CompTIA CloudNetX CNX-001

Course Duration: 40 Hours **Course code: CNX-001**

1. Course Overview

The CompTIA CloudNetX CNX-001 certification validates advanced capabilities in designing and managing secure, scalable hybrid network solutions across cloud and on-premises environments. This course equips seasoned IT professionals with expertise in network architecture, security (including Zero Trust frameworks), monitoring, automation, troubleshooting, and operations. It prepares learners for the demands of enterprise-level hybrid cloud networking and supports career advancement in roles such as Network Architect, Security Architect, Cloud Systems Architect, and Enterprise Infrastructure Engineer.

2. What you'll learn?

By the end of this course, you'll be able to:

- Analyze requirements and design secure hybrid network architectures for both on-premises and cloud environments.
- Apply Zero Trust principles and identity/access management strategies effectively.
- Implement network monitoring, performance tuning, automation, and scripting workflows.
- Troubleshoot issues spanning connectivity, security, access, and performance.
- Perform operational and maintenance tasks for stable network environments.

3. Target Audience

- Experienced IT professionals with ~10 years in IT and ~5 years in network or infrastructure architecture roles, especially in hybrid cloud contexts.

- Holders of foundational certs like Network+, Security+, Cloud+ or equivalent skills.

4. Pre-Requisites

- Minimum of 10 years in IT, with at least 5 years in network/architect roles.
- Prior experience and certification (Network+, Security+, Cloud+).

5. Course content

Module 1: Course Introduction

Introduction

Course Contents

Module 2: Introduction to CloudNetX & Hybrid Networking

What is CompTIA CloudNetX?

Vendor-neutral hybrid networking focus

Why CloudNetX matters today

Summary

Module 3: Network Architecture Design

IP addressing and routing concepts

Network topologies: mesh, star, spine-and-leaf

Hybrid connectivity: VPN, SD-WAN, MPLS, cloud links

Redundancy, autoscaling, load balancing, CDNs

Module 4: Network Security Design

Threat analysis and mitigation

Firewalls, NAC, encryption, ZTNA, CASB, SASE

Access controls: firewall rules, security groups, URL filtering

IAM: SSO, MFA, PKI, privileged access

Wireless network security

Module 5: Network Operations, Monitoring & Performance

Operational risk and continuity

Monitoring tools: dashboards, logging, alerting

Automation: IaC and scripting for hybrid networks

Module 6: Troubleshooting Hybrid Networks

DNS, VPN, and cloud connectivity issues

Latency, packet loss, load balancing issues

Firewall problems and unauthorized access fixes

Module 7: Planning an Exam-Ready Training Approach

Mapping learning to the official exam domains

Structuring hands-on labs and simulations

Best practices for mastering performance-based questions

Module 8: Practice Exam Simulation

Timed mock tests up to 90 questions (multiple-choice and performance-based)

Review answers, rationales, and improvement strategies

Module 9: Logging, Monitoring & Metrics for Certification

CloudNetX-aligned logging strategies

Setting performance baselines and alert thresholds

Using dashboards for monitoring readiness

Module 10: Exam Logistics & Strategy

Exam structure and format: up to 90 questions, 165 minutes, Pass/Fail grading

When and how the exam launched: February 18, 2025

Best practices for day-of readiness and time management in cloud/hybrid scenarios

Module 11: Advanced Topics & Emerging Trends

Multi-cloud networking best practices

Trends in Zero Trust and SASE adoption

Expanding role of automation and observability in network operations

Module 12: Certification Roadmap & Career Impact

Career paths unlocked: Network Operations Specialist, Security Architect, Enterprise Architect

CompTIA CloudNetX in government and DoD contexts (NICE/DCWF job mapping)

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com