Zscaler ZDTE Practice Questions

Shared by Little on 21-10-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What feature enables Zscaler logs to be sent to SIEM solutions for long-term storage?

Options:

A- Role-Based Access Control (RBAC)
B- Zero Trust Exchange Query Engine
C- Log Recovery Service
D- Log Streaming Services

Answer:

D

Explanation:

Zscaler provides specialized Log Streaming Services to export logs from the Zero Trust Exchange into external SIEM or log-analytics platforms for long-term storage and advanced analysis. For Zscaler Private Access (ZPA), the Log Streaming Service (LSS) forwards user activity, user status, App Connector metrics, and other diagnostic logs to a log receiver, which is typically a SIEM, syslog collector, or similar downstream system. Zscaler documentation notes that customers use LSS specifically to store logs beyond the default cloud retention period and to support external analytics and compliance use cases.

On the ZIA side, Nanolog Streaming Service (NSS) fulfills a similar purpose, streaming web and firewall logs from the Zscaler Nanolog cluster into SIEM solutions. Together, these streaming services give organizations centralized visibility and long-term retention while keeping the Zscaler cloud optimized for inline inspection and near-term reporting.

Role-Based Access Control (RBAC) governs who can view or manage configurations, not how logs are exported. The Zero Trust Exchange query or insights interfaces are used for in-portal searching and visualization, and ''Log Recovery Service'' is not the Zscaler term used for SIEM integration in ZDTE materials. Therefore, Log Streaming Services is the correct answer because it is the named mechanism for streaming Zscaler logs to external SIEM platforms for long-term storage.

==========

Question 2

Question Type: MultipleChoice

What is the default classification for a newly discovered application in the App Inventory in the Third-Party App Governance Admin Portal?

Options:

A- Sanctioned
B- Unsanctioned
C- Reviewing
D- Unclassified

P2P exams

Answer:

D

Explanation:

In Zscaler 3rd-Party App Governance documentation, the App Inventory is where administrators view and manage all discovered third-party apps, add-ons, and extensions. The ''Classifying Apps'' help article defines the available states: Unclassified, Sanctioned, Reviewing, and Unsanctioned. Crucially, it notes that Unclassified is the default state for any new application before an administrator evaluates it.

''Sanctioned'' is used once the organization has explicitly approved an app for use; ''Unsanctioned'' is used when an app is not allowed; and ''Reviewing'' indicates it is under investigation. Those labels are the result of governance decisions applied after discovery.

ZDTE study materials on SaaS and app governance mirror this behavior: newly discovered apps enter the inventory without an explicit decision, allowing security teams to triage risk, review permissions, and only then mark them as sanctioned or unsanctioned. Because the default state for a new entry is explicitly documented as Unclassified, the correct answer is D. Unclassified.

P2P exams

Question 3

Question Type: MultipleChoice

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?

Options:

A- Data Security Posture Management (DSPM)
B- Cloud Sandbox
C- Cloud Access Security Broker (CASB)
D- SaaS Security Posture Management (SSPM)

Answer:

A

Explanation:

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).

==========

Question 4

Question Type: MultipleChoice

How does log streaming work in ZIA?

Options:

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:

C

Explanation:

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.

==========

Question 5

Question Type: MultipleChoice

What are the four distinct stages in the Cloud Sandbox workflow?

Options:

A- Pre-Filtering Cloud Effect Behavioral Analysis Post-Processing
B- Behavioral Analysis Post-Processing Engage your SOC Team for further investigation
C- Cloud Effect Pre-Filtering Behavioral Analysis Post-Processing
D- Pre-Filtering Behavioral Analysis Post-Processing Cloud Effect

Answer:

C

Explanation:

Zscaler Cloud Sandbox is described in Zscaler threat-protection training as following a four-stage workflow. The documented order is: Cloud Effect, Pre-Filtering, Behavioral Analysis, and Post-Processing.

Cloud Effect -- Before detonation, files are checked against global threat intelligence and prior sandbox verdicts so that known malicious objects can be immediately blocked, and known benign files can be allowed without re-analysis.

Pre-Filtering -- Static and signature-based checks (antivirus, file heuristics, and related engines) quickly discard clearly malicious or clearly safe files, reducing load on deep analysis.

Behavioral Analysis -- Suspicious or unknown samples are executed in a virtual environment to observe behavior such as process spawning, registry changes, or C2 activity.

Post-Processing -- Final verdicts are generated, policies are enforced (block, quarantine, allow), and new indicators are fed back into threat intelligence for future Cloud Effect decisions.

This exact ordered sequence---Cloud Effect Pre-Filtering Behavioral Analysis Post-Processing---is what appears in ZDTE study material, so option C is correct.

Question 6

Question Type: MultipleChoice

What feature enables Zscaler logs to be sent to SIEM solutions for long-term storage?

Options:

A- Role-Based Access Control (RBAC)
B- Zero Trust Exchange Query Engine
C- Log Recovery Service
D- Log Streaming Services

Answer:

D

Explanation:

Zscaler provides specialized Log Streaming Services to export logs from the Zero Trust Exchange into external SIEM or log-analytics platforms for long-term storage and advanced analysis. For Zscaler Private Access (ZPA), the Log Streaming Service (LSS) forwards user activity, user status, App Connector metrics, and other diagnostic logs to a log receiver, which is typically a SIEM, syslog collector, or similar downstream system. Zscaler documentation notes that customers use LSS specifically to store logs beyond the default cloud retention period and to support external analytics and compliance use cases.

On the ZIA side, Nanolog Streaming Service (NSS) fulfills a similar purpose, streaming web and firewall logs from the Zscaler Nanolog cluster into SIEM solutions. Together, these streaming services give organizations centralized visibility and long-term retention while keeping the Zscaler cloud optimized for inline inspection and near-term reporting.

Role-Based Access Control (RBAC) governs who can view or manage configurations, not how logs are exported. The Zero Trust Exchange query or insights interfaces are used for in-portal searching and visualization, and ''Log Recovery Service'' is not the Zscaler term used for SIEM integration in ZDTE materials. Therefore, Log Streaming Services is the correct answer because it is the named mechanism for streaming Zscaler logs to external SIEM platforms for long-term storage.

==========

Question 7

Question Type: MultipleChoice

When making API calls into a Zscaler environment, which component is the administrator communicating with?

Options:

A- Logging Plane
B- Control Plane
C- Integration Plane
D- Enforcement Plane

Answer:

B

Explanation:

Zscaler's multi-tier cloud architecture is separated into distinct planes: the control plane, enforcement plane, and logging plane. The control plane is implemented by the Central Authority and is described in Zscaler architecture material as the ''brains'' of the platform, responsible for policy definition, administration, orchestration, and the admin UI. Crucially, this same layer also exposes the API interfaces that automation tools and scripts use. In architecture slides, the control plane is explicitly associated with ''Admin UI'' and ''API,'' showing that all administrative programmability terminates there.

The enforcement plane (Public/Private Service Edges) is focused on inspecting and enforcing policy on user traffic, while the logging plane is dedicated to storing and streaming Nanolog data to SIEM or analytics tools. Neither of these planes provides administrative configuration APIs. Study content for the ZDTE exam reinforces that the API infrastructure enables programmatic access to configure the Zero Trust Exchange and is part of the central management layer, not the traffic or logging tiers.

Therefore, when an administrator makes API calls, they are communicating with the Control Plane.

To Get Premium Files for ZDTE Visit

https://www.p2pexams.com/products/zdte

For More Free Questions Visit

https://www.p2pexams.com/zscaler/pdf/zdte

