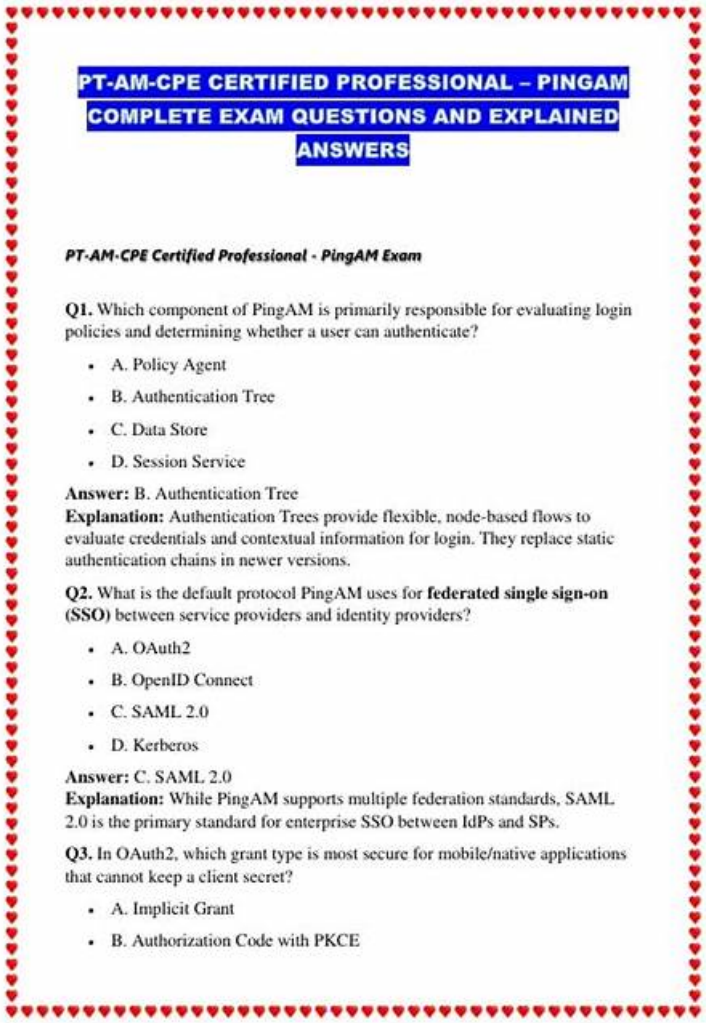
PT-AM-CPE模擬体験 & PT-AM-CPE無料問題


PT-AM-CPE CERTIFIED PROFESSIONAL – PINGAM
COMPLETE EXAM QUESTIONS AND EXPLAINED ANSWERS

PT-AM-CPE Certified Professional - PingAM Exam

Q1. Which component of PingAM is primarily responsible for evaluating login policies and determining whether a user can authenticate?

- A. Policy Agent
- B. Authentication Tree
- C. Data Store
- D. Session Service

Answer: B. Authentication Tree
Explanation: Authentication Trees provide flexible, node-based flows to evaluate credentials and contextual information for login. They replace static authentication chains in newer versions.

Q2. What is the default protocol PingAM uses for **federated single sign-on (SSO)** between service providers and identity providers?

- A. OAuth2
- B. OpenID Connect
- C. SAML 2.0
- D. Kerberos

Answer: C. SAML 2.0
Explanation: While PingAM supports multiple federation standards, SAML 2.0 is the primary standard for enterprise SSO between IdPs and SPs.

Q3. In OAuth2, which grant type is most secure for mobile/native applications that cannot keep a client secret?

- A. Implicit Grant
- B. Authorization Code with PKCE

証明書は私たちの日常生活で重要です。現在、PT-AM-CPE試験に合格するすべての受験者に、選択可能な3つの異なるバージョンを提供しています。 PT-AM-CPE試験問題のAPPバージョンは、オフライン状態で機能します。クイズ準備を使用する場合、最新のPT-AM-CPE試験トレントをいつでもどこでも使用できます。オフライン状態のPT-AM-CPE実践ガイドを使用して、どのようにして学習を楽しむことができますか？オフライン状態で動作するバージョンをダウンロードするだけで、初めてPT-AM-CPEクイズトレントのバージョンをオンラインで使用する必要があります。

Ping Identity PT-AM-CPE 認定試験の出題範囲：

トピック	出題範囲
トピック 1	• 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.
トピック 2	• 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.
トピック 3	• Enhancing Intelligent Access: This domain covers implementing authentication mechanisms, using PingGateway to protect websites, and establishing access control policies for resources.

トピック 4	• Federating Across Entities Using SAML2: This domain covers implementing single sign-on using SAML v2.0 and delegating authentication responsibilities between SAML2 entities.
トピック 5	• Improving Access Management Security: This domain focuses on strengthening authentication security, implementing context-aware authentication experiences, and establishing continuous risk monitoring throughout user sessions.

100％合格率のPing Identity PT-AM-CPE模擬体験 & 合格スムーズPT-AM-CPE無料問題 | 権威のあるPT-AM-CPE無料サンプル

献身と熱意を持ってPT-AM-CPEガイド資料を段階的に学習する場合、必死に試験に合格することを保証します。学習資料の権威あるプロバイダーとして、潜在顧客からより多くの注目を集めるために、常に同等のテストと比較してPT-AM-CPE模擬テストの高い合格率を追求しています。将来的には、PT-AM-CPE試験トレントは、高い合格率でより魅力的で素晴らしいものになると信じています。

Ping Identity Certified Professional - PingAM Exam 認定 PT-AM-CPE 試験問題 (Q91-Q96):

質問 # 91
Which of the following code examples inserts a may_act claim to the resulting token in a PingAM implementation?

- A. var mayAct = /* is a JSON object with may act property data */ token.addMayAct(mayAct)
- B. var mayAct = /* is a JSON object with may act property data */ requestedToken.setMayAct(mayAct)
- C. var mayAct = /* is a JSON object with may act property data */ requestedToken.addMayAct(mayAct)
- D. var mayAct = /* is a JSON object with may act property data */ token.setMayAct(mayAct)

正解：C

解説：
In PingAM 8.0.2, the OAuth 2.0 Token Exchange (RFC 8693) implementation allows for complex identity delegation scenarios. The may_act claim is a specific claim used to indicate that one entity is authorized to act on behalf of another. When customizing the behavior of token exchange via the OAuth2 Token Exchange Script, developers interact with specific scriptable objects provided by the PingAM engine.
According to the "Scripting API" for OAuth2 and the "Token Exchange" developer guide, the requestedToken object is the primary interface used to modify the structure of the token being issued during the exchange. To insert the may_act claim, the API provides the addMayAct() method.
The may_act claim is technically a JSON object that contains a sub (subject) claim of the entity that is allowed to act as the subject of the token. In the scripting environment:
The requestedToken variable represents the token currently being minted.
The .addMayAct() method is the defined function signature to append this delegation metadata.
Why other options are incorrect:
Options A and D: The object name token is not the standard binding used for the target token in the Token Exchange script context; requestedToken is the correct binding.
Option C: The method name setMayAct is incorrect. The PingAM API uses the add prefix for these types of claims (similar to addActor), reflecting the underlying structure where these claims are added to the claim set of the JWT.
Using the correct syntax requestedToken.addMayAct(mayAct) ensures that the resulting Access Token or ID Token contains the correctly formatted delegation information required by resource servers to validate that the "Actor" has the permission to represent the "Subject."

質問 # 92
When making a request to the /oauth2/access_token endpoint using the JWT profile client authentication method, which parameter is used to provide the JWT value?

- A. client_id

- B. client_assertion
- C. client_token_value
- D. client_credentials

正解：B

解説：
PingAM 8.0.2 supports advanced client authentication methods defined in the OpenID Connect and OAuth 2.0 specifications, including private_key_jwt and client_secret_jwt. These methods allow a client to authenticate without sending a static password/secret in the request. Instead, the client generates and signs a JSON Web Token (JWT).
According to the "OAuth 2.0 Client Authentication" and "JWT Profile for Client Authentication" (RFC 7523) documentation, when a client sends this JWT to the /oauth2/access_token endpoint, it must use the client_assertion parameter.
The request must also include the client_assertion_type parameter, which must be set to the constant value: urn:ietf:params:oauth:client-assertion-type:jwt-bearer.
Option A (client_credentials) is a grant type, not a parameter for providing a JWT.
Option B (client_token_value) is not a standard OAuth2 parameter name.
Option C (client_id) is often included in the request, but it is the identifier of the client, not the container for the cryptographic assertion itself.
When PingAM receives a request with a client_assertion, it extracts the JWT, verifies the signature using the client's public key (stored in the client's profile or retrieved via a JWKS URI), and validates the standard claims (iss, sub, aud, exp). This method is significantly more secure than simple secrets because it proves the client possesses the private key and limits the window for replay attacks through the token's expiration claim.

質問 # 93
Which authentication nodes can be used for risk analysis related to device context?
A) Device Profile Collector node1
B) Device GeoFencing node2
C) Device Profile Save node3
D) Device Tampering Verification node
E) Device Location Match node4
F) Device Match node
Multiple Choice Options:

- A. A, B, C, and D
- B. A, C, D, and E
- C. B, C, D, and F
- D. B, D, E, and F

正解：D

解説：
In PingAM 8.0.2, the Intelligent Access framework categorizes authentication nodes based on their primary function. While nodes like the Device Profile Collector (A) and Device Profile Save (C) are essential for the device context workflow, they are considered "Utility" or "Data Collection/Persistence" nodes. They do not perform analysis or branching logic based on risk scores or comparisons themselves; they simply gather metadata or write it to the user's profile.
According to the "Authentication Node Reference," Risk Analysis related to device context is performed by nodes that compare real-time data against a baseline or a set of rules. These nodes include:
Device Geofencing node (B): Analyzes the current device's location against a set of predefined "trusted" coordinates to determine if the user is within a permitted geographical area.5 Device Tampering Verification node (D): Assesses the integrity of the device (typically for mobile) to detect if it has been rooted, jailbroken, or otherwise compromised.6 Device Location Match node (E): Compares the current device's location with the user's historical location data stored in their profile to identify anomalies.7 Device Match node (F): Evaluates the current device's hardware and software signatures against a list of "trusted devices" previously registered by the user.8 Nodes B, D, E, and F all provide branching outcomes (e.g., True/False, Inside/Outside, Success/Failure) based on a risk evaluation of the device context. This makes Option B the correct selection. Understanding the distinction between a "Collector" and an "Evaluator" is vital for designing effective authentication journeys that can trigger step-up authentication or deny access when device-based risk signals are detected.

質問 # 94

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

正解：D

解説：
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.

質問 # 95
Which one of the default PingAM audit log file contains messages related to changes made to sessions by end users?

- A. activity.audit.json
- B. config.audit.json
- C. access.audit.json
- D. authentication.audit.json

正解：C

解説：
In PingAM 8.0.2, the audit logging service is designed to provide a comprehensive record of events for security, compliance, and troubleshooting. The audit logs are categorized by the type of event they record. According to the "Audit Logging Reference," PingAM generates several default log files, typically in JSON format.
The access.audit.json file is the primary log for events related to the lifecycle of a session and access to resources. This includes:
Session Creation: When a user successfully authenticates and a new session is established.
Session Termination: When a user logs out or a session expires.
Session Updates: Any changes made to the session, such as a Session Upgrade or modification of session properties by the end user or an application.
Policy Evaluations: Records of when a user requests access to a protected resource and the resulting permit or deny decision.
By contrast, the config.audit.json (Option B) records administrative changes to the system configuration (e.g., modifying a realm or a node). The authentication.audit.json (Option C) focuses specifically on the steps within an authentication tree, such as which nodes were visited and whether they succeeded or failed. While session changes happen after or as a result of authentication, the resulting session management event is logged in the access audit. The activity.audit.json (Option D) is generally used for internal system tasks and background processes. Therefore, for monitoring end-user session modifications, the access.audit.json is the correct authoritative source defined in the PingAM 8 documentation.

質問 # 96
.....

試験の準備をするためにIt-PassportsのPing IdentityのPT-AM-CPE試験トレーニング資料を買うのは冒険的行為と思ったとしたら、あなたの人生の全てが冒険なことになります。一番遠いところへ行った人はリスクを背負うことを恐れない人です。また、It-PassportsのPing IdentityのPT-AM-CPE試験トレーニング資料が信頼できるのは多くの受験生に証明されたものです。It-PassportsのPing IdentityのPT-AM-CPE試験トレーニング資料を利用したらきっと成功できますから、It-Passportsを選ばない理由はないです。

PT-AM-CPE無料問題: https://www.it-passports.com/PT-AM-CPE.html

- 認定するPT-AM-CPE模擬体験試験-試験の準備方法-ユニークなPT-AM-CPE無料問題 □ 検索するだけで[www.xhs1991.com]から➥ PT-AM-CPE □を無料でダウンロードPT-AM-CPE模擬モード
- PT-AM-CPE更新版 □ PT-AM-CPE受験記 □ PT-AM-CPEトレーリング学習 □ （ www.goshiken.com ）サイトにて最新☀ PT-AM-CPE □☀□問題集をダウンロードPT-AM-CPE教育資料
- 認定するPT-AM-CPE模擬体験試験-試験の準備方法-ユニークなPT-AM-CPE無料問題 □ ➠ www.mogiexam.com □を入力して{ PT-AM-CPE }を検索し、無料でダウンロードしてくださいPT-AM-CPE問題集
- 高品質なPT-AM-CPE模擬体験 - 合格スムーズPT-AM-CPE無料問題 | 実際的なPT-AM-CPE無料サンプル □「 www.goshiken.com 」で▸ PT-AM-CPE ◂を検索し、無料でダウンロードしてくださいPT-AM-CPE模擬問題
- PT-AM-CPE模擬問題 □ PT-AM-CPE日本語解説集 □ PT-AM-CPE受験記 □ ウェブサイト➡ www.passtest.jp □□□から➠ PT-AM-CPE □を開いて検索し、無料でダウンロードしてくださいPT-AM-CPE模擬問題
- PT-AM-CPE模擬問題 □ PT-AM-CPE模擬モード □ PT-AM-CPE模擬試験サンプル □ サイト⇒ www.goshiken.com ⇐で《 PT-AM-CPE 》問題集をダウンロードPT-AM-CPE赤本合格率
- PT-AM-CPE認証試験 □ PT-AM-CPE日本語解説集 □ PT-AM-CPE日本語解説集 □ ▹ www.passtest.jp ◃サイトにて最新▸ PT-AM-CPE ◂問題集をダウンロードPT-AM-CPE日本語版受験参考書
- PT-AM-CPE日本語独学書籍 □ PT-AM-CPE赤本合格率 □ PT-AM-CPE認証試験 □ ➥ www.goshiken.com □を開き、“PT-AM-CPE”を入力して、無料でダウンロードしてくださいPT-AM-CPE問題集
- よくできたPT-AM-CPE模擬体験 - 資格試験のリーダー - 信頼できるPT-AM-CPE無料問題 □ （ www.it-passports.com ）を入力して《 PT-AM-CPE 》を検索し、無料でダウンロードしてくださいPT-AM-CPE赤本合格率
- PT-AM-CPE教育資料 □ PT-AM-CPE日本語版参考資料 □ PT-AM-CPE受験記 □ □ www.goshiken.com □ サイトで（ PT-AM-CPE ）の最新問題が使えるPT-AM-CPE模擬試験サンプル
- PT-AM-CPE日本語独学書籍 □ PT-AM-CPE日本語解説集 □ PT-AM-CPE日本語版受験参考書 □ ➤ jp.fast2test.com □にて限定無料の➥ PT-AM-CPE □問題集をダウンロードせよPT-AM-CPE日本語版参考資料
- jaysonxupm385743.life3dblog.com, joantegr664908.wikimillions.com, 45listing.com, shaniannbw281972.wikimillions.com, sound-social.com, leaiqve752885.mappywiki.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, heiditxkl114039.blogsvirals.com, bookmarkworm.com, worldlistpro.com, Disposable vapes