

COMPTIA · XPERT SERIES

VERSIÓN 1

CompTIA CloudNetX V1

Examen CNX-001

Diseña y despliega redes híbridas seguras y escalables: la certificación de nivel experto para arquitectos de red.

¿Por qué debería asistir?

CompTIA CloudNetX es la certificación de nivel experto (Xpert Series) que valida la capacidad de diseñar y desplegar redes seguras y escalables en entornos híbridos. Cubre diseño de seguridad, monitoreo, optimización del rendimiento y solución avanzada de problemas, con implementación práctica de Zero Trust, y está orientada a arquitectos de red, de seguridad y empresariales.

Durante el curso, los participantes aprenden a evaluar los requisitos del negocio y diseñar arquitecturas de red seguras para entornos híbridos; a aplicar principios de Zero Trust, configurar controles de acceso y endurecer redes híbridas; a usar herramientas de monitoreo y automatización para mantener operaciones confiables, y a diagnosticar y resolver fallas de conectividad, rendimiento y seguridad en redes híbridas. El programa cubre el 100 % de los objetivos del examen CNX-001.

5 días	4	1	Prácticos	Experto
DURACIÓN	DOMINIOS OFICIALES	EXAMEN	LABORATORIOS	NIVEL



¿Quién debería participar?

Arquitectos de red
Profesionales que diseñan redes empresariales que integran centros de datos y nubes públicas.

Arquitectos de seguridad
Especialistas que llevan Zero Trust, SASE y microsegmentación a redes híbridas.

Arquitectos empresariales
Líderes técnicos que alinean la infraestructura de red con los objetivos del negocio.

Ingenieros de red sénior
Profesionales con Network+, Security+ y Cloud+ o experiencia equivalente que dan el salto al nivel experto.

Objetivos de aprendizaje

- Evaluar los requisitos del negocio y diseñar arquitecturas de red seguras para entornos híbridos.
- Diseñar topologías, enrutamiento y conectividad híbrida con VPN, SD-WAN, MPLS y enlaces a nubes públicas.
- Garantizar la disponibilidad con balanceo de carga, redundancia, autoescalado y CDN.
- Aplicar principios de Zero Trust (ZTNA, SASE, microsegmentación, CASB) y endurecer redes híbridas.
- Implementar soluciones de IAM con SSO, MFA, PKI y gestión de accesos privilegiados.
- Usar herramientas de monitoreo, métricas y alertas para mantener operaciones confiables.
- Automatizar la red con infraestructura como código y scripting en entornos híbridos.
- Diagnosticar y resolver fallas de conectividad, rendimiento y seguridad en redes híbridas.

Áreas de habilidad

Diseño de redes | Enrutamiento y NAT | Spine-and-leaf | SD-WAN y MPLS | Conectividad a la nube | Alta disponibilidad | Zero Trust | SASE y CASB | IAM y PAM | Monitoreo | Infraestructura como código | Troubleshooting avanzado

Programa del curso

Duración: 5 días

Modalidades de formación

- **Presencial** — En aula, con instructor
- **Online** — En vivo, con instructor
- **Híbrida** — Aula y online combinadas

Módulo	Contenido
Dominio 1 Día 1	**1.0 Diseño de arquitectura de red (31 %)** Direccionamiento IP, protocolos de enrutamiento, NAT y protocolos de red; arquitecturas en malla, estrella y spine-and-leaf; conectividad híbrida con VPN, SD-WAN, MPLS y enlaces a nubes públicas; disponibilidad con balanceo de carga, redundancia, autoescalado y CDN; instalaciones de campus.
Dominio 2 Día 2	**2.0 Seguridad de redes (28 %)** Amenazas, vulnerabilidades y mitigaciones; firewalls, protocolos de cifrado y NAC; reglas de firewall, grupos de seguridad y filtrado de URL; Zero Trust: ZTNA, SASE, microsegmentación y CASB; IAM con SSO, MFA, PKI y accesos privilegiados; seguridad inalámbrica.
Dominio 3 Día 3	**3.0 Operaciones, monitoreo y rendimiento de la red (16 %)** Gestión de operaciones: riesgo, continuidad y optimización del servicio; herramientas de monitoreo: métricas, dashboards, registros y alertas; automatización con infraestructura como código (IaC), herramientas y scripting en entornos híbridos.
Dominio 4 Día 4	**4.0 Solución de problemas de red (25 %)** Conectividad: DNS, VPN e interconexión con la nube; rendimiento: latencia, balanceo de carga y pérdida de paquetes; seguridad: fallas de firewall, accesos no autorizados y vulnerabilidades en entornos híbridos.
Integración **Caso práctico** Día 5	✔ **Caso integrador de diseño de red híbrida** Diseño, aseguramiento y validación de una arquitectura híbrida de extremo a extremo, aplicando los cuatro dominios del examen. ✔ **Repaso integral y preparación para el examen** Repaso por dominio, práctica con preguntas basadas en desempeño (PBQ) y simulacro cronometrado del examen CNX-001.

El contenido sigue los 4 dominios oficiales del examen CompTIA CloudNetX CNX-001 (V1); el porcentaje indica el peso de cada dominio en el examen. El quinto día integra los dominios en un caso práctico.

Examen y certificación

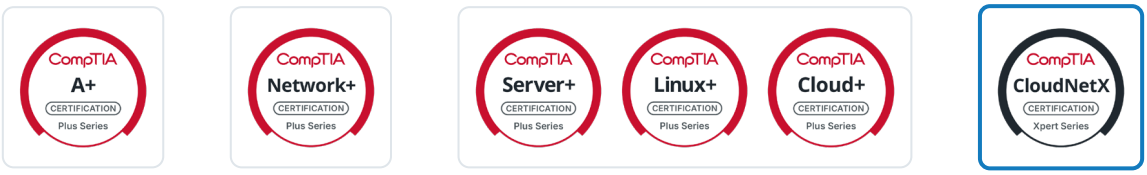
Título	CompTIA CloudNetX – Versión 1
Código	CNX-001
Preguntas	Máximo 90
Formato	Opción múltiple y preguntas basadas en desempeño
Duración	165 minutos
Aprobación	Aprobado / reprobado (sin puntaje escalado)
Idioma	Inglés
Plataforma	Pearson VUE (centro de pruebas o en línea con OnVUE)

Requisitos de elegibilidad

- No hay requisitos obligatorios. CompTIA recomienda al menos 10 años de experiencia en TI, incluidos 5 como arquitecto de redes en entornos de nube híbrida.
- Se recomiendan conocimientos equivalentes a CompTIA Network+, Security+ y Cloud+.
- La versión vigente (V1) se lanzó el 18 de febrero de 2025.

Ruta profesional CompTIA

CloudNetX es la certificación de nivel experto (Xpert Series) de la ruta de infraestructura de CompTIA: culmina el camino que comienza con A+ y Network+ y continúa con Server+, Linux+ y Cloud+.



Información general

- Material oficial de CompTIA, con laboratorios prácticos y preguntas de práctica.
- Instructor certificado y Savant Consultores como CompTIA Authorized Partner.
- Certificación acreditada por ANAB bajo la norma ISO/IEC 17024.
- Vigencia de 3 años, renovable mediante el programa de Educación Continua (CE) de CompTIA.

CompTIA Authorized Partner | ACADEMIC PARTNER

CompTIA CloudNetX CERTIFICATION Xpert Series