ExamsNest

Your Ultimate Exam Preparation Hub

Vendor: Ping Identity

Code: PAP-001

Exam: Certified Professional - PingAccess

https://www.examsnest.com/exam/pap-001/

QUESTIONS & ANSWERS

DEMO VERSION

Version: 4.0

Question: 1

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 override the SSO configuration for the administrative user interface.
D. To enable automatic authentication to the PingAccess administrative console.

Answer: C

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

Question: 2

An administrator is setting up a new PingAccess cluster with the following:
• Administrative node hostname: pa-admin.company.com

• Replica administrative node hostname: pa-admin2.company.com
Which two options in the certificate would be valid for the administrative node key pair? (Choose 2.)

A. Issuer = pa-admin.company.com
B. Subject = *.company.com
C. Subject = pa-admin.company.com
D. Subject Alternative Names = pa-admin.company.com, pa-admin2.company.com
E. Subject = pa-admin2.company.com

Answer: B, D

Explanation:

Exact Extract (from PingAccess documentation):
“The key pair that you create for the CONFIG QUERY listener must include both the administrative node and the replica administrative node. To make sure the replica administrative node is included, you can either use a wildcard certificate or define subject alternative names in the key pair that use the replica administrative node’s DNS name.”
Why B and D are correct:
*B . Subject = .company.com — A wildcard certificate for *.company.com is valid for both pa-admin.company.com and pa-admin2.company.com, satisfying the documented requirement that the key pair include both hostnames for the CONFIG QUERY listener.
D . Subject Alternative Names = pa-admin.company.com, pa-admin2.company.com — Explicitly placing both DNS names in the SAN extension also satisfies the requirement that the certificate cover both the administrative node and the replica administrative node.

Why the other options are incorrect:
A . Issuer = pa-admin.company.com — The Issuer field identifies the certificate authority (CA) that signed the certificate, not the service hostname. Setting the issuer to a host value is not how X.509 server certificates are validated and would not meet the hostname matching requirement.
C . Subject = pa-admin.company.com — While this covers the administrative node, it does not include the replica administrative node. Without a wildcard or SAN entries, it fails the requirement that the key pair include both hostnames.
E . Subject = pa-admin2.company.com — Similarly, this would only cover the replica administrative node and not the primary administrative node, failing the requirement.
Reference:
Configuring replica administrative nodes (PingAccess User Interface Reference Guide)
Configuring a PingAccess cluster (PingAccess documentation)
Certificates (PingAccess User Interface Reference Guide)

Question: 3

An organization wants to take advantage of a new product feature that requires upgrading the PingAccess cluster from 7.3 to the current version. The administrator downloads the required files and places the files on the PingAccess servers. What should the administrator do next?

A. Upgrade the Admin Console.
B. Disable cluster communication.
C. Disable Key Rolling.
D. Upgrade the Replica Admin.

Answer: A

Explanation:

When upgrading a PingAccess cluster, the Admin Console node must always be upgraded first before any replica admin or engine nodes. This ensures that the configuration and schema changes introduced in the new version are properly applied and replicated.
Exact Extract (from PingAccess documentation):
"In a clustered environment, you must first upgrade the administrative console node before upgrading any replica administrative nodes or engine nodes."
Why A is correct:
A . Upgrade the Admin Console — This is correct because the admin console node acts as the configuration master in a PingAccess cluster. Upgrading it first ensures the new version schema is available to replicas and engines.
Why the other options are incorrect:
B . Disable cluster communication — This is not required for standard upgrades. Cluster communication remains in place to synchronize changes after the upgrade.
C . Disable Key Rolling — Key rolling is unrelated to the upgrade process. It is a feature used for key rotation, not version upgrades.
D . Upgrade the Replica Admin — This is incorrect because upgrading a replica admin before the primary administrative console is against the documented procedure and would cause replication issues.
Reference:
Upgrading PingAccess in a Clustered Environment (PingAccess Upgrade Guide)
PingAccess Administration Guide – Upgrade Process

Question: 4

Where in the administrative console should an administrator make user attributes available as HTTP request headers?

A. Site Authenticators
B. Identity Mappings
C. Web Sessions
D. HTTP Requests

Answer: B

Explanation:

PingAccess uses Identity Mappings to take identity attributes provided by the authentication source (e.g., PingFederate, OpenID Connect) and map them into HTTP request headers for back-end

applications.
Exact Extract:
“An identity mapping allows you to map identity attributes from the user’s session to HTTP headers, cookies, or query parameters that are then forwarded to the target application.”
Option A (Site Authenticators) is incorrect because Site Authenticators configure how PingAccess communicates with applications requiring authentication, not how attributes are inserted into headers.
Option B (Identity Mappings) is correct — this is the feature designed specifically to expose user attributes to applications via HTTP headers.
Option C (Web Sessions) manages how sessions are stored and validated, but not the mapping of attributes into requests.
Option D (HTTP Requests) refers to request/response processing rules, but attributes are not mapped here.
Reference: PingAccess Administration Guide – Identity Mapping

Question: 5

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

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

Answer: B

Explanation:

PingAccess allows fine-grained authentication enforcement by applying Authentication Requirement rules at 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 A is incomplete. Creating a requirement does nothing unless it is applied.
Option B is correct because applying the Authentication Requirement rule to the specific resource (URL) enforces MFA only for that resource.
Option C is incorrect; Web Session Attribute rules are about evaluating existing session attributes, not triggering MFA.
Option D is incorrect; HTTP Request Parameter rules are used to evaluate request data, not enforce MFA policies.
Reference: PingAccess Administration Guide – Authentication Requirements

ExamsNest

Your Ultimate Exam Preparation Hub

Thank You for trying the PDF Demo

Vendor: Ping Identity

Code: PAP-001

Exam: Certified Professional - PingAccess

https://www.examsnest.com/exam/pap-001/

Use Coupon "**SAVE15**" for extra 15% discount on the purchase of Practice Test Software. Test your Exam preparation with actual exam questions.

Start Your Preparation