administration Guide – Configuring OIDC Web Sessions

5.An administrator needs to configure an application that uses a backend web server that has its own authentication mechanism.
Which type of object must be configured for PingAccess to provide access to the target server?
A. Token Provider

B. Web Session
C. Site Authenticator
D. Access Control Rule
Answer: C
Explanation:
When a backend application requires its own authentication (e.g., Basic Auth or mutual TLS), PingAccess uses a Site Authenticator to inject the necessary credentials.
Exact Extract:
“Site Authenticators provide the credentials PingAccess uses when authenticating to target applications that require their own authentication mechanisms.”
Option A (Token Provider) is incorrect — this is used for OIDC/OAuth tokens, not site-level authentication.
Option B (Web Session) manages end-user sessions, not backend site authentication.
Option C (Site Authenticator) is correct — it handles authentication between PingAccess and the backend.
Option D (Access Control Rule) enforces authorization, not backend authentication.
Reference: PingAccess Administration Guide – Site Authenticators