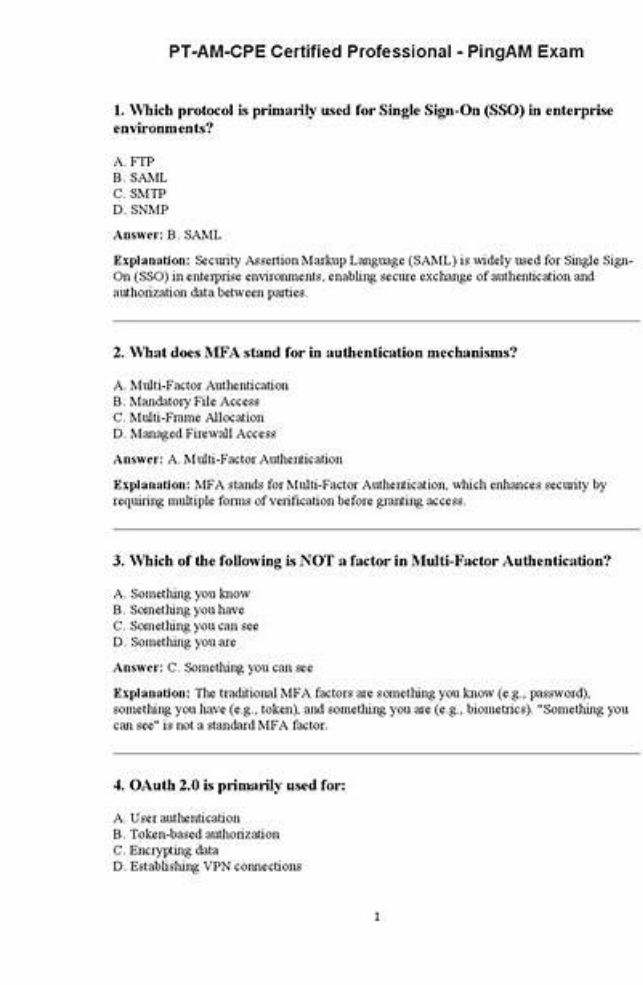
Valid PT-AM-CPE Prep Guide–The Best Reliable Test Syllabus Providers for PT-AM-CPE: Certified Professional - PingAM Exam



PT-AM-CPE Certified Professional - PingAM Exam

1. Which protocol is primarily used for Single Sign-On (SSO) in enterprise environments?

A. FTP
B. SAML
C. SMTP
D. SNMP

Answer: B. SAML

Explanation: Security Assertion Markup Language (SAML) is widely used for Single Sign-On (SSO) in enterprise environments, enabling secure exchange of authentication and authorization data between parties.

---

2. What does MFA stand for in authentication mechanisms?

A. Multi-Factor Authentication
B. Mandatory File Access
C. Multi-Frame Allocation
D. Managed Firewall Access

Answer: A. Multi-Factor Authentication

Explanation: MFA stands for Multi-Factor Authentication, which enhances security by requiring multiple forms of verification before granting access.

---

3. Which of the following is NOT a factor in Multi-Factor Authentication?

A. Something you know
B. Something you have
C. Something you can see
D. Something you are

Answer: C. Something you can see

Explanation: The traditional MFA factors are something you know (e.g., password), something you have (e.g., token), and something you are (e.g., biometrics). "Something you can see" is not a standard MFA factor.

---

4. OAuth 2.0 is primarily used for:

A. User authentication
B. Token-based authorization
C. Encrypting data
D. Establishing VPN connections

1

Our company will provide first class service on PT-AM-CPE exam questions for our customers. As a worldwide leader in offering the best PT-AM-CPE exam guide, we are committed to providing comprehensive service to the majority of consumers and strive for constructing an integrated service. What's more, we have achieved breakthroughs in PT-AM-CPE Study Materials application as well as interactive sharing and after-sales service. As long as you need help, we will offer instant support to deal with any of your problems about our PT-AM-CPE exam questions

Ping Identity PT-AM-CPE Exam Syllabus Topics:

Topic	Details
Topic 1	• Federating Across Entities Using SAML2: This domain covers implementing single sign-on using SAML v2.0 and delegating authentication responsibilities between SAML2 entities.
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	• 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.

>> PT-AM-CPE Prep Guide <<

Pass Guaranteed 2026 PT-AM-CPE: Certified Professional - PingAM Exam Marvelous Prep Guide

The Ping Identity PT-AM-CPE exam questions are being offered in three different formats. These formats are PT-AM-CPE PDF dumps files, desktop practice test software, and web-based practice test software. All these three PT-AM-CPE exam dumps formats contain the Real PT-AM-CPE Exam Questions that assist you in your Certified Professional - PingAM Exam practice exam preparation and finally, you will be confident to pass the final Ping Identity PT-AM-CPE exam easily.

Ping Identity Certified Professional - PingAM Exam Sample Questions (Q48-Q53):

NEW QUESTION # 48
What are the possible outcomes of the Push Result Verifier node?

- A. Success, Failure, Expired, Waiting, Retry
- B. Success, Failure, Expired, Waiting
- C. Success, Failure, Waiting, Retry
- D. Success, Failure, Expired, Retry

Answer: B

Explanation:
The Push Result Verifier node is a core component of the "MFA: Push Authentication" journey in PingAM 8.0.2. Its primary function is to check the status of a push notification that was previously dispatched to a user's mobile device (usually via the Push Sender node).22 According to the "Authentication Node Reference" for version 8.0.2, the node evaluates the state of the push request and yields exactly four distinct outcomes:
Success: This path is followed if the user has actively approved the push notification on their registered device using the ForgeRock/Ping Authenticator app.
Failure: This path is taken if the user explicitly denies or rejects the push notification on their device, indicating a potential unauthorized login attempt.
Expired: This outcome occurs if the notification reaches its "Message Timeout" limit (defined in the Push Sender node) without any response from the user.23 In standard trees, this path often loops back to allow the user to try a different MFA method or resend the push.
Waiting: This outcome is triggered if a response has not yet been received but the timeout has not yet been reached. This is used in conjunction with a Push Wait or Polling mechanism to create a "check-and-loop" logic until a final result (Success, Failure, or Expired) is determined.
The Retry outcome (mentioned in other options) is notably absent from this specific node's metadata. While a "Retry" might be implemented in the overall tree logic (for example, by using a Retry Limit Decision node after an Expired outcome), the Push Result Verifier node itself only reports the state of the specific push transaction it is tracking. Understanding these four discrete states is vital for designing resilient authentication journeys that handle user delays or network issues gracefully.

NEW QUESTION # 49
Which of the following options represents best practice for an implementation that configures an ID token in a subject condition for policies validating the token's claims?

- A. Policy evaluation only validates the claims, not the ID token. The ID token should be validated after making the policy

evaluation request
- B. Policy evaluation only validates the claims, not the ID token. There is no need to validate the ID token that was obtained before the policy is evaluated
- C. Policy evaluation validates the claims and the ID token. There is no need to validate the ID token before the policy is evaluated
- D. Policy evaluation only validates the claims, not the ID token. The ID token should be validated before making the policy evaluation request

Answer: D

Explanation:
In PingAM 8.0.2, Authorization Policies can be configured to use complex conditions to determine if access should be granted. When a policy uses a Subject Condition based on an OpenID Connect (OIDC) ID Token, the policy engine looks for specific claims within that token (such as group membership or a specific user ID).
According to the "Authorization and Policy Evaluation" best practices, it is crucial to understand the separation of concerns between the Policy Decision Point (PDP) and the client. The PingAM policy engine is designed to evaluate logic-it checks if claimX == valueY. However, the policy engine typically does not perform a full cryptographic validation of the ID token's signature every time it evaluates a condition, especially if the token is passed as a string in the evaluation request.
Therefore, the best practice is as follows:
The client application or the PEP (Policy Enforcement Point) must validate the ID token (ensuring it is signed by a trusted provider, has not expired, and contains the correct audience) before sending the claims to the AM policy service for evaluation. If an unvalidated or forged token is used to supply claims for a policy request, and the policy engine assumes the input is "trusted," it could result in unauthorized access.
By validating the token first (Option C), the implementation ensures that only legitimate identity data is processed by the authorization logic. Option D is incorrect because the policy engine's primary role is decision-making based on presented attributes, not act as a full OIDC validation service during a REST evaluation call. Option B is a security risk as it ignores the necessity of cryptographic proof of identity.

NEW QUESTION # 50
In a multi-server deployment, what is the impact of not ensuring stickiness in the load balancer configuration?

- A. The user will see more redirects in their browser
- B. Performance may decrease as load on the system will be higher
- C. The browser will not be able to validate the user session with the correct PingAM server
- D. Session failover will not work

Answer: B

Explanation:
In a high-availability PingAM 8.0.2 cluster, the Load Balancer (LB) is responsible for distributing traffic across multiple AM instances. Session Stickiness (also known as session affinity) ensures that all requests from a specific user session are routed to the same AM server that initially created the session.
According to the PingAM "Deployment Planning" and "Load Balancing" documentation, PingAM is designed to be "sticky-preferred" but not "sticky-required" if the Core Token Service (CTS) is used. If stickiness is not ensured:
Performance Impact: Every time a user request lands on a different AM server (Server B) than the one that holds the session in local memory (Server A), Server B must query the CTS (External Store) to retrieve the session details, deserialize the object, and reconstruct the session state. This cross-server look-up introduces significant latency and increases the load on the PingDS instances hosting the CTS.
CTS Load: Without stickiness, every single request becomes a "Global" session lookup. This drastically increases the I/O and CPU overhead on the back-end directory servers, potentially leading to performance degradation of the entire identity platform.
Why other options are incorrect:
Option A: Session failover requires the CTS, but stickiness actually minimizes the need for failover logic during normal operation. Failover still works without stickiness, it just becomes the "default" behavior for every request.
Option B: AM servers in a cluster share the same encryption keys and back-end stores. Any server can technically validate a session by looking it up in the CTS; the browser doesn't "know" which server is correct.
Option C: Redirects are handled at the application logic level. While some internal processing changes, it doesn't necessarily result in extra browser-level HTTP redirects.
Thus, the primary negative impact of lacking stickiness in a correctly configured cluster is a decrease in performance (Option D) due to the constant session synchronization overhead.

NEW QUESTION # 51
When developing a PingAM may act script for OAuth2 token exchange patterns, which variables are made available for use in the script?

- A. clientProperties, identity, logger, requestProperties, scopes, scriptName, session, requestedToken
- B. clientProperties, identity, logger, requestProperties, scopeList, scriptName, session, token
- C. clientProperties, identity, logger, requestProperties, scopes, scriptName, session, token
- D. clientProperties, identity, logger, requestProperties, scopeList, scriptName, session, requestedToken

Answer: A

Explanation:
The OAuth2 May Act script type in PingAM 8.0.2 allows administrators to programmatically determine if a token exchange request (impersonation or delegation) should be allowed by adding a may_act claim to the token.
According to the "Scripting" and "Token Exchange Scripting API" documentation, when this script is executed, the AM engine provides a specific set of "Bindings" or variables. These allow the script to inspect the context of the request before deciding to modify the token. The documented variables for the OAuth2 May Act script are:
clientProperties: A map of the OAuth2 client's configuration properties.
identity: The identity object for the user/subject.
logger: The logging object for debugging within the script.
requestProperties: Properties of the incoming HTTP request.
scopes: The set of scopes requested or associated with the token.
scriptName: The name of the script being executed.
session: The user's SSO session (if available).
requestedToken: This is the most important variable; it represents the token being issued. Methods like .addMayAct() or .setMayAct() are called on this specific object.
Why other options are incorrect:
Option B correctly lists the bindings.
Options A and D are incorrect because they use the variable name token. While token is a common variable name in other OAuth2 script types (like the Access Token Modification script), the Token Exchange script specifically uses requestedToken to distinguish the new token from the subject_token or actor_token provided in the request.
Option C uses scopeList, which is not the standard variable name for the scopes in this specific script context; the documentation defines it as scopes.

NEW QUESTION # 52
Why should module-based authentication be disabled in production?

- A. Module-based authentication allows a user to authenticate with the amAdmin account
- B. Module-based authentication allows a user to bypass steps in an authentication chain
- C. Module-based authentication allows a user to select any authentication level
- D. Module-based authentication allows users to authenticate in any realm

Answer: B

Explanation:
In PingAM 8.0.2, there is a critical distinction between Tree-based (or Chain-based) authentication and Module-based authentication. Module-based authentication is a legacy feature that allows a user to target an individual authentication module directly (e.g., .../UI/Login?module=DataStore).
According to the "Security Considerations" and "Hardening PingAM" documentation, module-based authentication poses a significant security risk and should be disabled in production. This is because it allows a user to bypass steps in an authentication chain (Option C).
If an administrator has designed a secure "Chain" that requires both a DataStore (password) check AND a One-Time Password (MFA) check, the intention is for these to be inseparable. However, if module-based authentication is enabled, a malicious user or a tester could bypass the MFA requirement by crafting a URL that calls only the "DataStore" module. This effectively circumvents the multi-factor security logic intended by the administrator.
To mitigate this, PingAM provides a global and realm-level setting to "Disable Module-based Authentication." Once disabled, PingAM will only process authentication requests that target a named Authentication Tree or Chain, ensuring that the user is forced through the entire sequence of nodes and logic defined by the security architect.

NEW QUESTION # 53
.....

Our company is a professional certificate exam materials provider, therefore we have rich experiences in offering exam dumps. PT-AM-CPE study materials are famous for high quality, and we have received many good feedbacks from our customers, and they think highly of our PT-AM-CPE exam dumps. Moreover, we also pass guarantee and money back guarantee, and if you fail to pass the exam, we will give you refund and no other questions will be asked. PT-AM-CPE Training Materials have free update for 365 days after purchasing, and the update version will be sent to you email automatically.

Reliable PT-AM-CPE Test Syllabus: https://www.trainingdumps.com/PT-AM-CPE_exam-valid-dumps.html

- PT-AM-CPE - Valid Certified Professional - PingAM Exam Prep Guide □ Search for □ PT-AM-CPE □ and download exam materials for free through ➡ www.vce4dumps.com □□□ □PT-AM-CPE Review Guide
- 100% Pass Ping Identity - PT-AM-CPE - Certified Professional - PingAM Exam –Efficient Prep Guide □ Search for ➠ PT-AM-CPE □ and obtain a free download on { www.pdfvce.com } □Study PT-AM-CPE Materials
- 100% Pass Ping Identity - PT-AM-CPE - Certified Professional - PingAM Exam –Efficient Prep Guide □ Search for ➥ PT-AM-CPE □ on [www.prepawayexam.com] immediately to obtain a free download □PT-AM-CPE Simulations Pdf
- Certified Professional - PingAM Examlatest test questions - PT-AM-CPE reliable braindumps - Certified Professional - PingAM Examfree practice dumps □ Search for { PT-AM-CPE } and obtain a free download on □ www.pdfvce.com □ □Valid PT-AM-CPE Test Sample
- PT-AM-CPE Reliable Source □ Online PT-AM-CPE Test □ PT-AM-CPE Sample Questions Pdf ❊ Search for □ PT-AM-CPE □ on （ www.practicevce.com ） immediately to obtain a free download □Examcollection PT-AM-CPE Dumps Torrent
- Valid Test PT-AM-CPE Format □ PT-AM-CPE Simulations Pdf □ PT-AM-CPE Reliable Source □ Immediately open （ www.pdfvce.com ） and search for 「 PT-AM-CPE 」 to obtain a free download □PT-AM-CPE Reliable Real Test
- 100% Pass Ping Identity - PT-AM-CPE - Certified Professional - PingAM Exam –Efficient Prep Guide □ Enter ▸ www.practicevce.com ◂ and search for 【 PT-AM-CPE 】 to download for free □PT-AM-CPE Sample Questions Pdf
- PT-AM-CPE - Valid Certified Professional - PingAM Exam Prep Guide □ Search on { www.pdfvce.com } for ⇛ PT-AM-CPE ⇚ to obtain exam materials for free download □PT-AM-CPE Review Guide
- Latest PT-AM-CPE Examprep □ Valid Test PT-AM-CPE Format □ New PT-AM-CPE Test Forum □ Simply search for ▸ PT-AM-CPE ◂ for free download on ▹ www.troytecdumps.com ◃ □Online PT-AM-CPE Test
- Valid Test PT-AM-CPE Format □ PT-AM-CPE Simulations Pdf □ PT-AM-CPE Practice Braindumps □ Enter □ www.pdfvce.com □ and search for { PT-AM-CPE } to download for free □Sample PT-AM-CPE Exam
- Updates To www.examcollectionpass.com PT-AM-CPE Dumps Every 1 year □ Search for ➤ PT-AM-CPE □ and download it for free immediately on ➤ www.examcollectionpass.com □ □PT-AM-CPE Valid Test Guide
- dist-edu.acharya-iit.ac.in, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, flysouthern.aero, www.stes.tyc.edu.tw, Disposable vapes