

Testking PAP-001 Exam Questions & PAP-001 Hottest Certification



BTW, DOWNLOAD part of Test4Engine PAP-001 dumps from Cloud Storage: <https://drive.google.com/open?id=10cAUNKTj4h6ykbGp1NwxKg82j1pbpKE>

Our PAP-001 exam materials can help you stand out in the fierce competition. After using our PAP-001 study questions, you have a greater chance of passing the PAP-001 certification, which will greatly increase your soft power and better show your strength. Our PAP-001 training guide can bring you something. After you have used our PAP-001 learning braindump, you will certainly have your own experience. Now let's take a look at why a worthy product of your choice is our PAP-001 actual exam.

Ping Identity PAP-001 Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none">• Installation and Initial Configuration: This section of the exam measures skills of System Engineers and reviews installation prerequisites, methods of installing or removing PingAccess, and securing configuration database passwords. It explains the role of run.properties entries and outlines how to set up a basic on-premise PingAccess cluster.
Topic 2	<ul style="list-style-type: none">• Security: This section of the exam measures skills of Security Administrators and highlights how to manage certificates and certificate groups. It covers the association of certificates with virtual hosts or listeners and the use of administrator roles for authentication management.
Topic 3	<ul style="list-style-type: none">• General Maintenance and File System: This section of the exam measures the skills of System Engineers and addresses maintenance tasks such as license management, backups, configuration imports or exports, auditing, and product upgrades. It also includes the purpose of log files and an overview of the PingAccess file system structure with important configuration files.
Topic 4	<ul style="list-style-type: none">• Policies and Rules: This section of the exam measures the skills of Security Administrators and focuses on how PingAccess evaluates paths for applying policies and resources. It covers the role of different rule types, their configuration, and the implementation of rule sets and rule set groups for consistent policy enforcement.
Topic 5	<ul style="list-style-type: none">• General Configuration: This section of the exam measures skills of Security Administrators and introduces the different object types within PingAccess such as applications, virtual hosts, and web sessions. It explains managing application resource properties, creating web sessions, configuring identity mappings, and navigating the administrative console effectively.

>> Testking PAP-001 Exam Questions <<

PAP-001 Hottest Certification & Test PAP-001 Price

Once the clients order our PAP-001 cram training materials we will send the PAP-001 exam questions quickly by mails. The clients abroad only need to fill in correct mails and then they get our PAP-001 training guide conveniently. Our PAP-001 cram training materials provide the version with the language domestically and the version with the foreign countries' language so that the clients at home and abroad can use our PAP-001 Study Tool conveniently. And after study for 20 to 30 hours, you can pass the PAP-001 exam with ease.

Ping Identity Certified Professional - PingAccess Sample Questions (Q11-Q16):

NEW QUESTION # 11

Developers report an issue with an application that is protected by PingAccess. Certain requests are not providing claims that are part of the access token.

What should the administrator add for the access token claims?

- A. An OAuth attribute rule
- B. A web session attribute rule
- C. An identity mapping definition
- D. An authentication requirement definition

Answer: A

Explanation:

In PingAccess, when an application relies on claims from an OAuth access token, you must configure PingAccess to evaluate those claims and potentially inject them into headers for the backend application.

* Exact Extract from PingAccess documentation:

"OAuth rules allow you to evaluate claims in OAuth access tokens. You can configure PingAccess to look at specific claims and enforce policies or pass them to target applications."

"To extract attributes from an access token, configure an OAuth Attribute Rule." This clearly matches option D.

Analysis of each option:

* A. An authentication requirement definition

* Incorrect. Authentication requirements determine how users authenticate to applications (OIDC provider, etc.), but do not manage access token claims.

* B. A web session attribute rule

* Incorrect. Web session attribute rules map attributes from the authenticated user's web session (SSO session), not from OAuth access tokens.

* C. An identity mapping definition

* Incorrect. Identity mappings transform user attributes (from IdP to app), but they don't directly pull claims from OAuth tokens.

* D. An OAuth attribute rule

* Correct. This rule is specifically designed to extract and enforce policies on claims from OAuth access tokens.

Therefore, the correct answer is D. An OAuth attribute rule.

Reference: PingAccess Administration Guide - Rules # OAuth Attribute Rules.

NEW QUESTION # 12

Which of the following is a processing rule?

- A. Web Session Attribute
- B. HTTP Request Parameter
- C. Cross-Origin Request
- D. HTTP Request Header

Answer: C

Explanation:

PingAccess rules are categorized into Access Control Rules and Processing Rules.

* Processing Rules modify or add to HTTP requests and responses.

* Cross-Origin Request (CORS) is specifically listed as a Processing Rule, because it modifies response headers to support cross-origin requests.

Exact Extract:

"Processing rules apply to HTTP traffic, such as Cross-Origin Resource Sharing (CORS), header injection, or response modification."

- * Option A (Web Session Attribute) is an access control rule.
 - * Option B (Cross-Origin Request) is correct - this is a processing rule.
 - * Option C (HTTP Request Parameter) is an access control rule.
 - * Option D (HTTP Request Header) is an access control rule.
- Reference: PingAccess Administration Guide - Rules Overview

NEW QUESTION # 13

A company uses an internally based legacy PKI solution that does not adhere to the Certification Path Validation section of RFC-5280. Which configuration option needs to be enabled when creating Trusted Certificate Groups in PingAccess?

- A. Use Java Trust Store
- **B. Validate disordered certificate chains**
- C. Skip Certificate Date Check
- D. Deny when unable to determine revocation status

Answer: B

Explanation:

Legacy PKIs often provide certificate chains that are out of order or non-compliant with RFC-5280 path validation. PingAccess provides an option in Trusted Certificate Groups called Validate disordered certificate chains to allow chaining even if the order is not RFC-5280 compliant.

Exact Extract:

"Enable Validate disordered certificate chains when the certificate chain is not in RFC-5280 compliant order but should still be accepted."

- * Option A is incorrect; using the Java trust store is unrelated to PKI ordering.
- * Option B is correct - this setting allows PingAccess to process disordered certificate chains.
- * Option C is incorrect; date checks are unrelated to RFC-5280 path ordering.
- * Option D is incorrect; revocation status handling does not address legacy PKI ordering issues.

Reference: PingAccess Administration Guide - Trusted Certificate Groups

NEW QUESTION # 14

What is the purpose of the admin.auth configuration setting?

- A. To configure SSO for the administrative user interface.
- B. To define the method to use for authenticating to the administrative API.
- C. To enable automatic authentication to the PingAccess administrative console.
- **D. To override the SSO configuration for the administrative user interface.**

Answer: D

Explanation:

The admin.auth setting in the run.properties file is used to specify a fallback authentication method for the administrative console.

Exact Extract from official documentation:

"To define a fallback administrator authentication method if the OIDC token provider is unreachable, enable the admin.auth=native property in the run.properties file. This overrides any configured administrative authentication to basic authentication." This makes it clear that the purpose of admin.auth is to override any configured SSO for the admin UI and enforce native (basic) authentication instead.

- * Option A is incorrect because the admin.auth setting does not configure SSO. SSO for the admin UI is configured separately.
- * Option B is incorrect because this setting does not apply to the administrative API; it specifically applies to the admin UI console.
- * Option C is correct because it directly reflects the documented behavior: admin.auth overrides SSO configuration for the administrative UI and enables native authentication.
- * Option D is incorrect because the setting does not enable automatic authentication. It still requires credentials, but falls back to basic auth.

Reference: PingAccess User Interface Reference Guide - Configuring Admin UI SSO Authentication

NEW QUESTION # 15

An API is hosted onsite and is using only header-based Identity Mapping. It is exposed to all clients running on the corporate

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, Disposable vapes

DOWNLOAD the newest Test4Engine PAP-001 PDF dumps from Cloud Storage for free: <https://drive.google.com/open?id=10cAUNKTj4h6ykbGp1NwxKg82j1pbpKE>