Vendor: Zscaler

Exam Code: ZDTE

Exam Name: Zscaler Digital Transformation Engineer

Version: DEMO

QUESTION 1
What is the primary benefit of using a subcloud in Zscaler?

A. To increase the number of available Public Service Edges
B. To eliminate the need for ZIA Public Service Edges
C. To guarantee that web traffic is forwarded to preferred ZIA Public Service Edges
D. To improve the accuracy of geolocation data

Answer: C
Explanation:
A subcloud in Zscaler is defined as a subset of ZIA Public Service Edges (data centers) that you group together and associate with specific locations or traffic. Conceptually, it is a logical "pool" of preferred Public Service Edges. When a user or site is mapped to a given subcloud, their traffic is steered only to that selected subset of Service Edges instead of any available data center in the wider cloud.

The main benefit of this design is control and predictability: you can guarantee that web traffic is forwarded to your preferred ZIA Public Service Edges, which is critical when you must keep egress IPs stable for SaaS allow-lists, regulatory requirements, or local data-residency mandates. Subclouds also help with operational resilience, because you can temporarily exclude problematic data centers from a subcloud without changing overall forwarding methods, ensuring continuity while still using your defined group of Service Edges. They do not increase the number of Service Edges, replace ZIA Public Service Edges, or directly affect IP geolocation precision. Therefore, option C correctly captures the primary benefit expected in the ZDTE/EDU-202 context.

QUESTION 2
What is the primary benefit of using a Custom Zscaler Connector for SaaS Application?

A. Minimum set of required credentials to access the SaaS Application Tenants
B. Temporary user credentials to access the SaaS Application Tenants
C. Broad access to all SaaS Application Tenants across Microsoft and Google
D. Full administrator credentials to access the SaaS Application Tenants

Answer: A
Explanation:
In Zscaler's SaaS Security and Data Protection services, a Custom Zscaler Connector (for example, for Google Workspace, Microsoft 365, or Salesforce) is designed so that Zscaler can connect to a specific SaaS tenant using only the minimum set of required credentials and scopes. The documentation for onboarding custom connectors explicitly emphasizes that, instead of providing full administrator rights, you authorize narrowly scoped API/OAuth permissions that allow Zscaler to scan data at rest and enforce security controls while adhering to least-privilege principles.

This minimal-credential approach reduces risk if the connector credentials are ever compromised, simplifies compliance audits, and aligns with modern security best practices. Zscaler needs just enough access to read, classify, and (where applicable) remediate or quarantine sensitive content in sanctioned SaaS applications, not broad tenant-wide admin access. Options suggesting temporary credentials, broad cross-tenant access, or full administrator rights contradict this design philosophy and the way the connectors are documented. Therefore, the primary benefit--and the key phrase you should associate with Custom Zscaler Connectors for the exam--is that they enable Zscaler to operate using a minimum set of required credentials for each SaaS Application tenant.

QUESTION 3
The Zscaler for Users - Engineer (EDU-202) learning path consists of various solutions covered in eleven courses. Which of the following topics is out of scope for the Zscaler for Users - Engineer learning path?

A. In-depth overview of Zscaler's architecture platform, including its global scale, additional capabilities, and API infrastructure.
B. Enabling versions to control which version (if any) of Zscaler Client Connector is available when end users manually update the app or when you configure automatic app updates.
C. Configuration of ZDX for applications, call quality monitoring, probes, diagnostics, alerts, and role-based administration to ensure effective SaaS and web application monitoring.
D. Exploring Intrusion Prevention System, DNS Control, Tenant Restrictions, and secure application segmentation.

Answer: B
Explanation:
Official EDU-202 materials describe the Engineer path as focusing on advanced architecture, connectivity, platform, access control, cyberthreat protection, data protection, risk management, ZDX, and Zero Trust Automation. The published learning outcomes explicitly include: discussing the architecture of the Zscaler platform and its API infrastructure; configuring advanced connectivity options; and configuring advanced cybersecurity services and Zscaler Digital Experience (ZDX)--including application monitoring, call quality, probes, diagnostics, alerts, and role-based administration. These map directly to options A, C, and D, which align to Zscaler Architecture, Cyberthreat/Access Control Services (IPS, DNS Control, Tenant Restrictions, segmentation), and ZDX content in the EDU-202 outline.

By contrast, Client Connector App Store "version enablement" and controlling which build is available when users manually or automatically update the app is documented as an administration task in the Client Connector help and is typically taught in the Essentials/Administrator (EDU-200) path, not in the Engineer path. Those materials show how to use the App Store to enable builds and control available versions, positioning it as operational client management rather than an advanced Engineer-level topic. Consequently, option B is considered out of scope for EDU-202 in the ZDTE context.

QUESTION 4
An engineer attempted to push a configuration using an API call to an endpoint but received a 409 response code. What was the reason for the error response code?

A. Exceeded the rate limit or quota
B. Resource does not exist
C. Edit conflict occurred
D. Request is not complete due to incorrect syntax

Answer: C
Explanation:
In the context of Zscaler's public APIs, HTTP status code 409 indicates a conflict with the current state of the target resource, most commonly an edit conflict. When configuration is managed via API, Zscaler uses versioning or similar concurrency controls to ensure that two administrators or systems do not overwrite each other's changes unintentionally. A 409 response typically appears when the payload being pushed is based on an outdated version of the object or when another change has been committed between the time the configuration was retrieved and the time the update was sent.

The Digital Transformation Engineer documentation explains that clients should first retrieve the latest configuration (often including a version or ETag-like value), apply their modifications, and then push the update. If the server detects that the version in the request no longer matches the current version, it returns 409 Conflict to signal that the update cannot be safely applied.

The other options map to different HTTP codes: rate limit or quota issues are indicated by 429 Too Many Requests, non-existent resources by 404 Not Found, and syntax or malformed payloads by 400 Bad Request. Thus, for a 409 response during a configuration push, the correct interpretation is an edit conflict.

QUESTION 5
Which tunnel mode supports both web and non-web applications, ensuring comprehensive security for modern enterprises?

A. IPSec Tunnel
B. Z-Tunnel 1.0
C. GRE Tunnel
D. Z-Tunnel 2.0

Answer: D
Explanation:
Zscaler Client Connector supports multiple tunnel modes to send user traffic to the Zscaler security cloud. In the Digital Transformation Engineer material, Z-Tunnel 2.0 is described as the recommended and most capable mode because it supports both web and non-web applications across all ports and protocols. This enables comprehensive inspection and Zero Trust policy enforcement for SaaS, web, and private applications from a single, unified tunnel.

Z-Tunnel 1.0 was primarily designed for web traffic, with limitations around non-web protocols and certain advanced use cases. As enterprises adopt more modern and diverse application stacks (VoIP, collaboration tools, custom TCP/UDP apps), Z-Tunnel 1.0 often cannot provide full coverage. GRE and IPSec tunnels (options A and C) are typically used for site-to-cloud connectivity from branch or data center routers, not as endpoint-based tunnels from user devices.

Z-Tunnel 2.0 uses an advanced encapsulation mechanism that can simultaneously support ZIA and ZPA, apply granular user- and device-based policies, and provide rich telemetry for analytics. It is explicitly positioned in Zscaler's training as the tunnel mode that delivers end-to-end protection for both web and non-web traffic, making it the correct answer for enterprises needing broad, modern coverage.

QUESTION 6
A security analyst is configuring Zscaler Data Loss Prevention (DLP) policies and wants to ensure that sensitive files are accurately identified and inspected. They ask about the methods Zscaler DLP uses to inspect files and detect potential data leaks. What are the three levels of inspection that Zscaler DLP employs to accurately identify and inspect files?

A. File header, file extension, and file signature
B. Magic Bytes, MIME type, and file extension
C. File header, file extension, and encryption status
D. Magic Bytes, MIME type, encryption status

Answer: B
Explanation:
The Data Protection section of the Zscaler Digital Transformation study guide explains that,

before applying DLP dictionaries, IDM/EDM, or OCR, Zscaler must reliably determine the actual file type being inspected. To prevent simple evasion techniques (for example, renaming an executable to .pdf), Zscaler performs a three-layer file-type inspection.

The documentation states that Zscaler first examines the file's "magic bytes" (the signature in the file header), then validates the MIME type reported by the content, and finally compares these to the file extension seen in the transaction. This layered approach ensures that if a user tampers with the extension or the declared MIME type, the underlying binary signature will still reveal the true file type, allowing the correct DLP engine and policy to be applied.

Other attributes like encryption status are indeed considered elsewhere in the DLP workflow (for example, to understand if a file can be decrypted or inspected), but the study guide is explicit that the three levels of file-type inspection are Magic Bytes, MIME type, and file extension, matching option B.

QUESTION 7
What is a digital entity that would be identified by Zscaler External Attack Surface Management?

A. A service hostname that contains revealing information.
B. Certificates installed on clients to enable SSL inspection.
C. The IP address of a properly deployed Zscaler App Connector.
D. Lists of known compromised usernames and passwords.

Answer: A
Explanation:
Zscaler External Attack Surface Management (EASM) is focused on discovering and monitoring an organization's internet-facing digital assets. In the Engineer curriculum, EASM is described as continuously identifying domains, subdomains, hostnames, IP addresses, TLS certificates, and cloud services that are exposed to the public internet. A key example used in the training is hostnames that "leak" internal context, such as environment names, projects, technologies, or business units. These hostnames are treated as digital entities because they represent externally reachable services and can give valuable clues to an attacker during reconnaissance.

By contrast, SSL inspection certificates installed on endpoints are internal controls and not part of the external attack surface. A Zscaler App Connector is designed to initiate only outbound connections and is intentionally not directly reachable from the internet, so its IP address is not an EASM discovery target. Likewise, lists of compromised usernames and passwords relate to threat intelligence and identity protection, not the mapping of exposed assets. Therefore, the only option that correctly matches the type of digital entity EASM is meant to identify is a service hostname that contains revealing information.

QUESTION 8
How many key engines does the Zscaler Firewall Module have?

A. Three
B. Two
C. Five
D. Four

Answer: D
Explanation:
In the Zscaler for Users ?Engineer path, the Zscaler Cloud Firewall (Firewall Module in ZIA) is described as being built around four key engines. The training emphasizes that the firewall is not

a single, monolithic filter but a set of parallel inspection engines that collectively provide advanced Layer 3/4 control, application and service awareness, DNS security, and inline threat prevention. These engines evaluate traffic simultaneously, and the most restrictive outcome is applied, aligning with Zscaler's broader "parallel processing" model for policy enforcement.

The curriculum highlights that this multi-engine design allows Zscaler to go beyond traditional firewalls, combining user and application awareness with security controls such as IPS and DNS-based protection within the same cloud-native enforcement stack. Having four coordinated engines enables granular, identity-based firewall policies that work for users regardless of location, without the need for separate appliances. Options suggesting two, three, or five engines do not match the way the Firewall Module is presented in the ZDTE/EDU-202 materials. Therefore, the correct answer, and the number you are expected to know for the exam, is four.

QUESTION 9
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:
Zscaler's core architecture in the Engineer course is explained using three main layers: Central Authority, Enforcement Nodes, and Logging / Nanolog services, supported by a distributed data fabric. The Central Authority is explicitly described as the "brains" or control plane of the Zscaler platform. It is responsible for global policy management, configuration, orchestration, and the API gateway that exposes Zscaler's administrative and automation APIs.

Enforcement nodes (such as ZIA Public Service Edges and ZPA enforcement components) form the data plane, inspecting traffic and applying policy decisions but not hosting the management APIs themselves. Nanolog clusters handle large-scale log storage and streaming, providing logging and analytics rather than control or configuration interfaces. The data fabric underpins global state and synchronization across the cloud but is not where customers interact with APIs.

In the Digital Transformation Engineer material, when you see references to OneAPI and other programmatic integrations, they are always associated with the Central Authority layer, reinforcing that APIs live in the control plane. Therefore, within the defined Zscaler Architecture levels, the APIs sit at the Central Authority.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**