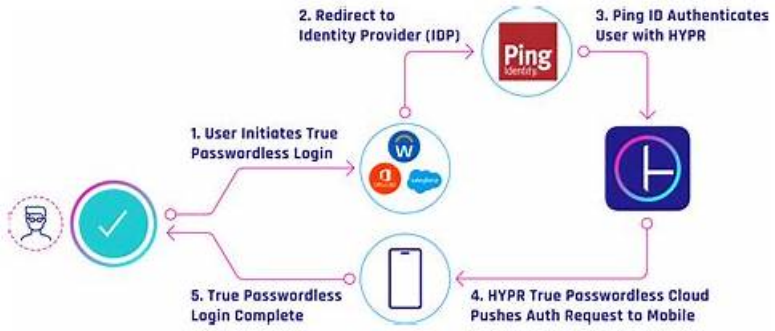
100% Pass Ping Identity - Updated PT-AM-CPE Instant Download



ActualTorrent almost aimed to meet the needs of all candidates who want to pass the PT-AM-CPE exam. If someone who don't have enough time to prepare for their exam, our website provide they with test answers which only need 20-30 hours to grasp; If someone who worry about failed the PT-AM-CPE Exam, our website can guarantee that they can get full refund. In summary, the easiest way to prepare for PT-AM-CPE certification exam is to complete PT-AM-CPE study material.

As you know that a lot of our new customers will doubt about our website or our PT-AM-CPE exam questions though we have engaged in this career for over ten years. So the trust and praise of the customers is what we most want. We will accompany you throughout the review process from the moment you buy PT-AM-CPE Real Exam. We will provide you with 24 hours of free online services to let you know that our PT-AM-CPE study materials are your best tool to pass the exam.

>> PT-AM-CPE Instant Download <<

PT-AM-CPE Latest Test Discount - PT-AM-CPE Test Answers

We are pleased to inform you that we have engaged in this business for over ten years with our Certified Professional - PingAM Exam PT-AM-CPE exam questions. Because of our experience, we are well qualified to take care of your worried about the PT-AM-CPE Preparation exam and smooth your process with successful passing results.

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	• 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 3	• 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 4	• Enhancing Intelligent Access: This domain covers implementing authentication mechanisms, using PingGateway to protect websites, and establishing access control policies for resources.
Topic 5	• 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.

Ping Identity Certified Professional - PingAM Exam Sample Questions (Q38-

Q43):

NEW QUESTION # 38
Which of the following steps must be configured in PingAM to implement mutual TLS using the public key infrastructure (PKI) approach?
Import the trusted certificates into the trust store used by the PingAM web container.
Create a secret store in the realm that maps the appropriate secret ID with the certificate alias in the trust store.18 Select tls_client_auth as the authentication method in the client profile.
Select self_signed_tls_client_auth as the authentication method in the client profile.19 Provide the certificate subject distinguished name in the client profile.20 Configure a revocation check in the client profile.
Register the X.509 certificate in the client profile.

- A. 1, 2, 4, and 5 only
- B. 1, 2, 4, and 6 only
- C. 1, 2, 4, and 7 only
- D. 1, 2, 3, and 5 only

Answer: D

Explanation:
In PingAM 8.0.2, there are two distinct ways to implement Mutual TLS (mTLS) for OAuth2 client authentication: the PKI Approach (CA-signed) and the Self-Signed Approach.21 According to the documentation on "Mutual TLS using PKI":
The PKI approach relies on a chain of trust. The steps required are:
Step 1 (Trust): You must import the CA certificates that signed the client certificates into the truststore of the web container (Tomcat) or the AM Secret Store.22 This allows AM to verify the signature of the client's certificate during the TLS handshake.
Step 2 (Mapping): You must configure a Secret Store and map the am.services.oauth2.tls.client.cert.authentication secret label to the trusted CA aliases.23 Step 3 (Authentication Method): In the OAuth2 Client Profile, you must select tls_client_auth. 24This is the specific OIDC standard string for CA-based mTLS. (In contrast, self_signed_tls_client_auth (Step 4) is used only when you trust individual certificates directly without a CA).25 Step 5 (Identity Mapping): Because multiple clients might have certificates signed by the same CA, you must provide the Subject Distinguished Name (DN) (e.g., CN=myClientApp) in the client profile. PingAM uses this to ensure that the certificate presented by the client during the handshake actually belongs to that specific Client ID.
Why other steps are excluded: Step 7 (Registering the certificate) is only required for the Self-Signed approach, as the PKI approach validates against the CA. Step 6 (Revocation check) is a global provider setting or an optional enhancement, but not a fundamental "must-configure" step for the basic PKI identity mapping logic. Thus, the correct sequence for the PKI approach is 1, 2, 3, and 5, making Option C the correct answer.

NEW QUESTION # 39
Which is the correct simplified TLS handshake sequence needed to authenticate clients using a mutual TLS exchange?

- A. 1. Client sends a request to a server to establish a secure connection
  2. The client sends its certificate to the server
  3. The server presents its certificate in a response to the client
  4. The client sends its session key to the server
  5. The mutually secure connection is established and the client is authenticated
- B. 1. Client sends a request to a server to establish a secure connection
  2. The server presents its certificate in a response to the client
  3. The client sends its certificate to the server
  4. The mutually secure connection is established and the client is authenticated
- C. 1. Client sends a request to a server to establish a secure connection
  2. The server requests the client certificate
  3. The client sends its certificate and the session key to the server
  4. The server sends its certificate to the client if the client certificate and key are valid
  5. The mutually secure connection is established and the client is authenticated
- D. 1. Client sends a certificate in the request to a server to establish a secure connection
  2. The client sends its session key to the server
  3. The server presents its certificate in a response to the client
  4. The mutually secure connection is established and the client is authenticated

Answer: B

Explanation:
Mutual TLS (mTLS) is a security enhancement where both the client and the server provide X.509 certificates to prove their identities.9 In PingAM 8.0.2, mTLS is frequently used for secure "Machine-to-Machine" (M2M) communication, such as between an OAuth2 client and the token endpoint, or between AM and a Directory Server (PingDS).
According to the PingAM documentation on "Secure Network Communication" and "mTLS for OAuth2," the handshake sequence for mTLS follows these logical steps:
Client Hello: The client initiates the request to the server.10
Server Hello & Certificate: The server responds by presenting its own certificate (verifying the server's identity to the client).11 In an mTLS scenario, the server also includes a CertificateRequest message.12 Client Certificate & Key Exchange: The client validates the server's certificate. If valid, the client then sends its own Client Certificate to the server, along with the encrypted pre-master secret or key exchange data.
Verification and Establishment: The server validates the client's certificate against its truststore. If the certificate is trusted and the cryptographic signatures match, the mutually secure connection is established.
Option D represents the most accurate "simplified" sequence. Option A is incorrect because the server presents its certificate before the client sends its own certificate. Option B and C are incorrect because the server always responds to the initial "Client Hello" with its own identity (Server Certificate) before the client proceeds with identity submission. This "handshake" ensures that no data is transmitted until both parties have cryptographically verified each other.

NEW QUESTION # 40
In the default Cloud Developer Kit (CDK) deployment of the forgeops repository, which pods provide the user interface functionality?

- A. admin-ui, end-user-ui, login-ui
- B. am-ui, idm-ui, login-ui
- C. amadmin-ui, idmadmin-ui, login-ui
- D. am-ui, idm-ui, end-user-ui

Answer: A

Explanation:
The Cloud Developer Kit (CDK), part of the forgeops repository, represents the modern approach to deploying the Ping Identity Platform (including PingAM 8.0.2) in a containerized, Kubernetes-native environment. According to the PingAM deployment and ForgeOps documentation, the platform has transitioned from a monolithic architecture-where the user interface was embedded within the AM web application-to a decoupled, microservices-aligned architecture. In a standard CDK deployment, the user interface components are separated into their own distinct pods to allow for independent scaling, updates, and management.
The three specific pods that provide user interface functionality in a default CDK environment are:
admin-ui: This pod hosts the administrative console. It is the centralized interface that administrators use to configure realms, manage identity stores, define authentication trees, and oversee the general health of both PingAM and PingIDM. By separating the administrative UI from the core engine, the platform reduces the attack surface and allows for more granular resource allocation.
end-user-ui: This pod serves the self-service portal for end-users. It is responsible for providing the interface where users can manage their own profiles, update passwords, register Multi-Factor Authentication (MFA) devices, and manage their consent for OAuth2/UMA applications. This UI interacts with the back-end via REST APIs to ensure a seamless and responsive user experience.
login-ui: This is a specialized pod dedicated to the authentication journey. When a user interacts with an "Intelligent Access" tree, the login-ui pod renders the callbacks (such as username prompts, password fields, or MFA challenges). This pod ensures that the presentation layer of the authentication process is modernized and distinct from the heavy processing logic of the PingAM core.
Collectively, these three pods ensure that the "User Interface" layer of the deployment is modular. This architecture is a prerequisite for high-availability deployments and is the standard configuration verified in the ForgeOps documentation for version 8.0.2 deployments.

NEW QUESTION # 41
Which OpenID Connect grant flow is best to use when the relying party knows the user's identifier and wishes to gain consent for an operation from the user by means of a separate authentication device?

- A. Implicit grant
- B. Backchannel request grant
- C. Authorization code grant
- D. Hybrid grant

Answer: B

Explanation:
The scenario described-where a client (Relying Party) already knows who the user is and needs them to authorize an action on a different device-is the primary use case for the Backchannel Request Grant, also known as Client-Initiated Backchannel Authentication (CIBA).
According to the PingAM 8.0.2 documentation on "OpenID Connect Grant Flows" and "CIBA":
Unlike traditional OIDC flows (Implicit, Authorization Code, Hybrid) that require a browser redirect (front-channel) to the OpenID Provider, CIBA is a back-channel flow. It is designed for "decoupled" authentication.
The Trigger: The RP sends a request directly to PingAM's backchannel authentication endpoint, providing a user identifier (like a username or email).
The Consent: PingAM then reaches out to the user's Authentication Device (usually a smartphone with the ForgeRock Authenticator app) via a Push notification.
The Approval: The user approves the request on their phone.
The Tokens: The RP, which has been polling PingAM or waiting for a callback, receives the ID Token and Access Token.
Common real-world examples include a bank teller initiating a login on their terminal which the customer approves on their mobile banking app, or a call center agent verifying a caller's identity via a push notification. Option D is the only flow that supports this decoupled, separate-device architecture. Options A, B, and C are all "Front-channel" flows that require the user's interaction to happen in the same browser session that initiated the request.

NEW QUESTION # 42
Which statements are correct in relation to an OAuth2 token exchange impersonation pattern?
A) The client may want to act as the subject on another service.
B) The client is used by a subject to act on behalf of another subject.
C) The requested token exchange involves a subject token only.
D) The requested token exchange involves a subject and actor token.

- A. A and D only
- B. B and D only
- C. A and C only
- D. B and C only

Answer: A

Explanation:
In PingAM 8.0.2, the OAuth 2.0 Token Exchange (RFC 8693) supports two primary patterns: delegation and impersonation. Understanding the difference between these is critical for secure microservices architecture.
According to the "Demonstrate Impersonation" section of the PingAM documentation, impersonation is a pattern where a client (the "Actor") acts as another identity (the "Subject") in a way that the downstream resource server sees only the Subject's identity.
Statement A is correct: In an impersonation flow, the client (which has been authorized by the user or is a trusted service) requests a token where it effectively "becomes" the subject to interact with another service. The downstream service treats the request as if it were coming directly from the subject, often with the same set of permissions.
Statement D is correct: To perform a token exchange for impersonation, the client must provide specific parameters to the /oauth2/access_token endpoint. It provides the subject_token (representing the identity to be impersonated) and the actor_token (representing the identity of the client/service that is performing the impersonation). PingAM validates both tokens to ensure the "Actor" has the permission to impersonate the "Subject." Why other statements are incorrect: Statement B describes delegation (where an actor acts on behalf of a subject but maintains their own identity in the act claim). Statement C is incorrect because a token exchange inherently requires proving who the requester is (the actor) and whom they represent (the subject). Without both tokens, the AM server cannot verify the authorization relationship required for impersonation. Therefore, the combination of A and D accurately reflects the impersonation pattern in PingAM 8.0.2.

NEW QUESTION # 43
.....

- Free PDF 2026 Unparalleled Ping Identity PT-AM-CPE: Certified Professional - PingAM Exam Instant Download □ Search for [PT-AM-CPE] and download it for free on { www.troytecdumps.com } website □Latest PT-AM-CPE Braindumps
- New Exam PT-AM-CPE Materials □ Reliable PT-AM-CPE Test Tutorial □ PT-AM-CPE Flexible Learning Mode □ □ Search for ⇛ PT-AM-CPE ⇚ and obtain a free download on 【 www.pdfvce.com 】 □Valid PT-AM-CPE Exam Dumps
- Valid Test PT-AM-CPE Tips □ PT-AM-CPE Valid Test Vce □ PT-AM-CPE Official Practice Test □ Easily obtain free download of ▷ PT-AM-CPE ◁ by searching on ⇛ www.exam4labs.com ⇚ □Books PT-AM-CPE PDF
- PT-AM-CPE Valid Test Vce □ PT-AM-CPE Valid Test Vce □ Valid Test PT-AM-CPE Tips □ Search for ▷ PT-AM-CPE ◁ and download it for free on 「 www.pdfvce.com 」 website □Reliable PT-AM-CPE Test Tutorial
- Pass Guaranteed Quiz 2026 PT-AM-CPE: Accurate Certified Professional - PingAM Exam Instant Download □ Download ➥ PT-AM-CPE □ for free by simply entering ➥ www.practicevce.com □ website □PT-AM-CPE Valid Test Vce
- New PT-AM-CPE Exam Format ◂ New Exam PT-AM-CPE Materials □ Valid Test PT-AM-CPE Tips □ Easily obtain [PT-AM-CPE] for free download through ➥ www.pdfvce.com □ □Books PT-AM-CPE PDF
- PT-AM-CPE Online Test □ PT-AM-CPE Flexible Learning Mode □ Latest PT-AM-CPE Exam Price □ Search for □ PT-AM-CPE □ on ☀ www.testkingpass.com □☀□ immediately to obtain a free download □Reliable PT-AM-CPE Test Tutorial
- Latest PT-AM-CPE Exam Price □ PT-AM-CPE Valid Test Vce □ Verified PT-AM-CPE Answers □ Search for □ PT-AM-CPE □ and download exam materials for free through ➠ www.pdfvce.com □ □PT-AM-CPE Online Test
- Latest PT-AM-CPE Braindumps □ Latest PT-AM-CPE Braindumps □ PT-AM-CPE Flexible Learning Mode □ Open ➽ www.torrentvce.com □ and search for " PT-AM-CPE " to download exam materials for free □PT-AM-CPE Online Test
- Books PT-AM-CPE PDF □ Verified PT-AM-CPE Answers □ PT-AM-CPE Flexible Learning Mode □ Search on 【 www.pdfvce.com 】 for ▷ PT-AM-CPE ◁ to obtain exam materials for free download □Books PT-AM-CPE PDF
- Reliable PT-AM-CPE Test Sims □ Test PT-AM-CPE Guide □ Practice PT-AM-CPE Test Online □ Simply search for □ PT-AM-CPE □ for free download on □ www.prep4away.com □ □Practice PT-AM-CPE Test Online
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, learnith.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes