CompTIA CloudNetX Certification Exam Objectives

EXAM NUMBER: CNX-001 V1

CompTIA CloudNetX CNX-001 V1 Certification Exam
Exam Objectives Document Version 5.0
Copyright © 2023 CompTIA, Inc. All rights reserved.

About the Exam

The CompTIA CloudNetX CNX-001 V1 certification exam will certify the successful candidate has the knowledge and skills required to:

- Analyze business requirements to design and configure secure network architecture for on-premises and cloud environments.
- Analyze requirements to design for network security, availability, Zero Trust, and identity and access management technologies.
- Apply and configure concepts and tools related to network monitoring and performance, automation, and scripting.
- Troubleshoot network issues related to connectivity, performance, access, and security.
- Perform network operation and maintenance.

EXAM ACCREDITATION

The CompTIA CloudNetX CNX-001 V1 exam is accredited by the ANSI National Accreditation Board (ANAB) to show compliance with the International Organization for Standardization (ISO) 17024 standard and, as such, undergoes regular reviews and updates to the exam objectives..

EXAM DEVELOPMENT

CompTIA exams result from subject matter expert workshops and industry-wide survey results regarding the skills and knowledge required of an IT professional.

COMPTIA AUTHORIZED MATERIALS USE POLICY

CompTIA Certifications, LLC is not affiliated with and does not authorize, endorse, or condone utilizing any content provided by unauthorized third-party training sites (aka “brain dumps”). Individuals who utilize such materials in preparation for any CompTIA examination will have their certifications revoked and be suspended from future testing in accordance with the CompTIA Candidate Agreement. In an effort to more clearly communicate CompTIA’s exam policies on use of unauthorized study materials, CompTIA directs all certification candidates to the CompTIA Certification Exam Policies. Please review all CompTIA policies before beginning the study process for any CompTIA exam. Candidates will be required to abide by the CompTIA Candidate Agreement. If a candidate has a question as to whether study materials are considered unauthorized (aka “brain dumps”), they should contact CompTIA at examsecurity@comptia.org to confirm.

PLEASE NOTE

The lists of examples provided in bulleted format are not exhaustive lists. Other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam, although not listed or covered in this objectives document. CompTIA is constantly reviewing the content of our exams and updating test questions to be sure our exams are current, and the security of the questions is protected. When necessary, we will publish updated exams based on existing exam objectives. Please know that all related exam preparation materials will still be valid.

Copyright © 2023 CompTIA, Inc. All rights reserved.

TEST DETAILS

Required exam	CloudNetX CNX-001 V1
Number of questions	Maximum of 90
Types of questions	Multiple-choice and performance-based
Length of test	
Recommended experience	A minimum of ten years of experience in the IT field and five years of experience in a network architect role, with experience in the hybrid cloud environment. Network+, Security+, and Cloud+ or equivalent experience.
Passing Score	Pass/fail only; no scaled score

EXAM OBJECTIVES (DOMAINS)

The table below lists the domains measured by this examination and the extent to which they are represented.

DOMAIN		PERCENTAGE OF EXAMINATION
1.0	Network Architecture Design	31%
2.0	Network Security	28%
3.0	Network Operations, Monitoring, and Performance	16%
4.0	Network Troubleshooting	25%
Total		**100%**

Copyright © 2023 CompTIA, Inc. All rights reserved.

1.0 Network Architecture Design

1.1 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
  - 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
      - Open Shortest Path First (OSPF)
      - Border Gateway Protocol (BGP)
    - Static
      - 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

1.2 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

Copyright © 2023 CompTIA, Inc. All rights reserved.

1.3 Given a scenario, analyze requirements to select appropriate connectivity solutions in a hybrid environment.

- Multiprotocol Label Switching (MPLS)
- Software-defined wide area network (SD-WAN)
- Cellular
- Satellite
- 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

1.4 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

1.5 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
  - 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

Copyright © 2023 CompTIA, Inc. All rights reserved.

1.6 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

1.7 Given a scenario, analyze business requirements to select the appropriate campus wireless network components.

- Wi-Fi
  - Wireless access points
    - Antenna types
      - Omni-directional
      - Directional
    - Placement
    - Enclosure
    - Power considerations
  - Controllers
  - Standards and protocols
    - 802.11
  - Frequencies
    - 2.4GHz
    - 5GHz
    - 6GHz
  - Channels
  - Service set identifier (SSID)
    - Hidden vs. advertised
  - Wireless roaming
- Bluetooth Low Energy (BLE)
- NFC
- Long-range wide area network (LoRaWAN)

1.8 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)

Copyright © 2023 CompTIA, Inc. All rights reserved.

2.0 Network Security

2.1 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
  - 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

2.2 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

2.3 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
  - Categories
  - Applications
  - File blocking
- DLP controls
- Port security

Copyright © 2023 CompTIA, Inc. All rights reserved.

2.4 Given a scenario, analyze requirements to apply the appropriate Zero Trust architecture (ZTA) principles to secure a network.

- Microsegmentation
- 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

2.5 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)
  - Passwordless
- 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)

2.6 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

2.7 Given a scenario, implement the appropriate appliance-hardening technique.

- Patch management
  - Delivery channels
  - Verification
- 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

Copyright © 2023 CompTIA, Inc. All rights reserved.

3.0 Network Operations, Monitoring, and Performance

3.1 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
- 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

3.2 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

Copyright © 2023 CompTIA, Inc. All rights reserved.

3.3 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
  - 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

Copyright © 2023 CompTIA, Inc. All rights reserved.

4.0 Network Troubleshooting

4.1 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

4.2 Given a scenario, use the appropriate tool or command.

- Tools
  - Wireshark
  - Netcat
  - Nmap
  - Iperf
  - radclient
  - OpenSSL
  - Postman
- Commands
  - tcpdump
  - dig
  - mtr
  - arp
  - netstat
  - curl
  - ping
  - nslookup
  - traceroute
  - ip
  - ipconfig
    - flushdns
  - ifconfig
  - route
  - ss
  - dhclient
  - top
  - snmpwalk
  - nfdump

4.3 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

Copyright © 2023 CompTIA, Inc. All rights reserved.

4.4 Given a scenario, troubleshoot connectivity issues.

- Intermittent connectivity
- DNS issues
- Asymmetric routing
- 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
- Internet Protocol Security (IPSec) issues
- BGP issues
- Routing loops
- Single point of failure

4.5 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

4.6 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

4.7 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
- Denial of service (DoS) issues
  - DDoS
  - SYN floods
- 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

Copyright © 2023 CompTIA, Inc. All rights reserved.

CompTIA CloudNetX CNX-001 Acronym List

The following is a list of acronyms that appears on the CompTIA CloudNetX CNX-001 V1 exam. Candidates are encouraged to review the complete list and attain a working knowledge of all listed acronyms as part of a comprehensive exam preparation program.

ACRONYM	DEFINITION
AAA	Authentication, Authorization, and Accounting
ABAC	Attribute-based Access Control
ACL	Access Control List
ACME	Automated Certificate Management Environment Protocol
AES	Advanced Encryption Standard
AI	Artificial Intelligence
AP	Access Point
API	Application Programming Interface
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
BGP	Border Gateway Protocol
BIA	Business Impact Analysis
BLE	Bluetooth Low Energy
BPDU	Bridge Protocol Data Units
BPF	Berkeley Packet Filter
BTU	British Thermal Unit
BYOD	Bring Your Own Device
CASB	Cloud Access Security Broker
CCM	Cloud Controls Matrix
CCTV	Closed-circuit TV
CDN	Content Delivery Network
CI/CD	Continuous Integration and Continuous Deployment
CIDR	Classless Inter-domain Routing
CIEM	Cloud Infrastructure Entitlement Management
CIS	Center for Internet Security
CLI	Command-line Interface
CMDB	Configuration Management Database
CPE	Customer Premises Equipment
CPU	Central Processing Unit
CSP	Cloud Service Provider
DAC	Discretionary Access Control
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DLP	Data Loss Prevention
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DoH	DNS over HTTPS
DoS	Denial of Service
DoT	DNS over TLS
EDR	Endpoint Detection and Response
EOL	End-of-life
EOS	End-of-support
EPO	Emergency Power Off

Copyright © 2023 CompTIA, Inc. All rights reserved.

ACRONYM	DEFINITION
FCoE	Fibre Channel Over Ethernet
FTP	File Transfer Protocol
GDPR	General Data Protection Regulation
GENEVE	Generic Network Virtualization Encapsulation
HCL	HashiCorp Configuration Language
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a Service
IaC	Infrastructure as Code
IAM	Identity and Access Management
IDF	Intermediate Distribution Frame
IDS	Intrusion Detection System
IoT	Internet of Things
IP	Internet Protocol
IPAM	IP Address Management
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
ISA	Interconnection Security Agreement
ISO	Industry Standards Organization
ISP	Internet Service Provider
JIT	Just-in-time
JSON	JavaScript Object Notation
KMS	Key Management System
KPI	Key Performance Indicator
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LoRaWAN	Long-range Wide Area Network
MAC	Media Access Control
MDF	Main Distribution Frame
MDM	Mobile Device Management
MFA	Multifactor Authentication
MIB	Management Information Base
MOU	Memorandum of Understanding
MPLS	Multiprotocol Label Switching
MSA	Master Service Agreement
MSP	Managed Service Provider
MTBF	Mean Time Between Failures
MTTD	Mean Time To Detect
MTTI	Mean Time To Investigate
MTTR	Mean Time To Recovery
MTU	Maximum Transmission Unit
MX	Mail Exchange
NAC	Network Access Control
NACL	Network Access Control List
NAS	Network-attached Storage
NAT	Network Address Translation
NDA	Non-disclosure Agreement
NFC	Near-field Communication
NFS	Network File System
NFV	Network Function Virtualization
NGFW	Next-generation Firewall
NIC	Network Interface Card
NOC	Network Operations Center

Copyright © 2023 CompTIA, Inc. All rights reserved.

ACRONYM	DEFINITION
NSG	Network Security Group
NTP	Network Time Protocol
OIDC	OpenID Connect
OLA	Operational-level Agreement
OOB	Out-of-band
OS	Operating System
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
OTP	One-time Password
OWASP	Open Worldwide Application Security Project
PaaS	Platform as a Service
PAM	Privileged Access Management
PAT	Port Address Translation
PCAP	Packet Capture
PDU	Power Distribution Unit
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PoE	Power over Ethernet
PSK	Pre-shared Key
QoS	Quality of Service
QR	Quick Response
RADIUS	Remote Authentication Dial-in User Services
RAID	Redundant Array of Independent Disks
RDP	Remote Desktop Protocol
REST	Representational State Transfer
RPO	Recovery Point Objective
RTMP	Real-time Messaging Protocol
RTO	Real Time Objective
RTSP	Real-time Streaming Protocol
S/MIME	Secure/multipurpose Internet Mail Extensions
SaaS	Software as a Service
SAE	Simultaneous Authentication of Equals
SAML	Security Assertion Markup Language
SASE	Secure Access Service Edge
SCIM	System for Cross-interdomain Identity Management
SDCI	Software-defined Cloud Interconnect
SDK	Software Development Kit
SD-WAN	Software-defined Wide Area Network
SFP	Small Form-factor Pluggable
SIEM	Security Information and Event Management
SIP	Session Initiation Protocol
SLA	Service-level Agreement
SLI	Service-level Indicator
SLO	Service-level Objective
SNMP	Simple Network Management Protocol
SOAR	Security Orchestration, Automation, and Response
SOW	Statement of Work
SQL	Structured Query Language
SSE	Secure Service Edge
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-on
STP	Spanning Tree Protocol

Copyright © 2023 CompTIA, Inc. All rights reserved.

ACRONYM	DEFINITION
TACACS+	Terminal Access Controller Access Control System Plus
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTL	Time to Live
UDP	User Datagram Protocol
UEBA	User and Entity Behavior Analytics
UPS	Uninterruptible Power Supply
URL	Uniform Resource Locator
VDI	Virtual Desktop Infrastructure
VIP	Virtual IP
VLAN	Virtual Local Area Network
VLSM	Variable Length Subnet Mask
VM	Virtual Machine
VoIP	Voice Over Internet Protocol
VPC	Virtual Private Cloud
VPN	Virtual Private Network
VXLAN	Virtual Extensible LAN
WAF	Web Application Firewall
WAN	Wide Area Network
WAP	Wireless Access Point
WBS	Work Breakdown Structure
WLAN	Wireless Local Area Network
WPA2	Wi-Fi Protected Access 2
WPA3	Wi-Fi Protected Access 3
XML	Extensible Markup Language
XXS	Cross-site Scripting
YAML	Yet Another Markup Language
ZTA	Zero Trust Architecture
ZTNA	Zero Trust Network Access

Copyright © 2023 CompTIA, Inc. All rights reserved.

CloudNetX Proposed Hardware and Software List

CompTIA has included this sample list of hardware and software to assist candidates as they prepare for the CloudNetX CNX-001 V1 exam. This list may also be helpful for training companies who wish to create a lab component to their training offering. The bulleted lists below each topic are a sample list and not exhaustive.

HARDWARE

- NGFWs
- Routers
- Switches
- Wireless access points
- Wireless controllers
- Cables
- Spectrum analyzer
- Cable tester

SOFTWARE

- Device enumeration software
- Protocol analyzer
- Cisco packet tracer
- Load balancer
- CLI
- Wireshark
- Nmap
- Sample packet capture (pcap) files
- Diagramming software
- Access to Linux and Windows operating systems
- Postman
- Terraform
- IPS/IDS
- Git client
- Python/Bash/PowerShell
- Log samples
- Integrated development environment

OTHER

- Whiteboard
- Access to a cloud provider
- OWASP Top Ten
- MITRE ATT&CK Framework
- Cloud Security Alliance Cloud Controls Matrix (CCM)
- CIS benchmarks

CompTIA

© 2023 CompTIA, Inc., used under license by CompTIA, Inc. All rights reserved. All certification programs and education related to such programs are operated exclusively by CompTIA, Inc. CompTIA is a registered trademark of CompTIA, Inc. in the U.S. and internationally. Other brands and company names mentioned herein may be trademarks or service marks of CompTIA, Inc. or of their respective owners. Reproduction or dissemination prohibited without the written consent of CompTIA, Inc. Printed in the U.S. 11563-Nov2024