CZTS-001

CERTIFICATION BOARD

Certified Zero Trust Specialist (CZTS)

Exam Objectives CZTS-001

About the exam

Item	Detail
Level	Advanced
Number of questions	120. A performance-based exam: each form can carry up to 5 to 12 performance-based questions alongside the multiple-choice questions.
Delivery model	Computer adaptive in 3 stages of 42, 39, 39 questions. Your score on each stage selects the difficulty of the next, so no two candidates sit the same paper.
Time limit	180 minutes
Scoring	You need a score of 700 out of 900 to pass. Results are reported on a scale of 100 to 900, and 700 corresponds to answering 72% of the exam correctly. Harder questions carry more weight, so a score means the same thing on any route. Multiple-response items and PBQs are scored all or nothing.
Delivery	Online, fully proctored (webcam, microphone and screen).
Prerequisites	No formal prerequisite. Candidates do best with two years in security, identity or infrastructure work and 50 to 80 hours of study.
Retakes	No waiting period after a failed first attempt. Candidates pay the exam price each time they attempt the exam. See the CertLabz Certification Retake Policy at certlabz.com/certification-retake-policy.html
Validity	3 years. Renew with 75 CEUs per cycle and the $55 annual continuing-education fee, or by passing the current exam.
Language	English
Exam voucher	$199 for one sitting, valid 12 months. Bundles add the study guide ebook and the All Access plan.

Domain weights

Domain	Questions
D1 Zero Trust Principles and Architecture (15%)	18
D2 Identity and Access (20%)	24
D3 Devices and Endpoints (13%)	16

D4 Networks and Segmentation (20%)

	24
D5 Applications, Workloads and Data (17%)	20
D6 Visibility, Automation and Migration (15%)	18
Total (100%)	**120**

Objectives by domain

Each objective may appear as knowledge, a scenario to judge, a circuit to trace or assemble, or a number to compute. Each form can carry up to 5 to 12 performance-based questions: drag-and-drop matching, sequencing and table completion, drawn fresh each attempt. The exam does not test any vendor's SDK syntax.

D1 Zero Trust Principles and Architecture — 15% — 18 questions

D1.1 NIST SP 800-207 tenets, logical components and trust algorithms
D1.2 Policy decision point, policy enforcement point, control and data planes
D1.3 CISA Zero Trust Maturity Model 2.0 pillars, cross-cutting capabilities and stages
D1.4 Implicit trust zones, protect surfaces and assume breach
D1.5 Deployment approaches: identity governance, micro-segmentation, software-defined perimeter
D1.6 Threats to the architecture itself and federal mandates (EO 14028, OMB M-22-09)

D2 Identity and Access — 20% — 24 questions

D2.1 Phishing-resistant MFA: FIDO2, passkeys and PIV
D2.2 Conditional and risk-adaptive access, ABAC and dynamic policy
D2.3 Continuous access evaluation, token binding and session revocation
D2.4 Least privilege, just-in-time elevation and privileged access management
D2.5 Workload and service identity: SPIFFE, short-lived credentials, secrets
D2.6 Identity governance: lifecycle automation, access reviews, federation risk

D3 Devices and Endpoints — 13% — 16 questions

D3.1 Device identity: enrollment, hardware-backed certificates and attestation
D3.2 Posture signals from MDM, EDR and configuration management
D3.3 Trust levels for managed, unmanaged, BYOD, server, IoT and OT assets
D3.4 Continuous posture evaluation and graduated enforcement
D3.5 Privileged access workstations and tiered administration
D3.6 Asset inventory as an input to the policy engine

D4 Networks and Segmentation — 20% — 24 questions

D4.1 Micro-segmentation: flow discovery, labels, monitor mode and default deny
D4.2 Zero trust network access, software-defined perimeter and app connectors
D4.3 mTLS, service mesh and encrypting east-west traffic
D4.4 Cloud security groups, Kubernetes NetworkPolicy and identity-based rules
D4.5 Encrypted DNS, egress control and loss of passive visibility
D4.6 Replacing VPN and the hairpin, NAC and SD-WAN as transport

D5 Applications, Workloads and Data — 17% — 20 questions

D5.1 Identity-aware proxies and per-request authorization in applications and APIs
D5.2 Treating internal applications as internet-facing: testing and hardening
D5.3 Workload identity, attestation, signed images and dynamic secrets
D5.4 Data classification driving required assurance
D5.5 Encryption at rest with key access control, DLP and rights management
D5.6 SaaS governance through identity integration and API-based controls

D6 Visibility, Automation and Migration — 15% — 18 questions

D6.1 Telemetry across pillars, decision logs and analytics
D6.2 UEBA, risk scoring and continuous evaluation
D6.3 Automation and orchestration: revocation, quarantine, policy as code
D6.4 Migration roadmaps: inventory, protect surface, iterate, measure
D6.5 Governance: policy standard, exception register, break-glass and metrics
D6.6 Testing with assumed-breach exercises and maturity self-assessment

Continuing education

Renewal	Requirement
Validity	3 years from the date of issue
CEUs required per cycle	75
Annual CE fee	$55
Alternative to CEUs	Pass the current version of the exam before the expiry date

Qualifying activities

Activity	CEUs
CertLabz labs, PBQs, courses and SkillTracker assessments	1 CEU per hour, up to 25 per cycle
Other industry certifications earned or renewed	10 to 25 each, depending on level
Conferences, webinars and training	1 CEU per hour, up to 20 per cycle
Security architecture or engineering work experience	3 per year, up to 9 per cycle
Teaching, mentoring, publishing or open-source contributions	Up to 15 per cycle
College courses in security, networking or computing	10 per completed course

CertLabz Certification Retake Policy

- **No waiting period after a failed first attempt:** If you fail your first attempt at any CertLabz certification examination, CertLabz does not require any waiting period between the first and second attempt.
- **Once you pass, you cannot resit the same exam code:** A candidate who has passed an exam and achieved a certification cannot take that exam again under the same exam code without prior consent from CertLabz. You will need to wait until a new series of the exam is published before attempting to recertify by examination.
- **Beta examinations, one attempt only:** A CertLabz beta examination may be taken one time by each candidate.
- **Violations invalidate the attempt:** A test found to be in violation of this policy will be invalidated, and the candidate may be subject to a suspension period. Repeat violators will be permanently banned from the CertLabz Certification Program.
- **Every attempt is paid for:** Candidates must pay the exam price each time they attempt the exam. CertLabz does not offer free retests or discounts on retakes.

Published by the CertLabz Certification Board, a division of CertLabz LLC. Objectives document CZTS-001.
https://certlabz.com/certifications/certified-zero-trust-specialist.html