

ADVANCED VCF NETWORKING TASKS · EXAM 3V0-25.25

Work task 1 to task 195 and you have designed, built, broken and fixed an NSX fabric

Exam 3V0-25.25, Advanced VMware Cloud Foundation Networking. This is the only advanced VCF exam that tests design, build and troubleshooting together: its twenty-two objectives sit in sections 3, 4 and 5 of the blueprint. Sections A to E are written design work, F to P are performed, Q to U are faults you create and then diagnose. The code at the right of each task is the objective it practises.

Dr Pranay Jha · drpranayjha.com

A. NSX ARCHITECTURE AND COMPONENTS

Written tasks. Get the vocabulary right before you build anything with it.

- | | | |
|-----|--|-----|
| 1. | Draw the NSX management, control and data planes and name what lives in each. | 3.2 |
| 2. | Write what the NSX Manager cluster does, how many nodes it has, and what a virtual IP buys you. | 3.2 |
| 3. | Write the difference between a host transport node and an edge transport node, and what each can do alone. | 3.2 |
| 4. | Write what a transport zone is, the two types, and what a node joining one gains. | 3.2 |
| 5. | Explain the tunnel endpoint: what it is, where it lives, and what rides over it. | 3.2 |
| 6. | Draw the path of an east-west packet between two virtual machines on different hosts, same segment. | 3.2 |
| 7. | Draw the same for different segments, and show where the distributed router does its work. | 3.2 |
| 8. | Write what the distributed firewall is attached to, and why that placement matters. | 3.2 |
| 9. | List the NSX components a VCF deployment creates for you, and which ones you still create by hand. | 3.2 |
| 10. | Write the version and interoperability checks you would run before any NSX change in a VCF fleet. | 3.2 |

B. CENTRALIZED AGAINST DISTRIBUTED CONNECTIVITY

Objective 3.3 in one phrase. Most design questions in this exam resolve here.

- | | | |
|-----|---|-----|
| 11. | Write which NSX functions are distributed across hosts and which are centralised on edges. | 3.3 |
| 12. | Write the test you apply to decide: if the function needs to see every packet of a flow, it is centralised. | 3.3 |
| 13. | Given a design with only east-west traffic between segments, state whether an edge cluster is needed and justify it. | 3.3 |
| 14. | Given a design needing NAT and a gateway firewall, state what that forces and why. | 3.3 |
| 15. | Draw a topology where traffic is hairpinned to an edge unnecessarily, then redraw it without the hairpin. | 3.3 |
| 16. | Write the throughput consequence of centralising a service, and where the ceiling comes from. | 3.3 |
| 17. | Design a connectivity solution for three tenants that must not route to each other, and justify centralised or distributed for each decision. | 3.3 |
| 18. | Write when you would put a service on the Tier-0 and when on the Tier-1, with the reason for each. | 3.3 |

C. MULTISITE DESIGN

Objective 3.4. Know the options before you are asked to choose between them.

- | | | |
|-----|--|-----|
| 19. | Write the multisite options available in NSX and what problem each one solves. | 3.4 |
| 20. | Write the difference between a stretched design and a Federation design, in one sentence each. | 3.4 |
| 21. | Write what Federation gives you that two independent NSX instances do not. | 3.4 |

- | | | |
|-----|---|-----|
| 22. | Record the latency and bandwidth requirements between sites, and which link each applies to. | 3.4 |
| 23. | Design a two-site solution for disaster recovery, and say what is stretched and what is rebuilt. | 3.4 |
| 24. | Design a two-site solution for active-active workloads, and say what changes from the recovery design. | 3.4 |
| 25. | Write what happens to each design when the inter-site link fails, step by step. | 3.4 |
| 26. | Write the failure domain of each option: what one failure can take out. | 3.4 |
| 27. | Write which multisite option you would choose for a data residency requirement, and why the others fail it. | 3.4 |

D. NSX FLEET DESIGN CONSIDERATIONS

Objective 3.5. Designing NSX across a VCF fleet rather than a single instance.

- | | | |
|-----|--|-----|
| 28. | Write what a fleet means for NSX: how many instances, and what is shared between them. | 3.5 |
| 29. | Write the decision of one NSX instance per workload domain against one shared across several. | 3.5 |
| 30. | Write what drives the NSX Manager sizing, and the sizes available. | 3.5 |
| 31. | Write how NSX lifecycle works in a VCF fleet, and what upgrades it alongside. | 3.5 |
| 32. | Write the identity and certificate design across a fleet of NSX instances. | 3.5 |
| 33. | Write the backup design for a fleet: how many targets, how often, and the restore order. | 3.5 |
| 34. | Write the object count drivers, and which design model grows objects fastest. | 3.5 |
| 35. | Design the fleet networking for an estate that will double in two years, and say what you did to leave room. | 3.5 |

E. OPTIMISATION AND ACCELERATION

Objective 3.6. Where performance comes from, and what it costs.

- | | | |
|-----|--|-----|
| 36. | Write what Enhanced Data Path is, note that it is the default host switch mode in VCF 9, and record what each mode requires of the host and the NIC. | 3.6 |
| 37. | Write the trade-off between EDP interrupt mode and poll mode: what you gain and what you give up. | 3.6 |
| 38. | Write where NIC offloads help NSX traffic, and which offloads matter for overlay. | 3.6 |
| 39. | Write the MTU design across the fabric and what breaks when one hop is wrong. | 3.6 |
| 40. | Write the edge node form factor decision, virtual against bare metal, with the throughput reason. | 3.6 |
| 41. | Write how you would scale north-south throughput without replacing hardware. | 3.6 |
| 42. | Given a latency-sensitive workload, make three design decisions to protect it and justify each. | 3.6 |
| 43. | Write what you would measure to prove an optimisation worked, before and after. | 3.6 |

F. EDGE CLUSTERS

Build section starts here. Everything from F onward is performed where you can.

- | | | |
|-----|---|-----|
| 44. | Record the process to deploy an NSX Edge cluster, including form factors and the networking each needs. | 4.3 |
| 45. | Deploy two edge transport nodes and confirm their tunnels to the host transport nodes come up. | 4.3 |
| 46. | Form an edge cluster from those nodes and check its status. | 4.3 |
| 47. | Write what the edge cluster is required for that host transport nodes cannot provide. | 4.3 |
| 48. | Record the uplink design for the edges: how many, to which VLANs, and with what teaming. | 4.3 |
| 49. | Add a third edge node to an existing cluster and record what rebalances and what does not. | 4.3 |
| 50. | Put an edge node into maintenance mode and watch where its services move. | 4.3 |
| 51. | Record the sizing of your edge nodes and the throughput that size is rated for. | 4.3 |

G. TIER-0 GATEWAYS

The north-south boundary, and the mode decision that shapes everything above it.

- | | | |
|-----|---|-----|
| 52. | Create a Tier-0 gateway in active-active mode with Stateful left off, and record what that rules out. | 4.4 |
| 53. | Create a Tier-0 in active-active with Stateful enabled, and confirm you can configure stateful NAT on it. | 4.4 |
| 54. | Create a Tier-0 in active-standby and configure a stateful service, and record which node is active. | 4.4 |
| 55. | Write the three modes side by side with what each allows, because the old rule that active-active is always stateless is out of date. | 4.4 |
| 56. | Record the scale-out rule for stateful active-active: add edge nodes in even numbers so each has a backup. | 4.4 |
| 57. | Create the uplink interfaces, one per edge node, and confirm the gateway is up on each. | 4.4 |
| 58. | Configure BGP to two upstream routers and bring both sessions to established. | 4.4 |
| 59. | Configure route redistribution and prove a segment prefix reaches the upstream router. | 4.4 |
| 60. | Create a VRF on the Tier-0 and record what it inherits from the parent and what it does not. | 4.4 |
| 61. | Attach two tenants to two VRFs and prove their routing tables stay separate. | 4.4 |
| 62. | Record that the high availability mode is fixed at creation, and what that means for your design. | 4.4 |

H. TIER-1 GATEWAYS AND SEGMENTS

The tenant-facing layer.

- | | | |
|-----|---|-----|
| 63. | Create a Tier-1 gateway and link it to the Tier-0. | 4.6 |
| 64. | Assign an edge cluster to the Tier-1 and record when that is required and when it is not. | 4.6 |
| 65. | Enable route advertisement and confirm the Tier-0 learns the routes. | 4.6 |

- | | | |
|-----|--|-----|
| 66. | Create an overlay logical segment on the Tier-1 and give it a gateway address. | 4.5 |
| 67. | Attach a virtual machine and test reachability in three steps: gateway, another host, outside. | 4.5 |
| 68. | Create a VLAN-backed segment and write when you would use one instead of overlay. | 4.5 |
| 69. | Create a segment with no gateway attached and record what it is useful for. | 4.5 |
| 70. | Move a Tier-1 between edge clusters with a continuous ping running, and record the loss. | 4.6 |
| 71. | Delete a segment that still has a workload attached, and record what stops you. | 4.5 |

I. STATEFUL SERVICES

Objective 4.8, and one of only two Section 4 objectives this exam does not share with the Administrator exam.

- | | | |
|-----|---|-----|
| 72. | List the stateful services NSX offers and where each can run. | 4.8 |
| 73. | Configure source NAT on a Tier-1 so a segment leaves with a predictable address, and verify at the far end. | 4.8 |
| 74. | Configure destination NAT to publish one internal service, and restrict it by port. | 4.8 |
| 75. | Write when NAT is the right answer and when a load balancer is. | 4.8 |
| 76. | Configure a gateway firewall rule and prove it is enforced at the gateway, not at the vNIC. | 4.8 |
| 77. | Configure DHCP with a local server on the Tier-1 and confirm a lease. | 4.8 |
| 78. | Configure a DHCP relay to an external server and verify the request arrives with the right relay address. | 4.8 |
| 79. | Configure a VPN and record what it requires of the edge cluster. | 4.8 |
| 80. | Record what every stateful service has in common: it needs an edge cluster and a single owner of the flow. | 4.8 |
| 81. | Record which stateful services you may run on a Tier-0 in each high availability mode. | 4.8 |

J. VIRTUAL PRIVATE CLOUDS

Self-service networking, and a large part of what is new in VCF 9.

- | | | |
|-----|--|-----|
| 82. | Create an NSX Project to hold the VPCs. | 4.7 |
| 83. | Create a VPC connectivity profile and record what it controls. | 4.7 |
| 84. | Create a VPC inside the project and list the objects NSX created underneath it. | 4.7 |
| 85. | Create a private subnet and a public subnet, and record where each address range came from. | 4.7 |
| 86. | Attach a workload to each subnet and test what can reach what. | 4.7 |
| 87. | Publish a workload from a private subnet externally, and trace every hop. | 4.7 |
| 88. | Configure a distributed firewall rule inside the VPC and prove it follows the workload across hosts. | 4.7 |
| 89. | Configure a Transit Gateway and record what it connects. | 4.7 |
| 90. | Record what a tenant can do in a VPC without ever contacting the network team. | 4.7 |
| 91. | Delete a VPC and record what is cleaned up and what is left behind. | 4.7 |

K. PROJECTS AND TENANCY

Objective 4.9, shared word for word with the Administrator exam.

- | | | |
|-----|---|-----|
| 92. | Create a Project and assign a quota to it. | 4.9 |
| 93. | Map a tenant group to the project with the appropriate role. | 4.9 |
| 94. | Create objects inside the project and confirm a tenant administrator sees only their own. | 4.9 |
| 95. | Confirm a provider administrator sees every project from above. | 4.9 |
| 96. | Record which objects stay shared across projects, because that is where the boundary actually sits. | 4.9 |
| 97. | Exhaust a project quota and record the error the tenant receives. | 4.9 |
| 98. | Write the difference between a Project and a VPC in one sentence each. | 4.9 |

L. NSX FEDERATION

Objective 4.1. Know the process before you are asked to order its steps.

- | | | |
|------|--|-----|
| 99. | Write the Federation deployment order: Global Manager, standby Global Manager, then register each Local Manager. | 4.1 |
| 100. | Write what the Global Manager owns and what stays with the Local Manager. | 4.1 |
| 101. | Configure remote tunnel endpoints on the edge nodes and record why they are needed. | 4.1 |
| 102. | Create a stretched segment from the Global Manager and confirm it appears at both sites. | 4.1 |
| 103. | Create a local object on a Local Manager and confirm the Global Manager does not manage it. | 4.1 |
| 104. | Record the one-way nature of importing local objects into the Global Manager. | 4.1 |
| 105. | Write the span of an object and what choosing one site against both actually changes. | 4.1 |
| 106. | Record what a stretched Tier-0 in active-active mode cannot do, and why. | 4.1 |
| 107. | Fail one site and record what the Global Manager still lets you do. | 4.1 |

M. CONFIGURING NSX COMPONENTS

Objective 4.2, the broadest in the blueprint. Work through the surface methodically.

- | | | |
|------|--|-----|
| 108. | Prepare a cluster of hosts as transport nodes and verify each one individually. | 4.2 |
| 109. | Create an uplink profile and record what it sets: teaming, MTU, transport VLAN. | 4.2 |
| 110. | Create an IP pool for tunnel endpoints and record what happens when it is exhausted. | 4.2 |
| 111. | Create a transport zone and add nodes to it. | 4.2 |
| 112. | Configure a security group with dynamic membership based on tags. | 4.2 |
| 113. | Create a distributed firewall policy with rules, and set the default posture deliberately. | 4.2 |
| 114. | Configure an IP discovery profile and record what fails without one. | 4.2 |
| 115. | Configure a segment security profile and record what each protection prevents. | 4.2 |
| 116. | Configure a QoS profile and apply it to a segment. | 4.2 |
| 117. | Change an uplink profile on a live transport node and record the impact. | 4.2 |
| 118. | Record which of these configurations VCF created for you and which you created by hand. | 4.2 |

N. ADVANCED INTEGRATIONS

Objective 4.10, shared with the Administrator exam.

- | | | |
|------|--|------|
| 119. | Integrate NSX with VCF Operations for Networks and confirm topology appears. | 4.10 |
| 120. | Integrate NSX with an external identity source and sign in as a mapped group member. | 4.10 |
| 121. | Integrate NSX with a load balancer such as Avi, and record what each product then owns. | 4.10 |
| 122. | Record how NSX integrates with the Supervisor, and which objects appear per namespace. | 4.10 |
| 123. | Record what the Antrea integration gives you for container workloads. | 4.10 |
| 124. | Configure an automation or API integration and make one change through it rather than the interface. | 4.10 |
| 125. | Record what each integration costs: another credential, another certificate, another upgrade dependency. | 4.10 |

O. OPERATIONAL TASKS

Objective 4.11, shared with the Administrator exam. Day 2 for the network.

- | | | |
|------|---|------|
| 126. | Configure a Manager backup to an SFTP target, with a passphrase stored separately. | 4.11 |
| 127. | Run a backup on demand and confirm the files land on the target. | 4.11 |
| 128. | Restore a Manager from backup in a lab and record the restore order. | 4.11 |
| 129. | Configure syslog export from NSX Manager and prove a line arrives at the collector. | 4.11 |
| 130. | Take a support bundle and open it, so you know what you are sending. | 4.11 |
| 131. | Check Manager cluster health and the status of every transport node. | 4.11 |
| 132. | Replace an NSX certificate and list everything that must be re-registered afterwards. | 4.11 |
| 133. | Record the upgrade order for NSX within a VCF domain and who drives it. | 4.11 |
| 134. | Record what a configuration backup does not contain, so you know the limits of a restore. | 4.11 |

P. MONITORING NSX

Objective 4.12. Knowing which product answers which question.

- | | | |
|------|--|------|
| 135. | List the VCF products that can monitor an NSX implementation, and what each one is best at. | 4.12 |
| 136. | Given a question about flow between two workloads, say which product answers it. | 4.12 |
| 137. | Given a question about Manager health over time, say which product answers it. | 4.12 |
| 138. | Given a question about who changed a firewall rule, say which product answers it. | 4.12 |
| 139. | Build an alert on an NSX condition and trigger it deliberately. | 4.12 |
| 140. | Build a dashboard showing NSX health for an operator, and say what it deliberately leaves out. | 4.12 |
| 141. | Record the data each product collects and how long it keeps it. | 4.12 |

Q. CHOOSING THE RIGHT TROUBLESHOOTING TOOL

Section 5 starts here, and it is the part the other VCF exams do not test at all.

- | | | |
|------|---|-----|
| 142. | List the NSX troubleshooting tools available and the question each one answers. | 5.1 |
| 143. | Given a dropped packet between two virtual machines, name the tool you reach for first and why. | 5.1 |
| 144. | Given a route that is not being learned, name the tool and the specific view. | 5.1 |
| 145. | Given a tunnel that will not come up, name the tool and the first thing you check. | 5.1 |
| 146. | Use Traceflow between two workloads and read every hop it reports. | 5.1 |
| 147. | Use a path trace in VCF Operations for Networks and compare it with the Traceflow result. | 5.1 |
| 148. | Record what the command line gives you that the interface does not, and when you need it. | 5.1 |
| 149. | Write the order you would use the tools in, from cheapest to most invasive. | 5.1 |

R. INFRASTRUCTURE FAULTS

Create each fault yourself before you diagnose it. A fault you built is a fault you understand.

- | | | |
|------|---|-----|
| 150. | Break the MTU on one hop and diagnose the result from the symptoms alone. | 5.2 |
| 151. | Break the transport VLAN on one host and watch which tunnels drop. | 5.2 |
| 152. | Exhaust the tunnel endpoint IP pool and diagnose a host that will not prepare. | 5.2 |
| 153. | Stop one NSX Manager node and record what still works and what does not. | 5.2 |
| 154. | Let a certificate expire in a lab and record the symptom it produces. | 5.2 |
| 155. | Break time synchronisation on a transport node and record what fails. | 5.2 |
| 156. | Put an edge node in a state where its tunnels are down, and work out why from the status alone. | 5.2 |
| 157. | Record the first four checks you would run on any NSX infrastructure problem, in order. | 5.2 |

S. CONNECTIVITY AND ROUTING FAULTS

The largest troubleshooting objective, and the one closest to real incidents.

- | | | |
|------|--|-----|
| 158. | Create a distributed firewall rule that drops traffic, then find it with Traceflow. | 5.3 |
| 159. | Create a gateway firewall rule that drops traffic, and note how the symptom differs. | 5.3 |
| 160. | Break a BGP session deliberately with a wrong autonomous system number, and diagnose from the session state. | 5.3 |
| 161. | Remove route redistribution and diagnose why a prefix stopped being advertised. | 5.3 |
| 162. | Misconfigure a NAT rule so return traffic fails, and work out why from one direction working. | 5.3 |
| 163. | Attach a workload to the wrong segment and diagnose it from the address it receives. | 5.3 |
| 164. | Create an asymmetric path through two edges and record what breaks when a stateful service is involved. | 5.3 |
| 165. | Break DHCP and separate a relay problem from a scope problem from a segment problem. | 5.3 |
| 166. | Diagnose a workload that reaches other workloads but not the outside world, and list the possible causes in order. | 5.3 |

167. Write the one question that most quickly narrows any connectivity fault: how far does it get. 5.3

T. ECMP AND HIGH AVAILABILITY

Objective 5.4. A describe objective, so make sure you can describe it precisely.

168. Write what Equal Cost Multi-Path is and the problem it solves. 5.4
169. Write what ECMP requires: the mode, the number of uplinks, and what the upstream must do. 5.4
170. Configure ECMP on a Tier-0 and confirm traffic uses more than one path. 5.4
171. Write how a flow is pinned to a path, and why that matters for stateful services. 5.4
172. Write the high availability model for each Tier-0 mode and what failover looks like in each. 5.4
173. Fail one edge node and measure how long traffic takes to recover. 5.4
174. Write the difference between ECMP for throughput and high availability for resilience, since they are often confused. 5.4
175. Record the maximum number of ECMP paths and what sets it. 5.4

U. LOGICAL ROUTING PACKET WALK

Objective 5.5. Be able to narrate this out loud, hop by hop.

176. Walk a packet between two virtual machines on the same segment, same host. 5.5
177. Walk a packet between two virtual machines on the same segment, different hosts. 5.5
178. Walk a packet between two segments on the same Tier-1, same host. 5.5
179. Walk a packet between two segments on the same Tier-1, different hosts, and show where the distributed router acts. 5.5
180. Walk a packet from a workload to the outside world, through Tier-1 and Tier-0 to the uplink. 5.5
181. Walk the return packet and show where NAT, if present, reverses. 5.5
182. Walk a packet between two Tier-1 gateways under the same Tier-0. 5.5
183. Walk a packet across a Federation stretched segment between two sites. 5.5
184. For each walk, mark where the distributed firewall is evaluated. 5.5
185. Narrate the north-south walk out loud in under two minutes, with no notes. 5.5

V. AGAINST THE CLOCK

Do this section twice in the final week, from a clean start, timing yourself.

186. Deploy an edge cluster, a Tier-0 with BGP, a Tier-1 and a segment, and get a workload talking to the outside. 45 minutes. 4.3
187. Create a Project, a VPC, two subnets, and publish one workload externally. 30 minutes. 4.7
188. Configure SNAT, DNAT, a gateway firewall rule and DHCP on one Tier-1. 25 minutes. 4.8
189. Write the Federation deployment order and object span rules from memory. 10 minutes. 4.1
190. Create three faults for a colleague, swap, and diagnose theirs. 30 minutes. 5.2
191. Diagnose a broken BGP session and a dropped flow, start to finish. 20 minutes. 5.3

- | | | |
|-------------|--|------|
| 192. | Narrate the full north-south packet walk, then the Federation one. 10 minutes. | 5.5 |
| 193. | Write the centralised against distributed decision table from memory. 10 minutes. | 3.3 |
| 194. | Design a two-site solution from a one-page brief and justify every decision. 35 minutes. | 3.4 |
| 195. | Configure a Manager backup, run it, and write the restore order from memory. 15 minutes. | 4.11 |