KaozhengPro

# IT認證考試題庫

# 專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

**Exam** : **ZDTE**

**Title** : Zscaler Digital Transformation Engineer

**Version** : DEMO

1.What is the default classification for a newly discovered application in the App Inventory in the Third-Party App Governance Admin Portal?
A. Sanctioned
B. Unsanctioned
C. Reviewing
D. Unclassified
**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.

2.How many rounds of analysis are performed on a sandboxed sample to determine its characteristics?
A. One static analysis, one dynamic analysis, and a second static analysis of all dropped files and artifacts from the dynamic analysis.
B. As many rounds of analysis as the policy is configured to perform.
C. Only a static analysis is performed.
D. Only one static and one dynamic analysis is performed.
**Answer:** A
**Explanation:**
Zscaler Cloud Sandbox is designed to detect advanced and previously unknown threats by deeply analyzing suspicious files in an isolated environment. According to Zscaler’s documented analysis pipeline, every sandboxed sample goes through a structured, multi-stage process rather than a single pass.
First, the file undergoes static analysis, where the system inspects the file without executing it. This phase looks at elements such as structure, headers, embedded resources, and known malicious patterns or indicators. Next, the file is executed in a dynamic analysis environment (a sandbox) where Zscaler observes runtime behavior such as process creation, registry modifications, file system changes, network connections, and attempts at evasion or privilege escalation.
During this dynamic phase, the file may drop or create additional files and artifacts. Zscaler then performs a second round of static analysis on those dropped components. This secondary static analysis is crucial because many sophisticated threats unpack or download their real payload only at runtime; analyzing those artifacts provides a much clearer view of the full attack chain.
Because of this defined three-step approach—static, dynamic, then secondary static analysis on dropped artifacts—option A is the correct description of how many rounds of analysis are performed on a sandboxed sample.

3.Which type of sensitive information can be protected using OCR (Optical Character Recognition) technology?
A. Personally Identifiable Information (PII)
B. Network configurations
C. Software licenses
D. Financial transactions
**Answer:** A
**Explanation:**
Zscaler's Data Protection platform integrates Optical Character Recognition (OCR) into its inline Data Loss Prevention (DLP) capabilities. OCR enables Zscaler to extract text embedded within images—such as screenshots, scanned documents, or photos of forms—and subject that text to the same DLP inspection engines that normally analyze plain text content.
Once OCR has converted image content into text, Zscaler can apply predefined dictionaries, custom dictionaries, and advanced classifiers to detect sensitive data types, including personally identifiable information (PII) such as national ID numbers, passport numbers, addresses, or other regulated personal data. This is crucial because many data leaks occur via screenshots or scanned documents that traditional, text-only DLP engines would miss.
While OCR could, in theory, detect patterns related to network configurations, software licenses, or financial transactions, Zscaler's training and exam materials emphasize its use to protect sensitive data in images— especially user-related regulated data such as PII and other compliance-relevant information. Network configurations and software licenses are better addressed through configuration management and IP protection policies, and "financial transactions" describes activities rather than a specific information pattern. Therefore, Personally Identifiable Information (PII) is the best and most exam-accurate answer for the type of sensitive information protected using OCR.

4.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
**Explanation:**
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.

5.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
**Explanation:**
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.