PassQueen
a.k.a dumpsqueen.com

Versa Certified SD-WAN Specialist (VNX300)

Versa Networks VNX301

Version Demo

Total Demo Questions: 7

Total Premium Questions: 79

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

You have deployed a group of devices in Versa Director, and the field technicians have performed the onboarding tasks onsite. One of the devices has not finished the onboarding process and does not appear in the **Appliances** list in Versa Director. The onboarding VPN tunnel from the device to the Controller is up. Which two actions would help you solve this problem? **(Choose two.)**

A. View the Tasks list in Versa Director to see whether an error was encountered during the onboarding process.

B. Use the Monitor dashboard in Versa Director to view the status of the missing device.

C. Review the Unknown Devices dashboard in the **Administration > Inventory** menu.

D. Verify that the device is listed in the **Connectors > Local > Resource Pool** dashboard.

ANSWER: A C

Explanation:

Viewing the Tasks list in Versa Director is appropriate because onboarding and deployment operations are tracked as Director tasks. Once the onboarding VPN tunnel is established, connectivity between the branch device and the Controller has progressed far enough that the remaining failure may be associated with a Director-driven workflow, such as device association, staging configuration delivery, template processing, or a configuration commit. Task details and logs provide the operational result and error context needed to identify where that workflow stopped.

Reviewing the Unknown Devices dashboard under Administration > Inventory is also appropriate. A device can establish its initial onboarding connection while still failing to become a fully recognized appliance in Director. The inventory view is intended to help administrators identify devices that have contacted the infrastructure but have not yet been claimed, matched, or incorporated into the expected managed-device workflow. Reviewing that record helps validate device identity and continue the onboarding process. These actions align with Versa Director's operational role in inventory, workflow execution, and lifecycle management of SD-WAN appliances. See the Versa Networks Documentation portal and the Versa SD-WAN product overview for Versa platform and management information.

QUESTION NO: 2

You are configuring the BGP routing protocol between a Versa Secure SD-WAN CPE with AS number 64514 and two upstream service providers: SP1 with AS number 64515 and SP2 with AS number 64519. You want to prefer BGP routes learned from AS 64515 over routes learned from AS 64519. Which BGP path attribute would be used to accomplish this task?

A. The BGP MULTI_EXIT_DISC path attribute

B. The BGP ORIGIN path attribute

C. The BGP LOCAL_PREF path attribute

D. The BGP NEXT_HOP path attribute

ANSWER: C

Explanation:

The BGP LOCAL_PREF path attribute is the appropriate mechanism because it controls the preferred outbound path for BGP destinations within the local autonomous system. The Versa CPE can apply an inbound BGP routing policy to routes received from AS 64515 and assign those routes a higher LOCAL_PREF value than equivalent routes received from AS 64519. During BGP best-path selection, a route with the higher local preference is selected, provided that the compared routes are otherwise eligible. This lets the organization express a clear provider preference for traffic leaving AS 64514 while retaining the alternate provider as a usable path. LOCAL_PREF is propagated to internal BGP peers within the autonomous system, allowing the same egress preference to be consistently applied throughout the local routing domain. In Versa

Secure SD-WAN deployments, route policies are the normal configuration construct for matching received routes and setting BGP attributes such as local preference. The BGP specification defines LOCAL_PREF as an attribute used to inform other internal BGP speakers of the degree of preference for an advertised route. See RFC 4271, section 5.1.5 and the Versa Networks documentation portal for Versa routing-policy configuration guidance.

QUESTION NO: 3

A branch device is powered on with factory-default staging configuration. The device establishes an IKE session to the staging server and receives an IP address, but it does not proceed to establish an IKE session with the Versa Controller. Which staging phase is failing?

A. Stage 1

B. Stage 2

C. Stage 3

D. Post-activation template commit

ANSWER: B

Explanation:

Stage 2 is the failing phase. The successful IKE connection to the staging server and receipt of an IP address demonstrate that the branch has completed the initial bootstrap interaction using its factory-default staging configuration. During the next phase, Versa Director supplies the stage-two configuration through the staging infrastructure. This configuration changes the branch's IPsec/IKE peer from the staging server to the Versa Controller and provides the information required for the branch to restart or re-establish connectivity toward that controller.

Because the device has already reached the staging server but does not advance to an IKE session with the Versa Controller, the failure occurs at the handoff represented by Stage 2. Operationally, investigation should focus on delivery and application of the stage-two configuration, the configured Controller address and reachability, IKE/IPsec parameters, and any firewall or NAT behavior affecting the branch-to-Controller path. Establishing the Controller IKE session is the expected outcome of the Stage 2 transition and is prerequisite to subsequent activation and operational configuration. Versa documentation and training resources are available through the Versa Documentation portal and the Versa Networks website.

QUESTION NO: 4

A service provider creates one reusable device template for many branches. WAN interface address, gateway, and VLAN values differ at each location, but the remaining branch design must remain standardized. Which two statements are true? **(Choose two.)**

A. Template variables can represent the WAN values that differ for each branch.

B. Device Bind Data can supply the branch-specific values for those variables.

C. A separate device template is required for every distinct WAN VLAN ID.

D. The Controller automatically replaces WAN VLAN IDs after IPsec connectivity is established.

ANSWER: A B

Explanation:

Template variables allow the shared device template to contain site-specific fields without changing the common configuration design. Device Bind Data supplies the individual values that are substituted for those variables when Versa Director generates configuration for each appliance.

A separate device template is not required solely because WAN values differ by site. The Controller does not rewrite VLAN identifiers after tunnel establishment; those values are generated from the template and associated bind data during deployment.

QUESTION NO: 5

You are asked to deploy a Versa Secure SD-WAN branch for 1000 locations. You need to profile the branches based on common deployment requirements.

In this scenario, which three configuration objects would be shared by multiple appliances? (Choose three.)

A. device templates

B. device groups

C. workflow device

D. service templates

E. device bind data

ANSWER: A B D

Explanation:

Device templates, device groups, and service templates are reusable configuration objects intended to standardize deployments across many Versa Secure SD-WAN appliances. A device template supplies the common post-staging appliance configuration, allowing a consistent baseline to be defined once and applied to every branch with the same design profile. This is essential when deploying a large estate because shared configuration can be maintained centrally rather than recreated for each location.

Device groups provide the scalable organizational layer for appliances that have common requirements. They enable branches with the same deployment profile to be associated with the appropriate shared configuration and operational policy scope. For example, branches with the same WAN design, security posture, or service needs can be grouped for consistent management.

Service templates define reusable service-level behavior that can be attached across applicable appliances. Such behavior commonly includes SD-WAN policy, traffic steering, QoS, application handling, and security-related service configuration. Combining common appliance settings in device templates, logical population management in device groups, and common service definitions in service templates supports repeatable, centrally governed onboarding at scale. Versa's product documentation and training resources describe this template-driven operational model: Versa Documentation and Versa Secure SD-WAN.

QUESTION NO: 6

A branch uses a template variable for the WAN VLAN ID. During deployment, Branch-A receives VLAN 100 and Branch-B receives VLAN 200 from device bind data while using the same template. Which statement is correct?

A. This is expected because template variables allow unique per-device values.

B. This is impossible because all devices using a template must share identical VLAN IDs.

C. The device template must be duplicated for each branch.

D. The Controller automatically rewrites VLAN IDs after IPsec comes up.

ANSWER: A

Explanation:

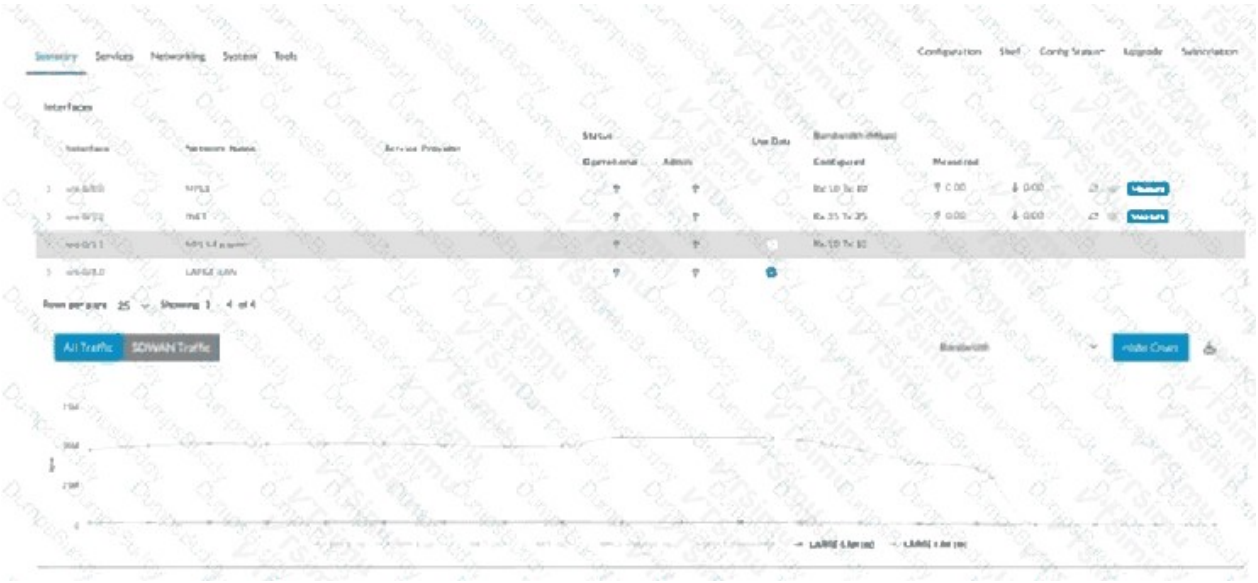
This is expected because template variables allow unique per-device values. Versa Director and Versa Orchestrator use a template-based provisioning model in which a shared device template defines the common configuration for multiple appliances, while device-specific bind data supplies the values that differ at each site. A VLAN identifier is an appropriate site-specific value: the template can contain a variable at the WAN interface VLAN field, and the value assigned during device binding is substituted when the configuration is generated for that particular appliance. Consequently, one branch can receive VLAN 100 and another can receive VLAN 200 without changing the shared template or affecting its reusable routing, interface, service, and SD-WAN design. This separation is central to scalable deployments because administrators can maintain common policy and configuration logic once, then onboard sites with their individual circuit and addressing details. The resulting configuration delivered to each device contains the bound VLAN value as part of its intended interface configuration. Versa describes its centralized orchestration and template-driven SD-WAN operations at Versa Orchestrator; additional product and documentation resources are available through the Versa Documentation portal.

QUESTION NO: 7

Examine the exhibit below.

As an administrator of a Versa Secure SD-WAN, you are asked to find the current bandwidth of each WAN circuit used for SD-WAN connectivity in a branch, but the Director is not displaying any information for the WAN circuits.

In this scenario, what should be done to get the graph populated for all WAN circuits?



A. Refresh the page to get the graphs populated in the dashboard.

B. Select live data for all WAN circuits in the dashboard.

C. Select live data for MPLS circuits alone.

D. Unselect live data for INET circuit and select again. group

ANSWER: B

Explanation:

Select live data for all WAN circuits in the dashboard. The requirement is to view the *current* bandwidth for every WAN circuit at the branch, which requires Versa Director to retrieve and display real-time interface statistics for each relevant WAN interface. The Live Data control determines the interfaces for which Director presents live operational information, including traffic-rate data used by the bandwidth graph. Enabling it consistently across all WAN circuits ensures that each circuit contributes data to the displayed graph rather than leaving some links without live measurements.

Live monitoring is particularly useful when an administrator needs an immediate operational view of link utilization for troubleshooting, verification, or capacity assessment. Versa Director provides the management interface for monitoring Versa Operating System devices, while Versa Analytics complements the platform with collected and analyzed operational data. For this scenario, selecting live data on every WAN circuit aligns the monitoring scope with the requested outcome: a

populated graph covering all branch WAN connections. Versa documentation resources are available through the Versa Documentation portal, and Versa's SD-WAN platform overview describes centralized visibility and operations capabilities at Versa Secure SD-WAN.