Juniper

JN0-480 Exam

Data Center Specialist
Questions & Answers
Demo

Version: 4.0

Question: 1

Which statement is true when onboarding a Juniper Networks device using a Juniper Apstra ZTP server?

A. The Device Key lo be used can be set In the dhcpd.conf file on the ZTP server.
B. The State can be set In the ztp.Json file on the ZTP server.
C. The Management IP address cannot be predetermined.
D. The Hostname will be the serial-number of the device.

Answer: B

Explanation:

The ztp.Json file on the Apstra ZTP server contains the configuration parameters for each device that is onboarded using ZTP. One of the parameters is the State, which can be one of the following values: init, ready, in_progress, done, error, or disabled. The State indicates the current status of the device in the ZTP process. For example, if the State is ready, it means that the device is ready to be onboarded by the Apstra ZTP server. If the State is done, it means that the device has completed the ZTP process and is managed by the Apstra server. The State can be manually set or changed in the ztp.Json file to control the behavior of the device during ZTP. For more information, see Apstra ZTP Configuration File. Reference:
Apstra ZTP Configuration File
Apstra ZTP Introduction
Configure Apstra ZTP

Question: 2

You have designed your fabric in Juniper Apstra prior to deploying the network devices.
Which Apstra element in the Staged tab would be used to assist the team that is installing and cabling the devices?

A. Connectivity Templates
B. Virtual Networks table
C. Managed Devices list
D. Links table

Answer: D

Explanation:

The Links table in the Staged tab shows the physical connections between the devices in the fabric. It provides information such as the source and destination device names, hostnames, serial numbers, roles, interfaces, and link status. The Links table can be used to assist the team that is installing and cabling the devices by verifying that the devices are connected correctly and that the links are operational. The Links table can also be used to troubleshoot any connectivity issues that may arise during the installation process. For more information, see Links (Staged). Reference:
Links (Staged)
Topology (Staged)
Staged

Question: 3

When editing a device configuration to install some manual changes, which procedure should be followed?

A. Edit the configuration on the device directly by the CLI; the changes will automatically be adjusted in the Juniper Apstra configuration
B. Edit the pristine configuration of the device.
C. Add a persistent change to a device configuration with a configlet.
D. Delete the device from the Juniper Apstra system, change the configuration, then re-import the device.

Answer: C

Explanation:

A configlet is a small piece of configuration that can be applied to a device or a group of devices to make persistent changes that are not overwritten by Apstra. Configlets can be used to install manual changes that are not part of the Apstra rendered configuration, such as custom commands, scripts, or features. Configlets can be created, edited, and deleted from the Apstra GUI or CLI12. Reference:
Configlets Overview
Configlets User Guide

Question: 4

In Juniper Apstr
a. which statement is correct?
A. VMware anomaly detection is on by default.
B. VMware anomaly detection requires a vCenter server configured under External Systems
C. VMware anomaly detection requires a VMware hypervisor with exports enabled.
D. VMware anomaly detection requires an Apstra server running on VMware.

Answer: B

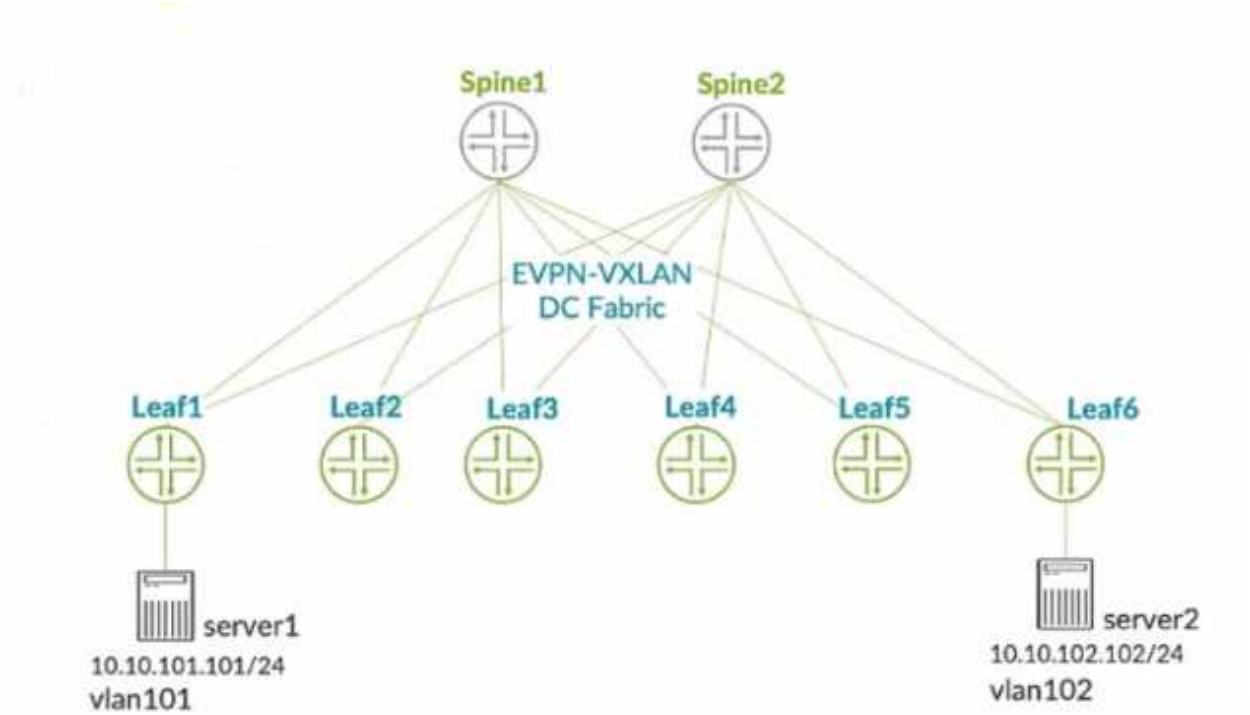
Explanation:

VMware anomaly detection is a feature of Apstra that provides visibility and validation of the virtual network settings and the physical network settings in a VMware vSphere environment. To enable this feature, Apstra requires a connection to a vCenter server that manages the ESX/ESXi hosts and the

VMs connected to the Apstra-managed leaf switches. The vCenter server must be configured under External Systems in the Apstra web interface, and the vCenter integration must be staged and committed in the blueprint. This allows Apstra to collect information about VMs, ESX/ESXi hosts, port groups, and VDS, and to flag any inconsistencies or mismatches that might affect VM connectivity.
The other options are incorrect because:
VMware anomaly detection is not on by default. It must be enabled by configuring a vCenter server under External Systems and adding a virtual infra to the blueprint.
VMware anomaly detection does not require a VMware hypervisor with exports enabled. It only requires LLDP transmit to be enabled on the VMware distributed virtual switch to associate host interfaces with leaf interfaces.
VMware anomaly detection does not require an Apstra server running on VMware. It can run on any supported platform, such as Linux, Windows, or Docker. Reference:
VMware vCenter/vSphere Virtual Infra
Anomalies (Service)
A Better Experience: VMware + Juniper Apstra

Question: 5

Exhibit.



You connect two single-homed servers using Juniper Apstra as shown in the exhibit. You are using the ERB design blueprint with two virtual networks in a common routing zone.
In this scenario, which two types of VXLAN tunnels will be automatically created by the EVPN control plane? (Choose two.)

A. EVPN signaled route Type-8 VXLAN tunnels
B. EVPN signaled route Type-3 VXLAN tunnels
C. EVPN signaled route Type-6 VXLAN tunnels
D. EVPN signaled route Type-2 VXLAN tunnels

Answer: BD

Explanation:

According to the Juniper documentation1, EVPN route Type-3 is used to advertise the IP address of the VTEP and the VNIs that it supports. This allows the VTEPs to discover each other and form VXLAN tunnels for the VNIs that they have in common. EVPN route Type-2 is used to advertise the MAC and IP addresses of the hosts connected to the VTEPs. This allows the VTEPs to learn the MAC-to-IP bindings and the MAC-to-VTEP mappings for the hosts in the same VNI. Therefore, these two types of VXLAN tunnels will be automatically created by the EVPN control plane when using Juniper Apstra with the ERB design blueprint and two virtual networks in a common routing zone. Reference: Example: Configure an EVPN-VXLAN Centrally-Routed Bridging Fabric