PassQueen
a.k.a dumpsqueen.com

Data CenterSpecialist (JNCIS-DC)

Juniper JN0-481

Version Demo

Total Demo Questions: 8

Total Premium Questions: 84

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Data Center Architecture	5
Topic 2, Data Center Switching	11
Topic 3, Data Center Routing	13
Topic 4, Data Center Security	4
Topic 5, Data Center Automation and Orchestration	51
Total	84

QUESTION NO: 1

Within Managed Devices in the Juniper Apstra UI, you notice that several devices have the OOS-Quarantined status. The devices cannot be added to any blueprint. Which action would solve this problem?

A. Acknowledge the device.

B. Fix the hardware issues with the quarantined devices.

C. Install the agent, even though connectivity is established.

D. Upload a new pristine configuration.

ANSWER: A

Explanation:

Acknowledge the device. is the required action because an *OOS-Quarantined* managed device is intentionally held outside normal blueprint use until an operator explicitly acknowledges its state. Quarantine is a safeguard in Apstra's device-management workflow: it prevents a device that Apstra has identified as requiring administrative attention from being consumed by a blueprint prematurely. Acknowledging the device confirms that the administrator has reviewed the condition and accepts returning it to the managed-device workflow. After acknowledgement, the device can transition out of the quarantined state as appropriate and become eligible for blueprint assignment.

This action is performed from the Managed Devices view, where Apstra exposes lifecycle and operational actions for discovered and managed switches. The purpose is not to alter the intended fabric design; it is to clear the administrative quarantine gate that blocks blueprint inclusion. Once the device is acknowledged and its managed status is restored, it can be selected during blueprint creation or assigned to an existing blueprint according to the normal Apstra workflow. See the Juniper Apstra User Guide for managed-device operations and the Juniper Technical Documentation portal for the release-specific Apstra documentation.

QUESTION NO: 2

In an EVPN-VXLAN fabric, leaf1 learns a locally attached server MAC address and IP address and advertises the information to remote VTEPs. Which two statements are correct about the EVPN route used for this purpose? (Choose two.)

A. It advertises a learned endpoint MAC address.

B. It can advertise an associated endpoint IP address.

C. It advertises VTEP membership for BUM replication.

D. It advertises only IP prefixes without MAC reachability.

ANSWER: A B

Explanation:

A **Type 2 MAC/IP Advertisement route** distributes a learned endpoint MAC address and can also carry the associated IP address. Remote VTEPs use the advertising VTEP information to direct known unicast traffic to the leaf where that endpoint is attached.

A Type 3 route advertises VTEP membership for BUM replication, not individual endpoint reachability. A Type 5 route is used to advertise IP prefixes and is not the route used to advertise a specific endpoint MAC address.

QUESTION NO: 3

You are onboarding a supported third-party switch that cannot run an Apstra on-box device agent. The Apstra controller has Layer 3 management reachability to the switch. Which agent model should be used?

A. An on-box agent

B. An off-box agent

C. A configuration deviation agent

D. A worker-node agent

ANSWER: B

Explanation:

An **off-box agent** is correct because it runs outside the managed device and communicates with the device through its reachable management interface. This model supports devices that cannot host the Apstra device-agent software directly.

An on-box agent requires agent processes to run on the managed device. A worker node can provide capacity to host off-box-agent workloads, but it is not itself the agent model selected for the switch.

QUESTION NO: 4

Which two statements are correct about a Juniper Apstra server? (Choose two.)

A. The Juniper Apstra server uses Layer 2 to communicate with managed devices.

B. The Juniper Apstra server requires one network adapter connection for each managed device.

C. The Juniper Apstra server uses Layer 3 to communicate with managed devices.

D. The Juniper Apstra server requires a single network adapter.

ANSWER: C D

Explanation:

The statements “The Juniper Apstra server uses Layer 3 to communicate with managed devices” and “The Juniper Apstra server requires a single network adapter” correctly describe the basic Apstra controller connectivity model. Apstra operates as an IP-based controller: its server or controller cluster must be able to reach the management addresses of the switches and other managed infrastructure. This communication supports device discovery, configuration deployment, telemetry collection, and operational-state retrieval. Consequently, the controller does not depend on being directly adjacent at Layer 2 to every managed device; routable management-network connectivity is the relevant requirement.

A single server network adapter can provide this management reachability when it is connected to a management network with appropriate routing to the fabric devices. The adapter is not dedicated per switch. This design lets an Apstra deployment manage a growing number of devices without requiring a corresponding increase in physical network interfaces on the Apstra server. Administrators should still ensure that the management network, addressing, routes, firewall policy, and credentials allow the controller and managed devices to communicate reliably. Juniper’s installation guidance describes the server networking prerequisites and controller deployment model in the Apstra Server Installation documentation; additional platform requirements are provided in the Apstra system requirements documentation.

QUESTION NO: 5

You have accessed your deployed blueprint and see the banner shown in the exhibit.



Which two statements are correct in this scenario? (Choose two.)

A. Devices must be assigned to profiles.

B. There are changes that are not active on the fabric.

C. Resources must be assigned to devices.

D. There are anomalies that must be addressed.

ANSWER: B D

Explanation:

The deployed-blueprint banner presents status indicators for the blueprint's intent and operational state. An Uncommitted status means that modifications have been staged in the blueprint but have not been committed. Until the commit operation is completed and the resulting configuration is deployed, those intent changes are not active on the fabric. Therefore, "There are changes that are not active on the fabric." accurately describes the indicated state.

The Active status indicator also communicates the health state of the deployed blueprint. An alert condition in this area means Apstra has detected active operational issues through its assurance and anomaly monitoring. Such findings require investigation and remediation to return the fabric to its expected healthy and compliant state. Therefore, "There are anomalies that must be addressed." is also correct.

These two conditions can exist at the same time: an operator may have pending, uncommitted design changes while Apstra is also reporting anomalies in the currently active fabric. The status banner distinguishes pending intent from the health of the running deployment, enabling operators to determine both whether work remains to be committed and whether active issues need attention. See Juniper's documentation on uncommitted changes and active anomalies.

QUESTION NO: 6

You are designing an EVPN-VXLAN fabric that uses symmetric IRB for communication between virtual networks in the same routing zone. Which two statements are correct? (Choose two.)

A. The ingress VTEP routes traffic into the tenant VRF before VXLAN encapsulation.

B. The routed overlay traffic uses a Layer 3 VNI.

C. Every VTEP must locally bridge every virtual network in the routing zone.

D. The spine devices must decapsulate VXLAN traffic before forwarding it.

E. Traffic is routed only after it arrives at the egress VTEP.

ANSWER: A B

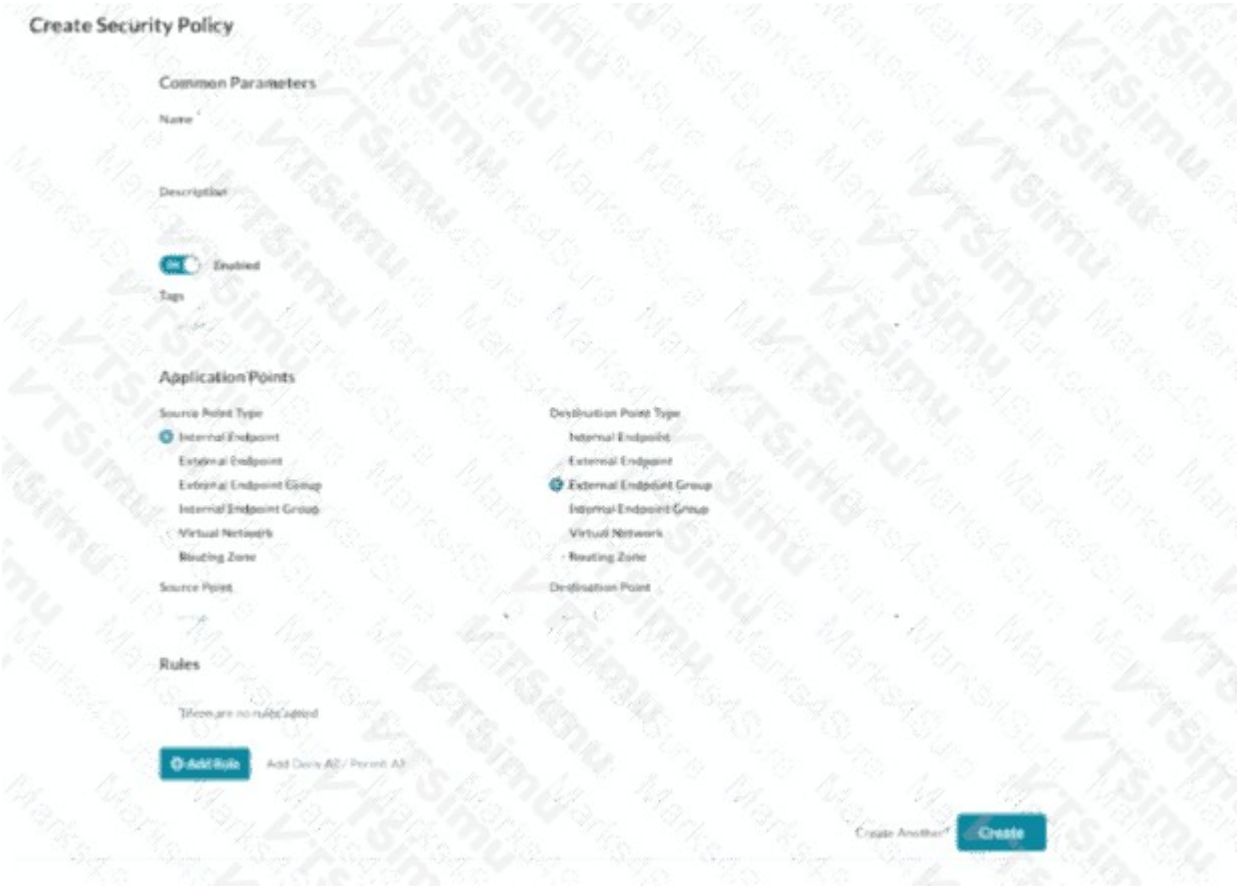
Explanation:

With **symmetric IRB**, the ingress VTEP routes traffic from the source virtual network into the tenant VRF and encapsulates the packet toward the egress VTEP using the Layer 3 VNI. The egress VTEP then forwards the packet into the destination virtual network. This model allows the tenant routing context to be carried across the VXLAN overlay.

A symmetric IRB design uses a Layer 3 VNI for routed tenant traffic and does not require every VTEP to bridge every destination VLAN locally. By contrast, asymmetric IRB requires a VTEP that routes traffic to have local knowledge of both the source and destination bridge domains.

QUESTION NO: 7

You are creating a new security policy using Juniper Apstra.



Referring to the exhibit, which application point should you select to allow or deny traffic to or from a particular VRF?

A. Routing Zone

B. External Endpoint

C. Internal Endpoint

D. Virtual Network

ANSWER: A

Explanation:

Routing Zone is the correct application point because Apstra uses a routing zone as the intent-model abstraction for a VRF. A routing zone defines an isolated Layer 3 routing domain and corresponds to the VRF context implemented on the fabric devices. Consequently, a policy whose scope is traffic entering, leaving, or otherwise associated with a particular VRF must be attached to that routing-zone boundary. This allows Apstra to interpret the policy in the context of that tenant or routing domain and render the required device-level enforcement consistently across the relevant fabric elements.

Using the routing-zone application point is especially appropriate when the VRF contains multiple virtual networks. The policy can then govern the VRF as a whole rather than being limited to one individual Layer 2/Layer 3 segment. Apstra's security-policy workflow uses these application points to express intent according to the required scope, with routing zones providing the VRF-level scope needed here. Juniper's Apstra documentation describes routing zones and virtual networks as core logical constructs in the reference design and policy model. See the Juniper Apstra 5.1 User Guide and the Apstra 5.1 documentation landing page.

QUESTION NO: 8

You have a virtual network that needs controlled access to other virtual networks in the same routing zone. Using the Juniper Apstra UI. which feature would be used to accomplish this task?

A. interface policy

B. anti-affinity policy

C. routing policy

D. security policy

ANSWER: D

Explanation:

security policy is the Apstra feature used to control communication between virtual networks that belong to the same routing zone. In Apstra, routing zones provide the routing context that allows virtual networks to exchange traffic. A security policy adds the required segmentation and access-control layer by defining which flows are permitted between endpoints or virtual networks within that routing context. Policy rules can match traffic using attributes such as source and destination, protocol, and port, allowing an operator to implement controlled application access rather than unrestricted east-west connectivity.

This policy-based approach is especially useful in a data center fabric where multiple tenant, application, or workload networks must share a routing domain but require explicit authorization for communication. The policy is modeled centrally in the Apstra UI and then rendered into the relevant fabric configuration, which supports consistent enforcement and operational intent across the blueprint. Consequently, security policy is the appropriate mechanism when the requirement is to permit, restrict, and govern traffic between virtual networks in one routing zone.

Juniper's Apstra documentation provides the product documentation and configuration concepts for virtual networks, routing zones, and policy-driven fabric operations: Apstra User Guide and Juniper Technical Documentation.