Designing and Implementing Cisco Service Provider Cloud Network Infrastructure v1.0 (300-540)

Exam Description: Designing and Implementing Cisco Service Provider Cloud Network Infrastructure v1.0 (SPCNI 300-540) is a 90-minute exam associated with the CCNP Service Provider. This exam certifies a candidate's knowledge of designing and implementing virtualized architecture, cloud interconnect, high availability, security, and service assurance and optimization.

The following topics are general guidelines for the content likely to be included on the exam. However, other related topics may also appear on any specific delivery of the exam. To better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

25% 1.0 Virtualized Architecture

- 1.1 Describe IaaS constraints such as VLAN scale and segmentation
- 1.2 Determine the cloud service model (such as IaaS, PaaS, SaaS, and FaaS) for private, public, or hybrid deployments
- 1.3 Describe container orchestration and virtual machines
- 1.4 Implement virtualization functions
  - 1.4.a NFV
  - 1.4.b VNF
  - 1.4.c NSO
  - 1.4.d Virtualized Cisco platforms
- 1.5 Deploy NFV using automation and orchestration
  - 1.5.a Onboarding VNF
  - 1.5.b NFV orchestration using NSO
  - 1.5.c NETCONF, RESTCONF, and REST APIs
  - 1.5.d Yang models and gNMI/gRPC
  - 1.5.e OpenStack

25% 2.0 Cloud Interconnect

- 2.1 Describe carrier-neutral facilities
  - 2.1.a Connectivity options to cloud providers
  - 2.1.b Connectivity options to other carrier-neutral facilities or customer locations
  - 2.1.c Cloud edge facilities and interconnections
- 2.2 Evaluate WAN infrastructure connectivity
  - 2.2.a Direct connect
  - 2.2.b MPLS/segment routing
  - 2.2.c IPsec VPN

2.3 Troubleshoot DCI solutions
- 2.3.a EVPN VXLAN
- 2.3.b EVPN over SR/MPLS
- 2.3.c ACI
- 2.3.d Pseudowires

20% 3.0 High Availability

3.1 Implement technologies for high availability
- 3.1.a VNF data plane redundancy using placement and network resiliency
- 3.1.b Control plane high availability within single VIM
- 3.1.c Data plane high availability (compute, vNIC, and TOR)

3.2 Implement multi-homing

3.3 Implement EVLAG

3.4 Implement a virtual private cloud

3.5 Implement ECMP from NFVI to physical infrastructure such as BGP multi-path, OSPF, and IS-IS

3.6 Recommend design models for high availability such as DNS, routing, and load balancers

15% 4.0 Security

4.1 Implement infrastructure security
- 4.1.a ACL
- 4.1.b uRPF
- 4.1.c RTBH and router hardening
- 4.1.d BGP flowspec
- 4.1.e TACACS
- 4.1.f MACSEC

4.2 Describe DoS mitigation techniques

4.3 Describe NFVI security
- 4.3.a API security
- 4.3.b Secure NFVI control and management plane
- 4.3.c Network segmentation in service provider cloud environment
- 4.3.d TLS and mTLS

4.4 Describe cloud security solutions such as DNS security, zero-day exploit, and virus detectors

15% 5.0 Service Assurance and Optimization

5.1 Describe network assurance
- 5.1.a NFVI MANO

- 5.1.b VNF workloads
- 5.1.c VIM control plane KPIs
- 5.1.d Streaming telemetry with gRPC and gNMI

5.2 Describe cloud infrastructure and performance monitoring
- 5.2.a SR-PM
- 5.2.b NetFlow and IPFIX
- 5.2.c Logging with syslog
- 5.2.d SNMP traps and RMON
- 5.2.e Cloud agents
- 5.2.f Automatic fault management

5.3 Diagnose NFVI errors and events

5.4 Describe VNF optimization
- 5.4.a SR-IOV
- 5.4.b Software accelerated virtual switch (DPDK and VPP)