Implementing and Operating Cisco Data Center Core Technologies v1.0 (350-601)

Exam Description: Implementing and Operating Cisco Data Center Core Technologies v1.0 (DCCOR 350-601) is a 120-minute exam associated with the CCNP and CCIE Data Center Certifications. This exam tests a candidate's knowledge of implementing core data center technologies including network, compute, storage network, automation, and security. The course, Implementing Cisco Data Center Core Technologies, helps candidates to prepare for this exam.

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 Network

1.1 Apply routing protocols
- 1.1.a OSPFv2, OSPFv3
- 1.1.b MP-BGP
- 1.1.c PIM
- 1.1.d FHRP

1.2 Apply switching protocols such as RSTP+, LACP and vPC

1.3 Apply overlay protocols such as VXLAN EVPN and OTV

1.4 Apply ACI concepts
- 1.4.a Fabric setup
- 1.4.b Access policies
- 1.4.c VMM
- 1.4.d Tenant policies

1.5 Analyze packet flow (unicast, multicast, and broadcast)

1.6 Analyze Cloud service and deployment models (NIST 800-145)

1.7 Describe software updates and their impacts
- 1.7.a Disruptive / nondisruptive
- 1.7.b EPLD
- 1.7.c Patches

1.8 Implement network configuration management

1.9 Implement infrastructure monitoring such as NetFlow and SPAN

1.10 Explain network assurance concepts such as streaming telemetry

25% 2.0 Compute

- 2.1 Implement Cisco Unified Compute System Rack Servers
- 2.2 Implement Cisco Unified Compute System Blade Chassis
  - 2.2.a Initial setup
  - 2.2.b Infrastructure management
  - 2.2.c Network management (VLANs, pools and policies, templates, QoS)
  - 2.2.d Storage management (SAN connectivity, Fibre Channel zoning, VSANs, WWN pools, SAN policies, templates)
  - 2.2.e Server management (Server pools and boot policies)
- 2.3 Explain HyperFlex Infrastructure Concepts and benefits (Edge and Hybrid Architecture vs all-flash)
- 2.4 Describe firmware and software updates and their impacts on B-Series and C-Series servers
- 2.5 Implement compute configuration management (Backup and restore)
- 2.6 Implement infrastructure monitoring such as SPAN and Intersight

20% 3.0 Storage Network

- 3.1 Implement Fibre Channel
  - 3.1.a Switch fabric initialization
  - 3.1.b Port channels
  - 3.1.c FCID
  - 3.1.d CFS
  - 3.1.e Zoning
  - 3.1.f FCNS
  - 3.1.g Device alias
  - 3.1.h NPV and NPIV
  - 3.1.i VSAN
- 3.2 Implement FCoE Unified Fabric (FIP and DCB)
- 3.3 Describe NFS and NAS concepts
- 3.4 Describe software updates and their impacts (Disruptive/nondisruptive and EPLD)
- 3.5 Implement infrastructure monitoring

15% 4.0 Automation

- 4.1 Implement automation and scripting tools
  - 4.1.a EEM
  - 4.1.b Scheduler

4.1.c Bash Shell and Guest Shell for NX-OS
4.1.d REST API
4.1.e JSON and XML encodings

4.2 Evaluate automation and orchestration technologies
4.2.a Ansible
4.2.b Puppet
4.2.c Python
4.2.d POAP
4.2.e DCNM
4.2.f UCSD
4.2.g PowerShell

15% 5.0 Security

5.1 Apply network security
5.1.a AAA and RBAC
5.1.b ACI contracts and microsegmentation
5.1.c First-hop security features such as dynamic ARP inspection (DAI), DHCP snooping, and port security
5.1.d CoPP

5.2 Apply compute security
5.2.a AAA and RBAC
5.2.b Keychain authentication

5.3 Apply storage security
5.3.a AAA and RBAC
5.3.b Port security
5.3.c Fabric binding