Zscaler.ZDTE.v2026-03-30.q20

Exam Code:	ZDTE
Exam Name:	Zscaler Digital Transformation Engineer
Certification Provider:	Zscaler
Free Question Number:	20
Version:	v2026-03-30
# of views:	114
# of Questions views:	200
https://www.exam-tests.com/ZDTE-exam/Zscaler.ZDTE.v2026-03-30.q20.html	

NEW QUESTION: 1
An organization needs to comply with regulatory requirements that mandate web traffic inspected by ZIA to be processed within a specific geographic region. How can Zscaler help achieve this compliance?
A. By allowing traffic to bypass ZIA Public Service Edges and connect directly to the destination
B. By creating a subcloud that includes only ZIA Public Service Edges within the required region
C. By deploying local VPNs to ensure regional traffic compliance
D. By dynamically allocating traffic to the closest Public Service Edge, regardless of the region
Answer: (SHOW ANSWER)
Zscaler Internet Access (ZIA) supports regional processing requirements through the concept of subclouds. A subcloud is defined as a subset of ZIA Public Service Edges (and optionally Private Service Edges) that operate as full-featured secure internet gateways inspecting all web traffic. ZIA administrators can create a custom pool of data centers (Public Service Edges) that are constrained to a specific geography and then associate locations or tunnels with that subcloud. This ensures that user traffic forwarded to ZIA is only terminated and inspected within that defined regional pool, helping satisfy data-residency and regulatory mandates By contrast, Zscaler's default behavior is to use geo-IP and DNS to send traffic to the nearest available Public Service Edge globally, which may violate regional-processing rules (making option D unsuitable in a compliance-driven scenario) Bypassing ZIA (option A) or deploying local VPNs (option C) would undermine the Zero Trust model and remove ZIA's inline security controls. Therefore, configuring a subcloud that includes only Public Service Edges in the mandated region is the architecturally correct and exam-aligned method to keep inspection within a specific geography.

NEW QUESTION: 2
An IT administrator is reviewing the recently configured ZDX module in their environment and checks the performance data on the dashboard. The administrator notices that no software inventory has populated. What could be a probable reason?
A. ZDX client is not configured to collect inventory data
B. ZDX license doesn't have inventory collection entitlement
C. Zscaler Client Connector needs to be whitelisted on the EDR tool
D. ZDX client version being used is 4.3
Answer: A (LEAVE A REPLY)
Zscaler Digital Experience (ZDX) relies on Zscaler Client Connector to collect device and application telemetry from endpoints. Performance metrics (such as device, network, and application scores) are enabled as part of the core ZDX deployment, which explains why the administrator can already see performance data on the dashboard. However, software inventory is an additional inventory feature that must be explicitly enabled in the ZDX administration settings.
ZDX documentation describes an "Inventory Settings" page where administrators must turn on a setting such as "Collect Software Inventory Data." When this option is enabled and the minimum supported versions of Client Connector and the ZDX module are present, Client Connector begins collecting installed software details and sending this inventory to the ZDX cloud for visualization.
If the collection toggle is left disabled, ZDX will continue to show performance metrics but no entries appear under Software Inventory or related views, even though licensing and versions are otherwise correct. The other options listed either relate to licensing, generic EDR conflicts, or a specific client version and do not match the documented dependency on enabling software-inventory collection. Therefore, the most accurate reason is that the ZDX client (via policy) is not configured to collect inventory data.

NEW QUESTION: 3
Which user interface aims to simplify Zero Trust adoption and operations by providing an intuitive interface for all administrative users?
A. OneAPI
B. Zscaler Experience Center
C. ZIA
D. ZIdentity
Answer: (SHOW ANSWER)
Zscaler Experience Center is the unified, next-generation administration console designed to simplify Zero Trust adoption across the entire Zscaler platform. Zscaler describes Experience Center as a single, centralized command console that brings together management for Zscaler Internet Access (ZIA), Zscaler Private Access (ZPA), Zscaler Digital Experience (ZDX), Risk360, and other services in one place.

The official guidance states that Experience Center "aims to simplify Zero Trust adoption and operations by providing an intuitive interface for all administrative users." It introduces persona-driven workflows, consistent navigation, and a common policy framework across internet, SaaS, and private applications. This allows security, networking, and operations teams to configure access control, threat protection, data protection, and digital experience policies through a single, coherent UI instead of juggling separate consoles.
By contrast, OneAPI is a programmatic automation interface, not a graphical admin UI. ZIA is a core product whose original admin portal handles secure internet and SaaS access, but it is just one component of the broader platform. ZIdentity provides centralized identity and admin-role management, not the full Zero Trust operations UI across all services.
Therefore, the correct answer that matches the stated goal and wording is Zscaler Experience Center.

NEW QUESTION: 4
What capabilities within Zscaler External Attack Surface Management (EASM) are specifically designed to uncover and assess domains that are intentionally created to resemble your legitimate brand or websites?
A. Fake Domains
B. Mimic Domains
C. Spoofing Domains
D. Lookalike Domains
Answer: (SHOW ANSWER)
Zscaler External Attack Surface Management (EASM) includes a dedicated capability called Lookalike Domains. Zscaler defines lookalike domains as fraudulent or fake domains intentionally created by threat actors to mimic your legitimate domains and brand presence, often for phishing, credential theft, or brand abuse.
Within the EASM portal, the Lookalike Domains pages and widgets present a curated list of suspicious domains that closely resemble your seed or official domains. Analysts can review exposure scores, registrar details, hosting information, and other attributes to determine which of these domains pose the highest risk and warrant takedown or additional monitoring.
This feature is specifically designed for external risk and brand-protection use cases: it highlights where attackers are impersonating your organization on the public internet, which is a core component of digital-risk and external-attack-surface management. While words such as "fake," "mimic," or "spoofing" may be used generically in security discussions, "Lookalike Domains" is the exact term and feature name Zscaler uses in the EASM product and documentation. Options A, B, and C do not correspond to a named EASM capability and therefore are not correct in the ZDTE context.

NEW QUESTION: 5

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 (LEAVE A REPLY)

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.

NEW QUESTION: 6

What are the building blocks of App Protection?

A. Controls, Profiles, Policies

B. Policies, Controls, Profiles

C. Traffic Inspection, Vulnerability Identification, Action Based on User Behavior

D. Profiles, Controls, Policies

Answer: D (LEAVE A REPLY)

In Zscaler App Protection, the core design model is built around three fundamental building blocks presented in a specific logical order: Profiles, Controls, and Policies. The Digital Transformation Engineer material explains that App Protection's goal is to apply fine-grained security actions to applications and user sessions based on risk and context. First, Profiles define who is being governed. They group users or devices that share common characteristics (such as department, location, or risk level). Next, Controls define what actions are allowed, restricted, or inspected. Examples include limiting copy-and-paste, file uploads and downloads, printing, clipboard usage, or enforcing additional inspection for sensitive content and risky behaviors. Finally, Policies define when and where those controls are applied by mapping profiles to specific applications or traffic

categories under defined conditions (such as user risk posture, device posture, or access method).
Options A and B contain the same elements but in the wrong conceptual order compared to how App Protection is taught and implemented. Option C describes generic security concepts, not the explicit App Protection building-block terminology. Therefore, the correct sequence and terminology, matching the App Protection framework, is Profiles, Controls, Policies.

NEW QUESTION: 7
Which Zscaler technology can be used to enhance your cloud data security by providing comprehensive visibility and management of data at rest within public clouds?
A. Data Security Posture Management (DSPM)
B. Cloud Sandbox
C. Cloud Access Security Broker (CASB)
D. SaaS Security Posture Management (SSPM)
Answer: A (LEAVE A REPLY)
Zscaler Data Security Posture Management (DSPM) is specifically designed to discover, classify, and protect data at rest across public cloud environments such as object stores, databases, and other cloud-native services. Zscaler's DSPM solution continuously scans cloud data stores to identify where sensitive data resides, who can access it, how it is shared, and whether it violates corporate or regulatory policies, so security teams gain full visibility into their cloud data landscape and can remediate risks at scale.
In the broader Zscaler Data Protection portfolio, DSPM is highlighted as the capability that extends protection beyond inline traffic to data at rest in SaaS and public clouds, complementing DLP and malware controls that secure data in motion. Cloud Sandbox (option B) focuses on detonating suspicious files to detect zero-day malware; CASB (option C) secures SaaS usage and API-based access; and SSPM (option D) concentrates on assessing and fixing misconfigurations in SaaS applications. None of these options are as tightly aligned to continuous discovery and posture management of public-cloud data at rest as DSPM.
Therefore, the Zscaler technology that enhances cloud data security by providing comprehensive visibility and management of data at rest in public clouds is Data Security Posture Management (DSPM).

NEW QUESTION: 8
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 (LEAVE A REPLY)
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.

NEW QUESTION: 9
How does log streaming work in ZIA?
A. NSS (Nanolog Streaming Service) opens a secure tunnel to the cloud. User access goes through the ZEN (Zscaler Enforcement Node). ZEN sends the logs to the cloud Nanolog for storage. Cloud Nanolog streams a copy of the log to NSS. NSS sends the log to the SIEM over the network.
B. NSS opens a secure tunnel to the cloud. Cloud Nanolog streams a copy of the log to NSS. User access goes through the ZEN. ZEN sends the logs to the cloud Nanolog for storage. NSS sends the log to the SIEM over the network.
C. User access goes through the ZEN (Zscaler Enforcement Node). NSS (Nanolog Streaming Service) opens a secure tunnel to the cloud. ZEN sends the logs to the cloud Nanolog for storage. Cloud Nanolog streams a copy of the log to NSS. NSS sends the log to the SIEM over the network.
D. NSS opens a secure tunnel to the cloud. ZEN sends the logs to the cloud Nanolog for storage. User access goes through the ZEN. Cloud Nanolog streams a copy of the log to NSS. NSS sends the log to the SIEM over the network.
Answer: (SHOW ANSWER)
In ZIA, user traffic is first forwarded to a Zscaler Enforcement Node (ZEN), where security and access policies are enforced and transaction logs are generated. Those logs are then sent from the ZEN to the cloud- based Nanolog cluster, which is the highly scalable logging

and storage layer used by Zscaler. Nanolog compresses and stores the logs for reporting, analytics, and long-term retention.
To deliver logs to a customer's SIEM, the Nanolog Streaming Service (NSS) is deployed in the customer environment. NSS establishes a secure, outbound tunnel to the Nanolog service in the Zscaler cloud and subscribes to that customer's log stream. Nanolog then continuously streams a copy of relevant logs over this secure connection to NSS. NSS receives the logs, converts them into the required output format (for example, syslog or CEF), and forwards them on to the configured SIEM or log receiver.
Option C is the only answer that correctly represents the logical sequence: user traffic through ZEN, ZEN to Nanolog, secure tunnel from NSS, Nanolog streaming to NSS, and finally NSS forwarding to the SIEM.

NEW QUESTION: 10
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 (LEAVE A REPLY)
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.
Top of Form

NEW QUESTION: 11
What is the primary function of ZIA Public Service Edges in the Cloud Firewall architecture?
A. Managing endpoint security updates
B. Providing cloud storage services
C. Load balancing internet traffic
D. Acting as key policy enforcement engines
Answer: D (LEAVE A REPLY)
Within the ZIA Cloud Firewall and broader Zscaler Internet Access architecture, Public Service Edges (PSEs) are the core policy enforcement points. User traffic is steered (via tunnels, PAC files, or agents) to the nearest PSE, where Zscaler performs security inspection and policy evaluation. At this point, the Cloud Firewall, URL filtering, SSL inspection, IPS, sandboxing, and other security engines are applied according to the user's identity, group, location, and defined policies.
Although the PSEs naturally participate in traffic distribution across the global Zscaler cloud, their primary purpose is not generic load balancing or network transit; rather, they host the full security stack and make real- time allow/deny/log decisions. They also enforce bandwidth controls, application rules, and advanced threat protections before forwarding allowed traffic to the internet.
They are not responsible for managing endpoint security updates or providing general cloud storage. Instead, they serve as inline security gateways that enforce Zero Trust access and granular firewall rules at scale.
Therefore, the correct description of their role in the Cloud Firewall architecture is that they act as key policy enforcement engines.

NEW QUESTION: 12
What is one key benefit of deploying a Private Service Edge (PSE) in a customer's data center or office locations?
A. It allows users to access private applications without encryption overhead for increased performance.
B. It replaces the need for a Zscaler App Connector in the environment and simplifies the network.
C. It eliminates the need to use Zero Trust Network Access (ZTNA) policies for internal applications.
D. It provides Zero Trust Network Access policies locally, improving user experience and reducing latency.

Answer: D (LEAVE A REPLY)
The ZDTE study content groups Private Service Edge under Advanced Platform Services, explaining that PSEs host the same Zero Trust Exchange policy and inspection engines, but run as customer-managed service edges inside data centers or large offices. They are designed to give on-premises users a "local on-ramp" to ZIA and ZPA services while still enforcing full zero-trust policy.
The documentation emphasizes that PSEs do not replace App Connectors for ZPA; connectors are still required to establish inside-out application connectivity. Nor do PSEs remove the need for ZTNA policies- those policies remain central and are simply enforced closer to the user. Encryption is also preserved end-to- end; there is no "unencrypted fast path" described in the reference architecture.
Instead, the primary benefit highlighted is performance and user experience: by enforcing ZIA/ZPA policies at a local PSE rather than a distant public service edge, organizations reduce round-trip latency and keep traffic on optimal paths while maintaining identical security and access controls.

NEW QUESTION: 13
A customer requires 2 Gbps of throughput through the GRE tunnels to Zscaler. Which is the ideal architecture?
A. Two primary and two backup GRE tunnels from internal routers with NAT enabled
B. Two primary and two backup GRE tunnels from border routers with NAT disabled
C. Two primary and two backup GRE tunnels from internal routers with NAT disabled
D. Two primary and two backup GRE tunnels from border routers with NAT enabled
Answer: (SHOW ANSWER)
Zscaler design guidance for GRE connectivity emphasizes three key principles: terminate GRE on border (edge) devices, avoid NAT on GRE source addresses, and scale bandwidth by using multiple tunnels. In Zscaler documentation and engineering training, each GRE tunnel is typically sized for up to about 1 Gbps of throughput. For a 2 Gbps requirement, customers are advised to deploy at least two primary GRE tunnels, with two additional backup tunnels for redundancy and failover.
These tunnels should terminate on border routers that own public IP addresses, ensuring optimal routing and simplifying troubleshooting. Zscaler specifically recommends that the public source IPs used for GRE must not be translated by NAT, because the Zscaler cloud must see the original, registered public IP to associate tunnels with the correct organization and enforce policy. Enabling NAT on GRE traffic can break tunnel establishment and lead to asymmetric or unpredictable routing.
Using internal routers introduces extra hops and complexity and often requires NAT or policy-based routing, which goes against recommended best practices. Similarly, any architecture with NAT enabled on GRE traffic conflicts with Zscaler's published requirements. Therefore, the ideal and recommended design for 2 Gbps via GRE is two primary and two backup GRE tunnels from border routers with NAT disabled.

NEW QUESTION: 14
In a typical authentication configuration, Zscaler fulfills which of the following roles?
A. SaaS gateway
B. Identity provider
C. Identity proxy
D. Service provider
Answer: (SHOW ANSWER)
In a typical enterprise authentication setup, Zscaler functions as the Service Provider (SP) within the SAML authentication framework. This aligns with Zscaler's architectural principle that identity verification is delegated to an external authoritative Identity Provider (IdP) such as Azure AD, Okta, Ping, or ADFS. Zscaler does not authenticate user credentials directly. Instead, it relies on the IdP to validate the user and then deliver a signed SAML assertion back to Zscaler.
When a user attempts to access the Zscaler service, the authentication request is redirected to the enterprise IdP. The IdP performs credential verification and returns a SAML assertion containing the authenticated user identity and associated attributes. Zscaler, acting as the SP, consumes and validates this assertion, then maps the identity to its internal user records or SCIM-synchronized directory objects. This identity becomes the basis for all ZIA/ZPA policy evaluation, including URL filtering, CASB controls, DLP policies, firewall rules, and access-control enforcement.
Since Zscaler depends on the IdP for primary identity verification and only consumes assertions, Zscaler's role is clearly defined as the Service Provider in a standard authentication configuration.

NEW QUESTION: 15
Which authorization framework is used by OneAPI to provide secure access to Zscaler Internet Access (ZIA), Zscaler Private Access (ZPA), and Zscaler Client Connector APIs?
A. JSON Web Tokens
B. OAuth 2.0
C. SAML
D. API Keys
Answer: (SHOW ANSWER)
Zscaler OneAPI provides a unified, programmatic interface to automate configuration and operations across the Zscaler platform, including ZIA, ZPA, and Zscaler Client Connector. Zscaler's OneAPI documentation clearly states that OneAPI uses the OAuth 2.0 authorization framework to secure access to these APIs.
In practice, administrators or automation platforms register an API client in ZIdentity, obtain OAuth 2.0 access tokens, and then use those tokens to call OneAPI endpoints. The use of OAuth 2.0 ensures standardized flows for client authentication, token issuance, and scope-based authorization, aligning with modern security best practices and making it easier to

control and audit API access. Zscaler also highlights OAuth 2.0 as one of the three architectural pillars of OneAPI, along with a common endpoint and tight integration with ZIdentity.
While JSON Web Tokens (JWTs) can be used as a token format inside OAuth 2.0, they are not, by themselves, the authorization framework. SAML is typically used for browser-based SSO, not for securing REST APIs in this context. API Keys are simpler credential schemes and are not what Zscaler prescribes for OneAPI. As a result, OAuth 2.0 is the correct and exam-relevant answer.

NEW QUESTION: 16
A contractor is visiting an organization for a maintenance task. The administrator does not have a spare laptop to give them. How will the administrator provide secure access for the contractor?
A. SD-WAN
B. Branch Connector
C. Cloud Connector
D. Privileged Remote Access
Answer: D (LEAVE A REPLY)
Zscaler's Digital Transformation material is very clear that third-party admins, vendors, and contractors needing temporary, high-privilege access from unmanaged devices are a primary use case for Privileged Remote Access (PRA). PRA is built on ZPA and delivers a clientless remote desktop gateway: contractors simply use an HTML5-capable browser to reach RDP, SSH, or similar consoles without installing an agent or being placed on the internal network.
The study content explains that PRA enforces least-privilege access on a per-application or per-system basis, with capabilities such as time-bound access windows, credential vaulting/mapping (so credentials are never exposed), and full session recording and monitoring for audit and compliance. This directly matches the scenario of a short-term maintenance task from a contractor's own laptop.
By contrast, SD-WAN, Branch Connector, and Cloud Connector are connectivity constructs for sites and workloads, not for granting interactive, privileged access to individual admins on unmanaged endpoints. They don't solve the governance, session control, and just-in-time access requirements highlighted in the ZDTE content for third-party access. Therefore, Zscaler positions Privileged Remote Access as the correct and recommended approach here.

Valid ZDTE Dumps shared by BraindumpsPass.com for Helping Passing ZDTE Exam! BraindumpsPass.com now offer the **newest ZDTE exam dumps**, the BraindumpsPass.com ZDTE exam **questions have been updated** and **answers have**

been corrected get the **newest** BraindumpsPass.com ZDTE dumps with Test Engine here: https://www.braindumpspass.com/Zscaler/ZDTE-practice-exam-dumps.html (**62** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 17
In the Zscaler Client Connector (ZCC) Admin Portal, which posture element is supported on Windows but not on macOS?
A. Client Certificate
B. Full Disk Encryption
C. Domain Joined
D. CrowdStrike ZTA Sensor Setting Score
Answer: D (LEAVE A REPLY)
Zscaler's Device Posture framework in Client Connector supports a broad set of posture checks on both Windows and macOS, such as Certificate Trust, Client Certificate, Firewall status, Full Disk Encryption, Domain Joined, and multiple EDR detections. These are listed in Zscaler technical training material as common capabilities for "Windows und macOS." However, Zscaler's advanced integration with CrowdStrike introduces additional posture signals based on Zero Trust Assessment (ZTA). In the same material, CrowdStrike ZTA Score is explicitly annotated with a Windows-specific minimum version ("CrowdStrike ZTA Score (Win v.3.4.0+)"), highlighting that this ZTA- based posture is implemented for Windows only in the current releases, while the shared list for macOS does not include its own ZTA-specific version.
The newer ZTE/EDU-202 engineer materials build on this by describing separate ZTA Device OS and Sensor scores, and the exam maps this Windows-only ZTA enforcement to the CrowdStrike ZTA Sensor Setting Score option. In contrast, Client Certificate, Full Disk Encryption, and Domain Joined are documented as cross-platform posture types, not restricted to Windows.

NEW QUESTION: 18
The ZDX Dashboard is a comprehensive tool designed to provide a performance overview of an organization's digital experience. It encompasses various aspects to monitor and analyze performance, ensuring a smooth digital experience across the organization.
Which of the following is responsible for the automated root cause analysis within ZDX?
A. OAuth request
B. Application Performance
C. Y-Engine
D. Copilot
Answer: C (LEAVE A REPLY)
In the Zscaler Digital Experience (ZDX) section of the Digital Transformation Engineer material, Y-Engine is explicitly defined as ZDX's Automated Root Cause Analysis component. The EDU-200 and study-guide content describe Y-Engine as using machine

learning to automatically isolate root causes of performance issues, correlating metrics across applications, networks, and devices so that IT teams spend less time troubleshooting and can get users back to work faster.
Several ZDX overviews and integration documents reiterate that Y-Engine is ZDX's AI/ML-based approach to detect what is causing the ZDX score for a given application or user segment to drop, effectively automating the "why is it slow?" analysis that would otherwise require multiple domain-specific tools.
"Copilot" in the Zscaler context refers to generative-AI assistance that can surface insights and answer questions, but it is built on top of underlying telemetry and correlation engines like Y-Engine; it is not the core Auto-RCA engine itself. "Application Performance" is a metric category within ZDX, and "OAuth request" is simply an authentication mechanism, not a diagnostic engine. Accordingly, the training content makes it clear that Y-Engine is responsible for automated root cause analysis, so option C is correct.

NEW QUESTION: 19
What is one benefit of OneAPI?
A. Multiple registration processes
B. Repeated authorization messages required for increasing security
C. Simplifies API integration by using a single entry point
D. Multiple token requests
Answer: C (LEAVE A REPLY)
Zscaler OneAPI is described in the Digital Transformation Engineer and Zero Trust Automation content as a unified API gateway for the entire Zscaler platform. Official OneAPI overview material explains that it provides "a common API endpoint" and "a single programming interface for the entire Zscaler platform," so automation engineers no longer need to manage different endpoints, authentication patterns, or schemas for each product. The Zero Trust Automation at-a-glance guide further emphasizes that OneAPI "uses a single API to enable automation as an administrator," which accelerates deployment and reduces human error. Study resources summarizing OneAPI reinforce that it "simplifies integration by providing a single-entry point for accessing multiple APIs," reducing complexity and making it easier to build consistent automation across ZIA, ZPA, ZDX, and ZCC.
The other options contradict this design. OneAPI is specifically intended to avoid multiple registration processes and repeated token or authorization workflows; OAuth 2.0 is centralized via ZIdentity so that API clients authenticate once and then use scoped access across services. Therefore, the clearly documented benefit that matches the Zscaler Digital Transformation Engineer description is that OneAPI simplifies API integration by using a single entry point, making C the correct answer.

NEW QUESTION: 20

Safemarch is a retail company with hundreds of stores across the United States. Their core applications reside in two different data centers with a considerable presence on AWS.
Which would be a good connectivity solution for them to access applications from store locations?
A. Branch Connector at stores for Zscaler connectivity and Direct Connect from data centers to AWS.
B. SD-WAN connectivity to stores and Zscaler Edge, with App Connectors on-prem and on AWS.
C. Site-to-site VPNs from stores to Zscaler Edge, with App Connectors on-prem and on AWS.
D. Branch Connectors at stores with App Connectors on-prem and on AWS.
Answer: (SHOW ANSWER)
For a large retail organization with hundreds of geographically distributed stores and applications split across multiple data centers plus AWS, Zscaler reference designs emphasize an SD-WAN-to-Zscaler Edge model combined with ZPA App Connectors deployed close to the applications. In this model, each store uses SD- WAN to build resilient, policy-based connectivity to the nearest Zscaler Edge locations. Those edges then provide secure, optimized access to private applications published through App Connectors installed in the on- premises data centers and within AWS VPCs.
This approach centralizes security and access control in the Zscaler cloud while avoiding the operational burden of managing hundreds of direct site-to-site VPNs. It also aligns with Zero Trust principles by steering all store traffic to Zscaler rather than extending the corporate network to every store. Direct Connect between data centers and AWS (as in option A) is optional from a ZPA perspective because App Connectors in AWS communicate outbound to Zscaler over the internet. Branch Connector (option D) is typically used when SD- WAN or suitable edge devices are not present, whereas a large retail environment commonly standardizes on SD-WAN.

Valid ZDTE Dumps shared by BraindumpsPass.com for Helping Passing ZDTE Exam! BraindumpsPass.com now offer the **newest ZDTE exam dumps**, the BraindumpsPass.com ZDTE exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com ZDTE dumps with Test Engine here: https://www.braindumpspass.com/Zscaler/ZDTE-practice-exam-dumps.html (**62** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)