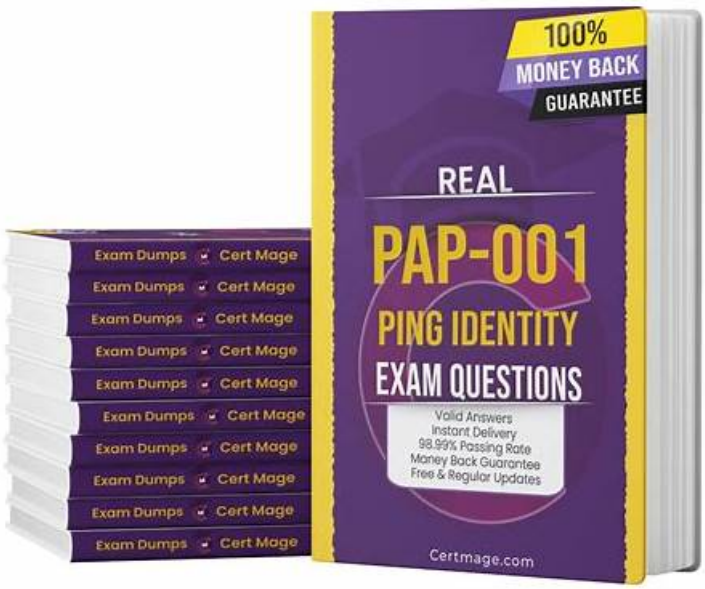
PAP-001 Certification Exam Cost - PAP-001 Dump Check



The company is preparing for the test candidates to prepare the PAP-001 exam guide professional brand, designed to be the most effective and easiest way to help users through their want to get the test PAP-001 certification and obtain the relevant certification. In comparison with similar educational products, our PAP-001 Training Materials are of superior quality and reasonable price, so our company has become the top enterprise in the international market. Our PAP-001 practice materials have been well received mainly for the advantage of high pass rate as 99% to 100%.

Our PAP-001 Study Materials are written by experienced experts in the industry, so we can guarantee its quality and efficiency. The content of our PAP-001 study materials is consistent with the proposition law all the time. We can't say it's the best reference, but we're sure it won't disappoint you. This can be borne out by the large number of buyers on our website every day. A wise man can often make the most favorable choice, I believe you are one of them.

>> PAP-001 Certification Exam Cost <<

PAP-001 Dump Check | Certification PAP-001 Test Answers

ActualTestsIT is a wonderful study platform that contains our hearty wish for you to pass the exam by our PAP-001 exam materials. So our responsible behaviors are our instinct aim and tenet. By devoting in this area so many years, we are omnipotent to solve the problems about the PAP-001 learning questions with stalwart confidence. we can claim that only studing our PAP-001 study guide for 20 to 30 hours, then you will pass the exam for sure.

Ping Identity PAP-001 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• Product Overview: This section of the exam measures skills of Security Administrators and focuses on understanding PingAccess features, functionality, and its primary use cases. It also covers how PingAccess integrates with other Ping products to support secure access management solutions.
Topic 3	• 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.

Ping Identity Certified Professional - PingAccess Sample Questions (Q34-Q39):

NEW QUESTION # 34
According to a new business requirement, critical applications require dual-factor authentication when specific resources are accessed in those applications. Which configuration object should the administrator use in the applications?

- A. Authentication Requirements
- B. UI Authentication
- C. Auth Token Management
- D. Authentication Challenge Policy

Answer: A

Explanation:
PingAccess enforces step-up or multi-factor authentication usingAuthentication Requirements, which can be applied to specific resources within an application.
Exact Extract:
"Authentication requirements allow administrators to configure additional authentication (for example, MFA) when accessing sensitive application resources."
* Option A (UI Authentication)applies to access to theadmin console, not application resources.
* Option B (Auth Token Management)relates to OAuth token lifetimes and refresh, not MFA enforcement.
* Option C (Authentication Requirements)is correct - these rules enforce MFA or step-up auth for specific URLs/resources.
* Option D (Authentication Challenge Policy)governs how failed auth challenges are presented but does not enforce MFA.
Reference:PingAccess Administration Guide -Authentication Requirements

NEW QUESTION # 35
Which of the following is a processing rule?

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

Answer: D

Explanation:
PingAccess rules are categorized intoAccess Control RulesandProcessing Rules.
* Processing Rulesmodify or add to HTTP requests and responses.
* Cross-Origin Request (CORS)is specifically listed as aProcessing 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 # 36
A company uses an internally based legacy PKI solution that does not adhere to theCertification Path Validationsection of RFC-5280. Which configuration option needs to be enabled when creating Trusted Certificate Groups in PingAccess?

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

Answer: B

Explanation:
Legacy PKIs often provide certificate chains that areout of orderor non-compliant with RFC-5280 path validation. PingAccess provides an option in Trusted Certificate Groups calledValidate disordered certificate chainsto allow chaining even if the order is not RFC-5280 compliant.
Exact Extract:
"EnableValidate disordered certificate chainswhen the certificate chain is not in RFC-5280 compliant order but should still be accepted."
* Option Ais incorrect; using the Java trust store is unrelated to PKI ordering.
* Option Bis correct - this setting allows PingAccess to process disordered certificate chains.
* Option Cis incorrect; date checks are unrelated to RFC-5280 path ordering.
* Option Dis incorrect; revocation status handling does not address legacy PKI ordering issues.
Reference:PingAccess Administration Guide -Trusted Certificate Groups

NEW QUESTION # 37
An application requires MFA for URLs that are considered high risk. Which action should the administrator take to meet this requirement?

- A. Apply an HTTP Request Parameter rule to the resource.
- B. Create an Authentication Requirement named MFA_Required.
- C. Apply a Web Session Attribute rule to the resource.
- D. Apply an Authentication Requirements rule to the resource.

Answer: D

Explanation:
PingAccess allows fine-grained authentication enforcement by applyingAuthentication Requirement rulesat the resource level. These rules can invoke MFA flows based on request context or policy.
Exact Extract:
"Authentication requirement rules determine whether PingAccess challenges a user to authenticate again (for example, with MFA) before allowing access to a protected resource."
* Option Ais incomplete. Creating a requirement does nothing unless it is applied.
* Option Bis correct because applying the Authentication Requirement rule to thespecific resource (URL)enforces MFA only for that resource.
* Option Cis incorrect; Web Session Attribute rules are about evaluating existing session attributes, not triggering MFA.
* Option Dis incorrect; HTTP Request Parameter rules are used to evaluate request data, not enforce MFA policies.
Reference:PingAccess Administration Guide -Authentication Requirements

NEW QUESTION # 38
An administrator needs to use attributes that are not currently available in theIdentity Mapping Attribute Namedropdown. Which action should the administrator take?

- A. Request that the additional attributes be added by the web developer
- B. Create a Web Session Attribute rule for the additional attributes
- C. Create a Rewrite Content rule for the additional attributes
- D. Request that the additional attributes be added by the token provider administrator

Answer: D

Explanation:
Identity Mapping in PingAccess relies on attributes provided by thetoken provider(e.g., PingFederate, OIDC provider). If the desired attributes are not present in the dropdown, it means they are not being provided in the token or userinfo response.
Exact Extract:
"Attributes available in identity mappings are those provided in the web session by the token provider. If attributes are missing, they must be added to the token by the identity provider."
* Option Ais correct - the token provider administrator must configure the IdP to include the additional attributes.
* Option Bis incorrect - rewrite rules modify content but do not supply new identity attributes.
* Option Cis incorrect - developers cannot directly add identity attributes; they must come from the IdP.
* Option Dis incorrect - Web Session Attribute rules only evaluate available attributes; they don't create new ones.
Reference:PingAccess Administration Guide -Identity Mapping and Attributes

NEW QUESTION # 39
......