PassQueen
a.k.a dumpsqueen.com

Zscaler Digital Transformation Engineer

Zscaler ZDTE

Version Demo

Total Demo Questions: 7

Total Premium Questions: 79

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

Which of the following external IdPs is unsupported by OIDC with Zscaler ZIdentity?

A. PingOne

B. Auth0

C. Microsoft AD FS

D. OneLogin

ANSWER: C

Explanation:

Microsoft AD FS is the external identity provider in this list that is unsupported for an OIDC-based integration with Zscaler ZIdentity. ZIdentity supports federation with external identity providers using either SAML or OpenID Connect, but the protocol support is specific to the provider integration documented in the ZIdentity administration guidance. AD FS is configured with ZIdentity as a SAML identity provider: the integration relies on SAML metadata, signing certificates, and AD FS claim rules to issue SAML assertions to ZIdentity. Consequently, AD FS should be selected when the question asks which listed provider is not supported through OIDC.

This distinction matters during an identity design or migration. An organization using AD FS can still federate authentication to ZIdentity, but it must plan and configure the federation as SAML rather than attempting to register AD FS as an OpenID Provider for this ZIdentity use case. Zscaler's ZIdentity documentation covers external IdP configuration and available federation methods at Zscaler ZIdentity Help. Microsoft's AD FS documentation also describes its federation and protocol capabilities, including its SAML-oriented relying-party configuration model, at AD FS overview.

QUESTION NO: 2

An administrator has created a ZPA Application Segment for an internal finance application and an Access Policy that allows the Finance group to use it. The App Connectors are healthy, but they belong to a different App Connector Group that is not associated with the Application Segment. Users are authenticated successfully but cannot establish a connection to the application.

Which configuration change is required?

A. Associate the App Connector Group with the Access Policy

B. Create a new provisioning key for the existing App Connectors

C. Associate the App Connector Group with the Application Segment

D. Allow inbound internet access to the App Connectors

ANSWER: C

Explanation:

The administrator must associate the App Connector Group that contains the healthy App Connectors with the Application Segment. An Application Segment identifies the private application and defines the App Connector Groups that can broker connections to it. An Access Policy can authorize the user, but authorization alone does not provide a path to the application when no eligible App Connector Group is associated with the segment.

Associating the group with the Access Policy does not define application reachability, and creating a new provisioning key is unnecessary because the existing App Connectors are already healthy and enrolled. ZPA App Connectors establish outbound connections to the Zscaler cloud, so an inbound internet firewall rule is not required.

QUESTION NO: 3

How does Zscaler apply Tenant Restriction policies to cloud applications?

A. By allowing unrestricted access to all cloud applications

B. By blocking all external traffic

C. By inserting headers with the appropriate information during authentication

D. By disabling cloud applications completely

ANSWER: C

Explanation:

By inserting headers with the appropriate information during authentication is correct because Zscaler enforces supported SaaS tenant restrictions inline as traffic passes through the Zscaler cloud proxy. Rather than merely identifying an application, the policy controls which organization tenant a user may authenticate to. During a sign-in request, Zscaler can add the tenant-specific information required by the SaaS provider, such as an allowed tenant identifier or restriction-related request header. The provider then evaluates that information as part of its native authentication process and permits access to the organization's sanctioned tenant according to the configured policy.

This approach is designed to distinguish approved corporate use from personal or otherwise unsanctioned tenant use while preserving a normal sign-in experience for authorized users. It is particularly important for SaaS services in which the same application domain can host both enterprise and consumer accounts. Zscaler's Tenant Restrictions capability therefore combines user and policy context with application-aware HTTP(S) controls to direct authentication to the intended tenant and enforce the organization's SaaS-access requirements. See Zscaler's Tenant Restrictions documentation and its Secure Internet and SaaS Access overview.

QUESTION NO: 4

What are common use cases of Zscaler OneAPI automation?

A. Enrolling users' device information and installing antivirus features in Zscaler Client Connector (ZCC).

B. Creating App Connector Groups and enrolling users' device information.

C. Creating URL filtering rules and accessing ZDX Copilot.

D. Creating App Connector Groups and accessing ZDX Copilot.

ANSWER: B

Explanation:

Creating App Connector Groups and enrolling users' device information are common Zscaler OneAPI automation use cases. Zscaler OneAPI provides a unified, programmatic interface for performing administrative tasks across Zscaler services. This makes it well suited to infrastructure-as-code and operational workflows where configuration must be created consistently and repeatedly. For Zscaler Private Access, automation can create and manage App Connector Groups, allowing organizations to standardize how App Connectors are grouped and deployed as private-application access environments scale. OneAPI can also support device-related onboarding and lifecycle workflows by programmatically enrolling device information, reducing manual administrative work and helping organizations integrate Zscaler operations with endpoint-management, asset-management, or IT service-management processes. These API-driven workflows enable repeatable provisioning, reduce configuration drift, and make it easier to incorporate Zscaler configuration into CI/CD pipelines and other automated operational processes. Zscaler describes OneAPI as its unified API framework for accessing platform capabilities and automating management tasks. See the Zscaler OneAPI documentation and the Zscaler OneAPI overview for further details.

QUESTION NO: 5

A contractor needs temporary access to an internal web-based ticketing application. The contractor cannot install Zscaler Client Connector, and the organization does not want to provide VPN access or broad network connectivity.

Which ZPA capability is the best fit?

A. Zscaler Browser Access

B. App Connector

C. Z-Tunnel 2.0

D. A traditional remote-access VPN

ANSWER: A

Explanation:

Zscaler Browser Access is correct because it provides clientless access to supported private web applications through a browser. It is suited to third parties and unmanaged devices that need controlled access to a specific web application without installing Zscaler Client Connector or receiving network-level access.

App Connectors provide the service-side connectivity used by ZPA, but they do not provide an end-user access method. Z-Tunnel 2.0 is a Client Connector forwarding method and therefore requires the managed endpoint client. A traditional VPN would provide broader network connectivity than the stated least-privilege requirement.

QUESTION NO: 6

At which level of the Zscaler Architecture do the Zscaler APIs sit?

A. Enforcement Plane

B. Nanolog Cluster

C. Central Authority

D. Data Fabric

ANSWER: C

Explanation:

Central Authority is the correct answer because it is the control-plane layer of the Zscaler cloud architecture. This centralized layer maintains the tenant's configuration and policy state, distributes policy changes throughout the cloud, and provides the management functions used to administer Zscaler services. Zscaler APIs are intended for programmatic administration and automation: customers and integrations use them to read or update configurations, manage policy objects, and operationalize workflows. Those functions require access to centrally governed configuration and orchestration services, which is why they belong with Central Authority rather than the traffic-processing layers.

In practical terms, a change submitted through a Zscaler API follows the same centralized governance model as a change made in the administrative portal. Central Authority processes and coordinates that change so the relevant enforcement infrastructure can apply the resulting policy consistently. This separation is fundamental to Zscaler's cloud-native design: centralized control and policy management are distinct from globally distributed inspection and enforcement. Zscaler's API documentation describes APIs as interfaces for managing Zscaler service configuration, while Zscaler's architectural material identifies the centralized control function as the authority for policy and configuration. See Zscaler: About Zscaler APIs and Zscaler: What Is Security Service Edge?.

QUESTION NO: 7

An organization wants to upload internal PII (personally identifiable information) into the Zscaler cloud for blocking without fear of compromise. Which of the following technologies can be used to help with this?

A. Dictionaries

B. Engines

C. IDM

D. EDM

ANSWER: D

Explanation:

EDM is the appropriate technology because Exact Data Match is designed to detect and protect an organization's specific sensitive data, including PII records such as employee, customer, or patient information. The organization prepares a dictionary containing the relevant identifiers and uploads it for use in Zscaler Data Loss Prevention policies. EDM uses a privacy-preserving matching approach: sensitive values are transformed into fingerprints rather than being retained as readable source values for inspection. Zscaler can then compare content being transmitted through the service against those fingerprints and identify an exact match.

Once the EDM dictionary is associated with a DLP rule, the organization can apply enforcement actions such as blocking uploads or other outbound transmissions that contain the protected PII. This provides high-confidence protection for known internal records while reducing the exposure associated with providing raw sensitive data to a cloud security service. Exact matching is particularly useful when the business needs to identify actual records rather than merely data that resembles a generic pattern. Zscaler documents EDM as a DLP capability for matching sensitive data through uploaded dictionaries and configuring policy enforcement against detected matches. See Zscaler: About Exact Data Match and Zscaler: Adding an Exact Data Match Dictionary.