DUMPSBOSS.

Certified ProfessionalPingAccess

Ping Identity PAP-001

Version Demo

Total Demo Questions: 9

Total Premium Questions: 93

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, PingAccess Architecture	2
Topic 2, PingAccess Installation	9
Topic 3, PingAccess Configuration	71
Topic 4, PingAccess Administration	8
Topic 5, PingAccess Troubleshooting	3
Total	93

QUESTION NO: 1

An application is hosted on a server that requires clients to authenticate using a username:password pair. This application is behind PingAccess, which is acting as a gateway. What action should the administrator take to allow PingAccess to access the application?

A. Apply an Identity Mapping that includes the username and password

B. Apply a valid Web Session that contains the username and password

C. Configure a Basic Authentication Site Authenticator to the Site

D. Configure a Mutual TLS Site Authenticator to the Site

ANSWER: C

Explanation:

Configure a Basic Authentication Site Authenticator to the Site is correct because the protected application requires the gateway itself to authenticate to the upstream server with a username and password. A Site Authenticator is the PingAccess component used for authentication on the connection from PingAccess to the target application, also called the site. The Basic Authentication Site Authenticator is designed to supply configured credentials using the HTTP Basic authentication mechanism, allowing PingAccess to establish an authenticated request to the application on behalf of the gateway.

This configuration separates the application's gateway-to-site authentication requirement from client authentication and authorization handled at the PingAccess web or application level. The administrator configures the Basic Authentication Site Authenticator with the credentials accepted by the application server, then associates that authenticator with the relevant Site definition. PingAccess can subsequently include the required Basic Authorization header when forwarding requests to that site. This is the appropriate pattern when the backend server expects a fixed service credential in a username:password form. Ping Identity documents Site Authenticators as the mechanism for configuring how PingAccess authenticates to a protected site; see the PingAccess Site Authenticators documentation and the Ping Identity documentation portal.

QUESTION NO: 2

An administrator is integrating a new PingAccess Proxied Application. The application will use an SSL certificate issued by a publicly trusted Certificate Authority. PingAccess is terminating SSL and is responsible for loading the SSL certificate for that application. What initial action must the administrator take in PingAccess in this situation?

A. Import the SSL public key with the full certificate chain into the Certificates.

B. Import the PKCS#12 file with the full certificate chain into the Certificates.

C. Import the SSL public key with the full certificate chain into the Key Pairs.

D. Import the PKCS#12 file with the full certificate chain into the Key Pairs.

ANSWER: D

Explanation:

Import the PKCS#12 file with the full certificate chain into the Key Pairs. Because PingAccess is the TLS termination point, it must present the application's server certificate to clients and prove possession of the corresponding private key during the TLS handshake. A PKCS#12 archive, typically using a `.p12` or `.pfx` extension, is designed to carry the server certificate, its private key, and, when included, the intermediate certificate chain. PingAccess stores this combination as a key pair, making the private key available for the HTTPS listener or site configuration that protects the proxied application.

The fact that the certificate was issued by a publicly trusted CA does not change this requirement. Public trust helps clients validate the certificate chain, while SSL termination requires PingAccess itself to access the private key associated with the public certificate. After the key pair is imported, the administrator can select and associate it with the appropriate PingAccess HTTPS configuration for the application. Ping Identity documents key pairs as the location for certificate-and-private-key material used by PingAccess. See the PingAccess key pairs documentation and the PingAccess product documentation.

QUESTION NO: 3

An administrator must protect a configuration by changing the default key. Which script can be used to meet this goal?

A. db-passwd-rotate.bat

B. memoryoptions.bat

C. run.bat

D. obfuscate.bat

E. generatekey.bat

ANSWER: E

Explanation:

`generatekey.bat` is the Windows script used to replace PingAccess's default configuration-encryption key with a newly generated key. PingAccess encrypts protected configuration data with its configuration encryption key, and an installation should not continue relying on the default key. Running the key-generation utility creates the replacement key material that PingAccess uses to protect its encrypted configuration values. The corresponding utility on Linux is `generatekey.sh`.

This operation should be planned carefully: the administrator must follow the documented procedure for the installed PingAccess version, preserve any required key material or backups, and restart the service as directed so that all nodes use the intended key. In clustered deployments, key consistency across the deployment is essential because every node that reads protected configuration must be able to decrypt it. The PingAccess documentation includes the administrative procedures and command-line utilities used for securing configuration and managing keys. See the PingAccess product documentation and the Ping Identity PingAccess support resources for version-specific key-management instructions.

QUESTION NO: 4

An administrator is integrating a new PingAccess Proxied Application. The application will temporarily need a self-signed certificate during the POC/demo phase. PingAccess is terminating SSL and is responsible for loading the SSL certificate for the application.

What initial action must the administrator take in PingAccess in this situation?

A. Go to the Certificates section and create a new certificate

B. Go to the Key Pairs section and import the PKCS#12 file provided by the customer's internal Certificate Authority

C. Go to the Key Pairs section and import the PKCS#12 file provided by the publicly trusted Certificate Authority

D. Go to the Key Pairs section and create a new certificate

ANSWER: D

Explanation:

Go to the Key Pairs section and create a new certificate is correct because SSL termination requires PingAccess to possess both the server certificate and its corresponding private key. PingAccess manages this material as a key pair, rather than as a standalone trusted certificate. For a proof-of-concept or demonstration deployment, creating a certificate in the Key Pairs area lets the administrator generate a self-signed certificate and private key directly in PingAccess. That generated key pair can then be selected when configuring the HTTPS listener or site that fronts the proxied application.

This is an appropriate initial setup for a temporary environment because the requirement is specifically for a self-signed certificate, not for a certificate issued by an organizational or public certificate authority. The administrator must subsequently ensure that clients which access the application trust the self-signed certificate, or accept its warning during controlled testing. Before production use, the self-signed certificate should normally be replaced with an appropriately issued certificate and private key, typically imported as a PKCS#12 key pair where required. Ping Identity documents key-pair management and TLS configuration in the PingAccess Key Pairs documentation and its SSL termination documentation.

QUESTION NO: 5

A financial application should be prompted for step-up authentication on a URL that allows money transfers. A previous administrator configured rules to be applied on the required application URL. Users are not prompted for step-up authentication when accessing the/sranafemmeneyURL endpoint.

Which two actions should the administrator take? (Choose 2 answers.)

A. Verify that a rejection handler rule exists and is applied to the application to see if a user has met the required authentication context

B. Verify that an authentication requirement rule is applied to the application to see if a user has met the required authentication context

C. Make sure that the existing rule's authentication requirements contain the appropriate minimum authentication requirements

D. Create a new identity mapping containing authentication context values and add the mapping to the existing rule

E. Make sure that the existing rule's token validation contains the appropriate minimum authentication requirements

ANSWER: B C

Explanation:

Step-up authentication for a protected PingAccess application resource is governed by an authentication requirement rule. Therefore, the administrator should first verify that an authentication requirement rule is actually associated with the application or applicable resource configuration that matches the money-transfer endpoint. The rule must be evaluated for the request URL before PingAccess can require an elevated authentication context from the user. Once it is correctly applied, PingAccess compares the user's current authentication context with the context required by the rule and can initiate the configured authentication flow when additional assurance is needed.

The administrator must also confirm that the existing rule specifies the appropriate minimum authentication requirements. For a money-transfer function, this requirement should represent the MFA or other elevated authentication context issued by the identity provider. A rule that is attached to the target but requires only the user's existing, lower-assurance context will not result in a step-up prompt. Correct rule association and an appropriately elevated minimum context together ensure that the sensitive endpoint requires stronger authentication. See the PingAccess documentation and Ping Identity product documentation.

QUESTION NO: 6

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:

`Subject = *.company.com` is valid because a wildcard DNS identity covering the `company.com` domain matches both `pa-admin.company.com` and `pa-admin2.company.com`. This allows one certificate key pair to be used by the administrative node and its replica for the PingAccess CONFIG QUERY listener. The wildcard represents exactly one host-name label, which is sufficient because both node names are direct subdomains of `company.com`.

`Subject Alternative Names = pa-admin.company.com, pa-admin2.company.com` is also valid because the certificate explicitly asserts both required DNS identities. A SAN extension is the standard X.509 mechanism for associating multiple DNS names with one certificate, so it directly meets the PingAccess requirement that the administrative-node key pair include the DNS names of both the administrative node and replica administrative node. Ping Identity's PingAccess documentation describes configuration and certificate requirements for clustered deployments at PingAccess documentation. The DNS-name matching behavior for certificate identities, including wildcard matching and DNS subject alternative names, is specified in RFC 6125.

QUESTION NO: 7

An application must be reachable through both `partners.company.com` and `suppliers.company.com`. PingAccess terminates TLS for both public hostnames, and the organization wants to use one certificate rather than separate certificates.

Which two actions should the administrator take? (Choose 2 answers.)

A. Create one Site for each public FQDN.

B. Create and associate Virtual Hosts for both public FQDNs.

C. Import the SAN certificate into a Trusted Certificate Group for the application.

D. Configure a Header Identity Mapping for each public FQDN.

E. Assign a Key Pair containing a SAN certificate for both names to the HTTPS Engine Listener.

ANSWER: B E

Explanation:

Create and associate Virtual Hosts for both public FQDNs. Virtual Hosts define the external hostname and port on which PingAccess receives requests for an application. Associating both hostnames with the application allows PingAccess to recognize and protect traffic sent to either address.

Assign a Key Pair containing a SAN certificate for both names to the HTTPS Engine Listener. The Engine Listener terminates TLS and must present a certificate valid for the hostname requested by the browser. A SAN certificate can explicitly include both `partners.company.com` and `suppliers.company.com`.

A Site controls the upstream target, not the client-facing hostname. A Trusted Certificate Group validates remote certificates and does not provide a server certificate for inbound client connections.

QUESTION NO: 8

An administrator needs to prevent PingAccess from automatically starting on a Windows Server. Which command would accomplish this task?

A. init.bat

B. uninstall-service.bat

C. remove-install.bat

D. wrapper-service.bat

ANSWER: B

Explanation:

`uninstall-service.bat` is correct because PingAccess runs as a Windows service when it has been installed with the supplied service scripts. A Windows service can be configured to start automatically as part of the operating system's service-management lifecycle. Running `uninstall-service.bat` removes the PingAccess service registration from Windows, so Windows no longer has a PingAccess service configured to launch automatically. This is the appropriate supplied command when the goal is to stop service-based automatic startup rather than merely stop a currently running PingAccess process. If the administrator later needs PingAccess to run as a Windows service again, the applicable installation script can be run to register the service anew, after which its Windows service startup configuration can be managed through standard Windows administration tools. Ping Identity's installation guidance describes the Windows service installation and removal scripts as part of administering a PingAccess deployment. See the PingAccess Installation Guide and the PingAccess documentation portal for product-version-specific installation and service-management instructions.

QUESTION NO: 9

PingAccess will terminate SSL for multiple proxied applications that share thecustomer.comURL domain. The administrator needs different ways to minimize the number of SSL certificates to manage these user-facing applications.

What are two ways this requirement can be met? (Choose 2 answers.)

A. Assign unique Key Pairs to each Virtual Host

B. Assign a wildcard certificate to the Engine Listener

C. Assign a Subject Alternative Name Certificate to the Engine Listener

D. Assign a Subject Alternative Name Certificate to the Agent Listener

E. Assign a wildcard certificate to the Agent Listener

ANSWER: B C

Explanation:

Assigning a wildcard certificate to the Engine Listener and assigning a Subject Alternative Name Certificate to the Engine Listener both reduce certificate-management overhead while allowing PingAccess to terminate TLS for multiple proxied applications. An Engine Listener is the PingAccess component that accepts incoming client HTTPS connections and therefore presents the server certificate for protected web applications. A wildcard certificate, such as one issued for `*.customer.com`, can secure multiple single-level hostnames including `app1.customer.com` and `app2.customer.com` with one certificate. A SAN certificate provides the alternative approach: it contains an explicit list of the required DNS names, enabling one certificate to cover several application hostnames. The appropriate choice depends on the hostname structure and the organization's certificate-issuance policy, but either certificate type can be associated with the Engine Listener to serve multiple virtual hosts. PingAccess listener and HTTPS configuration is documented in the PingAccess documentation. The certificate behavior underlying wildcard names and multiple DNS identities is defined in RFC 6125.