EDUSUM

#1 Online Certification Guide

COMPTIA CLOUDNETX CERTIFICATION QUESTIONS & ANSWERS PDF

COMPTIA CLOUDNETX CERTIFICATION QUESTIONS & ANSWERS

Get Instant Access to Vital Exam Acing Materials | Study Guide | Sample Questions | Practice Test

Table of Contents

Getting Ready for the CNX-001 Exam:

Use proven study tips and techniques to prepare for the CNX-001 exam confidently. Boost your readiness, improve your understanding regarding the infrastructure, and increase your chances of success in the CompTIA CloudNetX with our comprehensive guide. Start your journey towards exam excellence today.

CompTIA CloudNetX Certification Details:

Exam Name	CompTIA CloudNetX
Exam Code	CNX-001
Exam Price	$499 (USD)
Duration	165 mins
Number of Questions	90
Passing Score	Pass/Fail
Schedule Exam	**Pearson VUE**
Sample Questions	**CompTIA CloudNetX Sample Questions**
Practice Exam	**CompTIA CNX-001 Certification Practice Exam**

Explore CNX-001 Syllabus:

Topic	Details
Network Architecture Design - 31%	
Given a scenario, analyze business requirements to apply core networking concepts to a network design.	- Open Systems Interconnection (OSI) model - Internet Protocol (IP) addressing • IPv4 • IPv6 • IP subnetting • Classless Inter-domain Routing (CIDR) notation • Variable Length Subnet Mask (VLSM) • Public vs. private • Static vs. dynamic - Network address translation (NAT) • Port forwarding • Port address translation (PAT) • NAT64 - Networking protocols

Topic	Details
	• Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) • Authentication protocols - Power and cooling - 802.1X - Remote Authentication Dial-in User Service (RADIUS) - Terminal Access Controller Access Control System Plus (TACACS+) - Lightweight Directory Access Protocol (LDAP) • Routing protocols - Dynamic 1. Open Shortest Path First (OSPF) 2. Border Gateway Protocol (BGP) - Static 1. Routing tables • Dynamic Host Configuration Protocol (DHCP) • Network Time Protocol (NTP) • Domain Name System (DNS) - Domain Name System Security Extensions (DNSSEC) - DNS over Transport Layer Security (TLS) (DoT) - DNS over Hypertext Transfer Protocol Secure (HTTPS) (DoH) - Container networking - Network virtual interfaces
Given a scenario, analyze business requirements to select and implement the appropriate network architectures and topologies.	- Topology types • Mesh • Star • Hub-and-spoke • Spine-and-leaf • Point-to-point - Zones • Trusted • Untrusted • Screened subnet - Traffic flows • North/south • East/west - Segmentation • Virtual local area network (VLAN) • Virtual extensible LAN (VXLAN) • Generic Network Virtualization Encapsulation (GENEVE) - Environments • Production • Non-production
Given a scenario, analyze requirements to select appropriate connectivity solutions in a hybrid environment.	- Multi-protocol Label Switching (MPLS) - Software-defined wide area network (SD-WAN) - Cellular - Satellite

Topic	Details
	- Dark fiber - Direct internet access - Metro network - Public cloud connectivity • ExpressRoute • Direct Connect • Software-defined cloud interconnect (SDCI) - Remote access • Bastion host • Secure Shell (SSH) • Remote Desktop Protocol (RDP) - Application gateways - Private Platform as a Service (PaaS) connectivity • Service endpoints • Transit gateways • Virtual private cloud (VPC) peering • Private link - Virtual private network (VPN) • Site-to-site • Point-to-site • Remote access • Split tunneling • WireGuard
Given a scenario, analyze availability requirements to recommend technologies that meet business needs.	- Load balancing • Global • Local • Virtual IP (VIP) • Methods - Round robin - Load-based - Least connections - Weighted - High availability • Active-active • Active-passive - Link aggregation - Autoscaling - Regions and availability zones - Content delivery network (CDN) - Fault domains - Update domains - Redundancy • Devices • Paths
Given a scenario, evaluate business requirements to make recommendations for physical campus installations.	- Power considerations • Voltage • Wattage • Amperage • Power distribution unit (PDU) • Uninterruptible power supply (UPS) • Utility power

Topic	Details
	• Emergency power off (EPO) • Backup power generators - Power disruption • Blackout • Brownout • Surge • Spike - Environmental factors • Temperature • Humidity • British thermal units (BTUs) - Fire suppression - Physical access controls • Video surveillance • Biometrics • Proximity readers • Locks and keys • Near-field communication (NFC) • Door sensors
Given a scenario, analyze business requirements to select the appropriate campus wired network components.	- Layer 2 vs. Layer 3 • Switch • Router - Power over Ethernet (PoE) - Three-tier hierarchy • Core • Distribution • Access - Collapsed core - Intermediate distribution frame (IDF)/Main distribution frame (MDF) • Cable management - Spanning Tree Protocol (STP) - Tagging/trunking - Bonding - Voice and video • Session Initiation Protocol (SIP) • WebRTC • Real-time Streaming Protocol (RTSP) • H.323 - Customer premises equipment (CPE) • Media converters
Given a scenario, analyze business requirements to select the appropriate campus wireless network components.	- Wi-Fi • Wireless access points - Antenna types 1. Omni-directional 2. Directional - Placement - Enclosure - Power considerations - Controllers - Standards and protocols

Topic	Details
	1. 802.11 - Frequencies 1. 2.4GHz 2. 5GHz 3. 6GHz - Channels - Service set identifier (SSID) 1. Hidden vs. advertised - Wireless roaming - Bluetooth Low Energy (BLE) - NFC - Long-range wide area network (LoRaWAN)
Given a scenario, analyze requirements to select the appropriate artifacts for architecture documentation.	- Requirements analysis • Business • Technical • Regulatory compliance • Statement of work (SOW) - Network diagramming • Physical vs. logical • High-level vs. low-level designs • Flow diagrams - Verification and validation - Runbooks - Work breakdown structure (WBS) - Knowledge base articles - Baselines - Reference architectures • External • Internal - Configuration management database (CMDB)
Network Security - 28%	
Explain common cloud and network threats, vulnerabilities, and mitigations.	- Threats • Distributed denial-of-service (DDoS) attack • Data exfiltration • On-path attack • Credential reuse • Brute-force attack • Out-of-band (OOB) attack • IP spoofing • Buffer overflow • Privilege escalation • Insider threat • Evil twin • Rogue access point • Initialization vector attack • BGP hijacking • Social engineering attack - Vulnerabilities • Zero-day

Topic	Details
	• Open Worldwide Application Security Project (OWASP) top 10 • Overly permissive rules • IP reuse • Legacy access control lists (ACLs) • Insecure protocols • Unpatched devices • Misconfigurations - Mitigations • Input sanitization • Data loss prevention (DLP) controls • IP address management (IPAM) • MITRE ATT&CK Framework • Cyber Kill Chain • Cloud Controls Matrix (CCM) • Patch management • Vulnerability management • Center for Internet Security (CIS) benchmarks • Configuration reviews • Null routing
Given a scenario, analyze requirements to select the appropriate technology to secure a network.	- Firewalls • Next-generation firewall (NGFW) • Cloud-native firewall • Web application firewall (WAF) - Intrusion prevention system (IPS)/ intrusion detection system (IDS) - Encryption • Protocol types • Secure sockets layer (SSL)/TLS inspection • Cipher suites • Algorithms • Asymmetric • Symmetric - Application gateway - Secure web gateway - Network access control (NAC) • Posture assessment - Dynamic list
Given a scenario, configure the appropriate access controls to secure a network.	- Firewall rules • Decryption rules • Application aware • Source and destination • Allow list • Block list - Network access control lists (NACLs) - Network security groups • Inbound rules • Outbound rules - IPS/IDS signature rules - Geolocation rules - Content/Uniform Resource Locator (URL) filtering

Topic	Details
	• Categories • Applications • File blocking - DLP controls - Port security
Given a scenario, analyze requirements to apply the appropriate Zero Trust architecture (ZTA) principles to secure a network.	- Micro segmentation - Secure Access Service Edge (SASE) • Secure Service Edge (SSE) - Cloud Access Security Broker (CASB) - Identity as the perimeter - Device trust - Principle of least privilege - Zero Trust network access
Given a scenario, apply identity and access management to secure a network environment.	- Single sign-on (SSO) • Federation • Security Assertion Markup Language (SAML) • OAuth 2.0 • OpenID Connect (OIDC) - Multifactor authentication (MFA) - Conditional access - Geofencing - Privileged access management (PAM) - Risk-based authentication - Role-based access control - Attribute-based access control (ABAC) - Endpoint trust - User and entity behavior analytics (UEBA) - Public key infrastructure (PKI) • Certificate-based authentication • Key management system (KMS) - Session-based tokens - Just-in-time (JIT) provisioning - System for Cross-domain Identity Management (SCIM) - Cloud Infrastructure Entitlement Management (CIEM)
Given a scenario, use the appropriate wireless security method or configuration.	- Encryption • Advanced Encryption Standard (AES) • Wi-Fi Protected Access 2 (WPA2) • Wi-Fi Protected Access 3 (WPA3) - Authentication • Temporal Key Integrity Protocol (TKIP) • Preshared key (PSK) • PSK enterprise - Guest access - Captive portal - Layer 2 client isolation - Media access control (MAC) address filtering
Given a scenario, implement the appropriate appliance-hardening technique.	- Patch management • Delivery channels • Verification

Topic	Details
	- Default credential management - Disabling unneeded services - Local password management • Password complexity • Password length • Password rotation - Protocol configuration • Disabling insecure protocols - Restricting access to administrative interfaces - Disabling unused physical ports - Log management • Log rotation • Remote logging
Network Operations, Monitoring, and Performance - 16%	
Explain concepts related to operating and maintaining a network environment.	- Risk management • Risk acceptance - Waivers and exceptions • Risk avoidance • Risk transference • Risk mitigation • Risk register - Business continuity • Mean time to recovery (MTTR) • Mean time between failures (MTBF) • Mean time to detect (MTTD) • Mean time to investigate (MTTI) • Recovery point objective (RPO)/ recovery time objective (RTO) - Disaster recovery - Service management - Auditing - Failure rate - Contracts, agreements, and terms • Interconnection Security Agreement (ISA) • Memorandum of understanding (MOU) • Master service agreement (MSA) • Service-level indicator (SLI)/key performance indicator (KPI) • Service-level objective (SLO) • Service-level agreement (SLA) • Operational-level agreement (OLA) • Non-disclosure agreement (NDA) • Licensing agreements • End-of-life (EOL)/end-of support (EOS) - Network function virtualization (NFV) • Firewall as a service • Reverse proxy • Forward proxy • NAT gateways

Topic	Details
	- OOB management - Network cost management • Operating expenditure (OpEx) • Capital expenditure (CapEx) • Cost optimization • Chargeback model • Orphaned resources - Service delivery • Self-service • Cross-connect • Time to market
Given a scenario, use tools and techniques related to monitoring and performance.	- Traffic analysis • Traffic mirroring • Throughput • Latency • Loss • Jitter • Network flows • Reachability - Log collection • Centralized logging • Security information and event management (SIEM) • Syslog • JavaScript Object Notation (JSON) • Data lake - Simple Network Management Protocol (SNMP) - Quality of service (QoS) - Alerting - Telemetry - Dashboards • Status pages - Metrics - Continuous monitoring • Resource utilization • Bandwidth utilization • Reactive vs. proactive monitoring
Given a scenario, apply automation and scripting to administer a hybrid cloud environment.	- Infrastructure as code (IaC) • Resource provisioning • Resource configuration • Yet Another Markup Language (YAML) • JSON • Linters - Life cycle management • Mutable infrastructure • Immutable infrastructure • Patch management - Version control • Public vs. private repositories • Secrets management - DevOps

Topic	Details
	• Continuous integration and continuous delivery (CI/CD) pipeline management • GitOps - Generative artificial intelligence (AI) - Application programming interface (API) - Software development kit (SDK) - Command-line interface (CLI) - Desired state • Configuration reviews • Baselines/benchmarks • Configuration backup and restore - Change management
Network Troubleshooting - 25%	
Explain the troubleshooting methodology.	- Identify the problem • Gather information • Question users • Identify symptoms • Determine if anything has changed • Duplicate the problem, if possible • Approach multiple problems individually - Establish a theory of probable cause • Question the obvious • Consider multiple approaches - Top-to-bottom/bottom-to-top OSI model - Divide and conquer - Test the theory to determine cause • If the theory is confirmed, determine the next steps to resolve the problem • If the theory is not confirmed, re-establish a new theory or escalate - Establish a plan of action to resolve the problem and identify potential effects - Implement the solution or escalate as necessary - Verify full system functionality and if applicable implement preventive measures - Document findings, actions, outcomes, and lessons learned throughout the process
Given a scenario, use the appropriate tool or command.	- Tools • Wireshark • Netcat • Nmap • Iperf • radclient • OpenSSL • Postman - Commands • tcpdump • dig • mtr • arp

Topic	Details
	• netstat • curl • ping • nslookup • traceroute • ip • ipconfig - flushdns • ifconfig • route • ss • dhclient • top • snmpwalk • nfdump
Given a scenario, analyze output from network tools and commands to resolve issues.	- Tools • Wireshark • Netcat • Nmap • Iperf • radclient • OpenSSL • Postman • Spectrum analyzer • Heat map • SIEM - Commands • tcpdump • dig • mtr • arp • netstat • curl • ping • nslookup • traceroute • ip • ipconfig • ifconfig • route • ss • dhclient • top • snmpwalk • nfdump - Performance issues - Connectivity issues - Access and security issues
Given a scenario, troubleshoot connectivity issues.	- Intermittent connectivity - DNS issues - Asymmetric routing

Topic	Details
	- Port exhaustion - Port misconfiguration • VLAN assignment - Duplicated IP addresses - Duplicated MAC addresses - IP address exhaustion - NAT table exhaustion - DHCP issues - Request timeouts - IPv6 router advertisements - Physical layer disruptions - Stale cache - IPSec issues - BGP issues - Routing loops - Single point of failure
Given a scenario, troubleshoot network performance issues.	- Latency issues - Packet loss - Maximum transmission unit (MTU) issues • Misconfigured jumbo frames • Fragmentation - Hairpinning - Broadcast storm - Resource exhaustion - Bandwidth issues • Overutilization • Bottleneck • Throttling - Network scanning issues
Given a scenario, troubleshoot Wi-Fi performance issues.	- Signal interference - Signal loss - Signal degradation - Low signal strength - Band steering issues - Channel overlap - Incorrect channel width - Client disassociation - Roaming issues • Sticky clients - Transmitter/receiver incompatibility
Given a scenario, troubleshoot access and security issues.	- Rule and policy issues • Incorrect security group • Missing rules • Misconfigured rules • Overly permissive rules • URL/web content filtering • Geo-restriction • ACL issues - DoS issues • DDoS • SYN floods

Topic	Details
	- Authentication and authorization failures • Password issues • Incorrect group membership • Mismatched secrets - Certificate issues • Mismatch • Expired certificates • Revoked certificates • Trust issues • Hash incompatibility • TLS issues - Blocked or dropped traffic

Prepare with CNX-001 Sample Questions:

Question: 1

An organization uses a managed service provider for its network infrastructure. The organization decides to switch to another provider and implement the latest network technologies available in the market. As part of the transformation, different documents need to be prepared.

Which of the following documents would be the most valuable for a network architect to use?

a) Low-level designs
b) Flow diagrams
c) Runbooks
d) Baselines

Answer: d

Question: 2

A company that hosts its website in a private data center receives reports that the company's website is now pointing to a website with offensive material. No changes were made to the network, and the company's website appears normal from the internal network.

Which of the following attacks is the company most likely experiencing?

a) BGP hijack
b) Out-of-band
c) Evil twin
d) On-path

Answer: a

Question: 3

When analyzing traceroute output, what does a consistent timeout ("* * *") at a specific hop indicate?

a) DNS misconfiguration
b) ICMP rate limiting or firewall block
c) Packet fragmentation
d) MTU discovery failure

Answer: b

Question: 4

A network engineer suspects high latency in traffic between edge routers and cloud gateways during business hours. Which tools or techniques should be used to validate the issue? (Select TWO)

a) NetFlow collector
b) Packet capture at endpoints
c) BGP route injection
d) Latency heatmaps from monitoring tools

Answer: a, d

Question: 5

Why might a network admin receive failed login attempts from unknown IP addresses on port 22?

a) DoS attack
b) Brute-force attack
c) DNS amplification
d) VLAN hopping

Answer: b

Question: 6

What is the MOST likely cause of increased latency and packet retransmissions in a high-bandwidth, low-latency environment?

a) MTU fragmentation
b) Asymmetric routing
c) Duplex mismatch
d) VLAN misconfiguration

Answer: c

Question: 7

A company operates in a hybrid cloud environment and needs security solutions to monitor and protect services. Which of the following would best protect the environment?

a) Cloud Controls Matrix
b) MITRE ATT&CK framework
c) OWASP Top Ten
d) CIS Benchmarks

Answer: d

Question: 8

You are reviewing the configuration of a recently deployed intrusion prevention system (IPS). You must ensure that it follows hardened security practices. Which configurations should be validated? (Select TWO)

a) Disable remote administrative access over HTTP
b) Enable default alert logging
c) Integrate with centralized authentication (LDAP/RADIUS)
d) Allow anonymous read-only login

Answer: a, c

Question: 9

A network engineer is testing the network throughput between Linux servers in a hybrid environment. The engineer needs to measure bandwidth between the servers on premises and servers in the cloud to validate network throughput against the ISP SLA.

Which of the following is the best tool for this task?

a) iperf
b) tcpdump
c) netcat
d) netstat

Answer: a

Question: 10

Which of the following is an effective mitigation against Distributed Denial-of-Service (DDoS) attacks in a cloud environment?

a) Implementing strong password policies
b) Using web application firewalls (WAFs)
c) Deploying intrusion detection systems (IDS)
d) Utilizing cloud-based DDoS protection services

Answer: d

Study Tips to Pass the CompTIA CloudNetX Exam:

Understand the CNX-001 Exam Format:

Before diving into your study routine, it's essential to familiarize yourself with the CNX-001 exam format. Take the time to review the **exam syllabus**, understand the test structure, and identify the key areas of focus. Prior knowledge of what to expect on exam day will help you tailor your study plan.

Make A Study Schedule for the CNX-001 Exam:

To effectively prepare for the CNX-001 exam, make a study schedule that fits your lifestyle and learning style. Set specific time slots for studying each day and focus on the topics based on their importance and your proficiency level. Consistency is a must, so stick to your schedule and avoid procrastination.

Study from Different Resources:

Make sure to expand beyond one source of study material. Utilize multiple resources such as textbooks, online courses, practice exams, and study guides to understand the CNX-001 exam topics comprehensively. Each resource offers unique insights and explanations that can enhance your learning experience.

Practice Regularly for the CNX-001 Exam:

Practice makes you perfect for the **CNX-001 exam preparation** as well. Regular practice allows you to reinforce your knowledge of key concepts, enhance your problem-solving skills, and familiarize yourself with the exam format. Dedicate time to solving practice questions and sample tests to gauge your progress.

Take Breaks and Rest:

While it's essential to study, taking breaks and allowing yourself to rest is equally important. Overloading your brain with information without adequate rest can lead to burnout and decreased productivity. Set short breaks during your study sessions to recharge and maintain focus.

Stay Organized During the CNX-001 Exam Preparation:

Stay organized throughout your CNX-001 study journey by keeping track of your progress and materials. Maintain a tidy study space, use folders or digital tools to organize your notes and resources, and create a checklist of topics to cover. An organized approach helps you stay on track and minimize stress.

Seek Clarification from Mentors:

Feel free to seek clarification if you encounter any confusing or challenging concepts during your study sessions. Reach out to peers, instructors, or online forums for assistance. Clarifying doubts early on will prevent misunderstandings and ensure you have a **solid grasp** of the material.

Regular Revision Plays A vital Role for the CNX-001 Exam:

Consistent revision is essential for the long-term retention of information. Review previously covered topics to reinforce your understanding and identify any areas requiring additional attention. Reviewing regularly will help solidify your knowledge and boost your confidence.

Practice Time Management for the CNX-001 Exam:

Effective time management is crucial on exam day to ensure you complete all sections within the allocated time frame. During your practice sessions, simulate CNX-001 exam conditions and practice pacing yourself accordingly. Develop strategies for tackling each section efficiently to maximize your score.

Stay Positive and Confident:

Lastly, always have a positive mindset and believe in your abilities. Stay confident in your preparation efforts and trust that you have adequately equipped yourself to tackle the CNX-001 exam. Visualize success, stay focused, and approach the exam calmly and confidently.

Benefits of Earning the CNX-001 Exam:

- Achieving the CNX-001 certification opens doors to new career opportunities and advancement within your field.
- The rigorous preparation required for the CNX-001 exam equips you with in-depth knowledge and practical skills relevant to your profession.
- Holding the CNX-001 certification demonstrates your expertise and commitment to excellence, earning recognition from peers and employers.
- Certified professionals often grab higher salaries and enjoy greater earning potential than their non-certified counterparts.
- Obtaining the CNX-001 certification validates your proficiency and credibility, instilling confidence in clients, employers, and colleagues.

Discover the Reliable Practice Test for the CNX-001 Certification:

Edusum brings you comprehensive information about the CNX-001 exam. We offer genuine practice tests tailored for the CNX-001 certification. What benefits do these practice tests offer? You'll encounter authentic exam-like questions crafted by industry experts, providing an opportunity to enhance your performance in the actual exam. Count on Edusum for rigorous, unlimited access to **CNX-001 practice tests** over two months, enabling you to bolster your confidence steadily. Through dedicated practice, many candidates have succeeded in streamlining their journey towards obtaining the CompTIA CloudNetX.

Concluding Thoughts:

Preparing for the CNX-001 exam requires dedication, strategy, and effective study techniques. These study tips can enhance your preparation, boost your confidence, and improve your chances of passing the exam with flying colors. Remember to stay focused, stay organized, and believe in yourself. Good luck!

Here is the Trusted Practice Test for the CNX-001 Certification

EduSum.com offers comprehensive details about the CNX-001 exam. Our platform provides authentic practice tests designed for the CNX-001 exam. What benefits do these practice tests offer? By accessing our practice tests, you will encounter questions closely resembling those crafted by industry experts in the exam. This allows you to enhance your performance and readiness for the real exam. Count on Edusum to provide rigorous practice opportunities, offering unlimited attempts over two months for the CNX-001 practice tests. Through consistent practice, many candidates have found success and simplified their journey towards attaining the CompTIA CloudNetX.

Start Online Practice of CNX-001 Exam by Visiting URL

https://www.edusum.com/comptia/cnx-001-comptia-cloudnetx