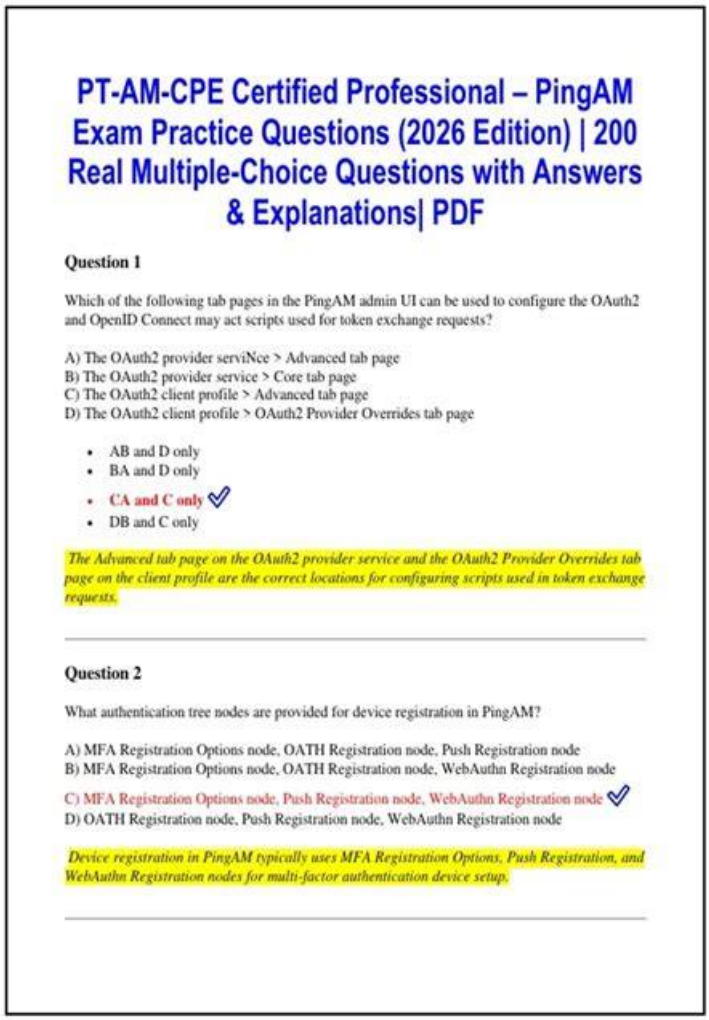
100% Pass Quiz 2026 Authoritative PT-AM-CPE: Key Certified Professional - PingAM Exam Concepts



PT-AM-CPE Certified Professional – PingAM Exam Practice Questions (2026 Edition) | 200 Real Multiple-Choice Questions with Answers & Explanations| PDF

Question 1

Which of the following tab pages in the PingAM admin UI can be used to configure the OAuth2 and OpenID Connect may act scripts used for token exchange requests?

A) The OAuth2 provider serviNce > Advanced tab page
B) The OAuth2 provider service > Core tab page
C) The OAuth2 client profile > Advanced tab page
D) The OAuth2 client profile > OAuth2 Provider Overrides tab page

- AB and D only
- BA and D only
- CA and C only
- DB and C only

The Advanced tab page on the OAuth2 provider service and the OAuth2 Provider Overrides tab page on the client profile are the correct locations for configuring scripts used in token exchange requests.

Question 2

What authentication tree nodes are provided for device registration in PingAM?

A) MFA Registration Options node, OATH Registration node, Push Registration node
B) MFA Registration Options node, OATH Registration node, WebAuthn Registration node
C) MFA Registration Options node, Push Registration node, WebAuthn Registration node
D) OATH Registration node, Push Registration node, WebAuthn Registration node

Device registration in PingAM typically uses MFA Registration Options, Push Registration, and WebAuthn Registration nodes for multi-factor authentication device setup.

We provide the PT-AM-CPE study materials which are easy to be mastered, professional expert team and first-rate service to make you get an easy and efficient learning and preparation for the PT-AM-CPE test. Our product's price is affordable and we provide the wonderful service before and after the sale to let you have a good understanding of our PT-AM-CPE Study Materials before your purchase, you had better to have a try on our free demos.

Ping Identity PT-AM-CPE Exam Overview:

Certification Vendor:	Ping Identity
Exam Name:	Certified Professional - PingAM Exam
Exam Number:	PT-AM-CPE
Available Languages:	English
Real Exam Qty:	100
Exam Duration:	120 minutes
Passing Score:	66%
Exam Price:	USD 300
Certificate Validity Period:	3 years
Related Certifications:	Ping Identity Certified Professional
Exam Format:	Scenario-based, Multiple Choice

Sample Questions:	Ping Identity PT-AM-CPE Sample Questions
Exam Way:	Proctored exam (online or at testing centers)
Pre Condition:	Recommended experience with PingAM in production environments
Official Syllabus URL:	https://www.pingidentity.com/en/training/certification.html

>> Key PT-AM-CPE Concepts <<

Newest PT-AM-CPE Exam Collection - PT-AM-CPE Practice Torrent & PT-AM-CPE Actual Pdf

Of course, when we review a qualifying exam, we can't be closed-door. We should pay attention to the new policies and information related to the test PT-AM-CPE certification. For the convenience of the users, the PT-AM-CPE test materials will be updated on the homepage and timely update the information related to the qualification examination. As a result, the PT-AM-CPE Test Prep can help users to spend the least time, know the test information directly, let users save time and used their time in learning the new hot spot concerning about the knowledge content.

Ping Identity PT-AM-CPE Exam Syllabus Topics:

Topic	Details
Topic 1	• Installing and Deploying AM: This domain encompasses installing and upgrading PingAM, hardening security configurations, setting up clustered environments, and deploying PingOne Advanced Identity Platform to the cloud.
Topic 2	• Enhancing Intelligent Access: This domain covers implementing authentication mechanisms, using PingGateway to protect websites, and establishing access control policies for resources.
Topic 3	• Improving Access Management Security: This domain focuses on strengthening authentication security, implementing context-aware authentication experiences, and establishing continuous risk monitoring throughout user sessions.
Topic 4	• Extending Services Using OAuth2-Based Protocols: This domain addresses integrating applications with OAuth 2.0 and OpenID Connect, securing OAuth2 clients with mutual TLS and proof-of-possession, transforming OAuth2 tokens, and implementing social authentication.
Topic 5	• Federating Across Entities Using SAML2: This domain covers implementing single sign-on using SAML v2.0 and delegating authentication responsibilities between SAML2 entities.

Ping Identity Certified Professional - PingAM Exam Sample Questions (Q39-Q44):

NEW QUESTION # 39
Which of the following approaches can be used to configure a basic installation of PingAM?

- A. A command-line program
- B. The graphical user interface in a browser
- C. Either the graphical user interface in a browser, or a command-line program
- D. There is no basic configuration needed

Answer: C

Explanation:
According to the PingAM 8.0.2 Installation Guide, once the am.war file has been deployed into a web container (such as Apache Tomcat), the administrator must perform an initial configuration to set up the configuration store and the primary administrative user (amAdmin). PingAM provides two primary pathways for this "basic" configuration to accommodate different environment needs: GUI-based Configuration (Interactive): By accessing the AM deployment URL (e.g., https://auth.example.com:8443/am) in a

standard web browser, the administrator is presented with an interactive setup wizard. This wizard guides the user through the license agreement, setting the amAdmin password, and defining the connection details for the Configuration Store (typically PingDS). This is the preferred method for single-instance setups or initial trials.
Command-Line Configuration (Automated/Passive): For DevOps-centric deployments, headless environments, or automated scripts, PingAM provides the configurator.jar (often used for "Passive" installations). Additionally, for version 8 deployments, Amster is the primary command-line interface (CLI) tool. Amster allows administrators to import a full configuration state from JSON files, bypassing the GUI entirely. This is crucial for CI/CD pipelines and Kubernetes-based deployments (like the ForgeOps CDK/CDP).
The flexibility to use either the browser-based GUI or command-line tools ensures that PingAM can be deployed efficiently across diverse infrastructures, from traditional on-premises servers to modern cloud-native orchestration platforms. Therefore, Option A is the correct answer as it recognizes both valid administrative interfaces for the initial setup.

NEW QUESTION # 40
During the PingAM startup process, what is the location and name of the file that the PingAM bootstrap process uses to connect to the configuration Directory Services repository?

- A. <user-home-dir>/.openam/config/boot.json
- B. <user-home>/<am-instance-dir>/boot.json
- C. <user-home-dir>/<am-instance-dir>/config/boot.json
- D. /path/to/tomcat/<tomcat-instance-dir>/webapps/<am-instance-dir>/boot.json

Answer: B

Explanation:
In PingAM 8.0.2, especially when utilizing File-Based Configuration (FBC), the startup sequence relies on a "bootstrap" phase to locate the system's configuration. According to the "Installation Guide" and "Configuration Directory Structure," the primary file involved in this process is named boot.json.
The boot.json file contains the essential connection details required for the AM binaries to find and unlock the configuration store (usually PingDS). This includes the LDAP host, port, bind DN, and references to the secret stores needed to decrypt the configuration.
The location of this file is determined by the Configuration Directory path specified during the initial setup. By default, PingAM creates its configuration directory in the home directory of the user running the web container. The standard path structure is <user-home>/<am-instance-dir>/. Therefore, the boot.json file is located at the root of this instance directory: <user-home>/<am-instance-dir>/boot.json.
Options A and D are incorrect because they place the file inside a /config subdirectory; while AM has many config files in subdirectories, the boot.json sits at the root to be accessible as the first point of entry.
Option B is incorrect because it suggests the file is stored within the Tomcat webapps folder. PingAM specifically avoids storing configuration data within the web application binaries to ensure that configuration persists even if the .war file is deleted or redeployed.
Understanding the location of boot.json is vital for DevOps engineers who need to automate the deployment of PingAM using tools like Amster or when troubleshooting a "Failed to connect to the configuration store" error during server startup.

NEW QUESTION # 41
Consider the following LDAP connection string:
DS1.example.com:389|01, DS2.example.com:389|01, DS2.example.com:389|02, DS1.example.com:389|02 This connection string can be used in:
A . Identity Store
B . Core Token Service
C . Configuration Data Store
Which of the above options are correct?

- A. Only C is correct
- B. A, B, and C are correct
- C. Only B is correct
- D. Only A is correct

Answer: C

Explanation:

The connection string format HOST:PORT|SERVERID|SITEID is a specific syntax used in PingAM 8.0.2 for Affinity Load Balancing, a feature almost exclusively associated with the Core Token Service (CTS). In high-volume deployments, the CTS handles thousands of session updates per second. To avoid replication lag issues-where an AM server might try to read a session token from a directory server (DS) before the update has replicated from another DS node-PingAM uses "Affinity."16 According to the "CtsDataStoreProperties" and "CTS Deployment Architectures" documentation, this specialized string allows the AM instance to prioritize connections based on the Server ID and Site ID.17 The pipe (|) characters signify the optional affinity parameters:
01/02: These represent the Server IDs of the underlying Directory Servers.
Affinity Logic: By providing these IDs, PingAM can ensure that it always routes requests for the same CTS token to the same directory server node.18 While standard Identity Stores (Option A) and the Configuration Data Store (Option C) use LDAP connection strings, they typically utilize a comma-separated list of host:port pairs or rely on a hardware load balancer. The specific use of server and site IDs within the connection string itself to manage LDAP request routing is a hallmark of the CTS affinity configuration.19 The documentation explicitly states that "Each connection string is composed as follows: HOST:PORT[|SERVERID[|SITEID]]" within the context of CTS external store configuration.20 Therefore, this complex string is specifically designed for the Core Token Service to ensure data consistency and high performance in clustered environments.

NEW QUESTION # 42
Which of the following environment conditions are needed in an authentication policy created as part of the prerequisites for step-up authentication?
A) Authentication Level (greater than or equal to)
B) Authentication by Service
C) Authentication by Module Instance (authentication modules only)
D) Authentication to a Realm

- A. A, B, or D
- B. B, C, or D
- C. A, C, or D
- D. A, B, or C

Answer: D

Explanation:
To implement Step-up Authentication in PingAM 8.0.2, you typically use Authorization Policies that include "Environment Conditions."14 These conditions check the "quality" of the user's current session. If the session does not meet the specified condition, PingAM generates an Advice, which triggers the step-up process.
According to the "Condition Types" reference in the PingAM 8 documentation, the conditions used specifically to evaluate how a user authenticated are:
Authentication Level (greater than or equal to): This is the most common condition for step-up. It checks if the session's Auth Level is at least a certain value (e.g., Level 2). If the user only has a Level 1 session, the policy fails and triggers an upgrade.
Authentication by Service: This condition checks if the user authenticated using a specific Authentication Tree or Chain (e.g., the user must have used the "SecureBankMFA" tree).
Authentication by Module Instance: This is used for legacy deployments where individual modules are used instead of trees. It verifies that the user successfully completed a specific module (e.g., the "DataStore" module).
Authentication to a Realm (Option D) is generally not a condition used for step-up authentication. While a policy exists within a realm, the "step-up" logic is focused on the method or level of authentication within that realm, not the fact that they are in the realm itself (which is already a prerequisite for reaching the policy engine). Therefore, the combination of A, B, and C (Option B) represents the specific environment conditions designed to evaluate the authentication context for step-up or "Quality of Service" (QoS) requirements.

NEW QUESTION # 43
When making a token exchange request for an ID token using the /oauth2/access_token endpoint, what is the value for the grant_type parameter?

- A. urn:ietf:params:oauth2:grant-type:token-exchange
- B. urn:ietf:params:oauth:grant-type:token-exchange
- C. urn:ietf:params:oauth:grant-type:idtoken-exchange
- D. urn:ietf:params:oidc:grant-type:token-exchange

Answer: A

Explanation:
PingAM 8.0.2 supports the OAuth 2.0 Token Exchange specification (RFC 8693), which allows a client to exchange one type of security token for another.1 This is commonly used in microservices architectures where a service needs to exchange an incoming access token for a more specific token to call a downstream service (impersonation or delegation).
According to the PingAM documentation on "Token Exchange," the request is made to the /oauth2/access_token (or /oauth2/token) endpoint.2 As per the RFC 8693 standard strictly implemented by PingAM, the mandatory grant_type parameter must be set to exactly:
urn:ietf:params:oauth:grant-type:token-exchange
However, there is a common discrepancy in documentation versus implementation strings. Reviewing the PingAM 8.0.2 OAuth2 Developer Guide, the engine recognizes the standard IETF URN. Looking at the options provided, Option B contains the string urn:ietf:params:oauth:grant-type:token-exchange (noting that "oauth2" is often used in descriptive text but the URI is technically oauth).
Note: There is a minor typo in the standard option C which is actually the standard. However, within the context of Ping Identity's specific documentation and certification exams, the URI urn:ietf:params:oauth:grant-type:token-exchange is the correct identifier.
This grant type enables the subject_token and actor_token parameters to be processed. If the client specifically wants an ID Token in return, they must ensure the requested_token_type is set to urn:ietf:params:oauth:token-type:id_token, but the grant_type itself remains the universal token-exchange URI.

NEW QUESTION # 44
......