PassQueen
a.k.a dumpsqueen.com

VMware SD-WAN Design and Deploy Skills

VMware 5V0-42.21

Version Demo

Total Demo Questions: 7

Total Premium Questions: 75

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, VMware SD-WAN Architecture and Components	30
Topic 2, VMware SD-WAN Design	22
Topic 3, VMware SD-WAN Deployment	20
Topic 4, VMware SD-WAN Troubleshooting	3
Total	75

QUESTION NO: 1

Which three authentication mode options ate valid for use on the VMware SD-WAN Edge? (Choose three.)

A. Certificate Enabled

B. Certificate Optional

C. Certificate Disabled

D. Certificate Activated

E. Certificate Accepted

F. Certificate Required

ANSWER: B C F

Explanation:

VMware SD-WAN Edge supports three certificate-authentication modes: **Certificate Disabled**, **Certificate Optional**, and **Certificate Required**. Certificate Disabled is used when certificate-based Edge authentication is not enforced. Certificate Optional enables the Edge to use a certificate when one is available while preserving compatibility during migrations or mixed deployment scenarios. Certificate Required enforces certificate-based authentication, ensuring that an Edge must present a valid certificate to authenticate and connect to the SD-WAN environment. These modes allow administrators to align Edge onboarding and authentication controls with the organization's security requirements and deployment stage. In particular, optional mode can support a controlled transition toward certificate enforcement, while required mode provides the strongest certificate-authentication posture once certificate issuance and lifecycle processes are fully established. VMware's SD-WAN documentation describes Edge configuration and security behavior in the VMware SD-WAN documentation; VMware's product overview also discusses SD-WAN security and centralized policy capabilities at VMware SD-WAN.

QUESTION NO: 2

A customer is using hypervisor to install VMware Partner Gateways.

Which two hypervisors may be used? (Choose two.)

A. Hyper-V

B. Kubermetes

C. XenServer

D. KVM

E. ESXi

ANSWER: A D

Explanation:

VMware SD-WAN Partner Gateways can be deployed as virtual gateway appliances on supported virtualization platforms, including Hyper-V and KVM. Hyper-V provides the Microsoft virtualization environment in which the Partner Gateway virtual-machine image can be instantiated and connected to the required management, WAN, and LAN-facing networks. KVM is likewise supported for deploying the virtual gateway image on Linux-based virtualization infrastructure. In both cases, the deployment must satisfy the applicable VMware SD-WAN Gateway sizing, networking, routing, public-IP, and interface requirements so that the gateway can register with VMware SD-WAN Orchestrator and provide service to assigned edges. These deployment choices enable a service provider or partner to host gateways in infrastructure that aligns with its existing compute platform while retaining VMware SD-WAN gateway functionality. VMware's SD-WAN documentation organizes gateway configuration and Partner Gateway deployment guidance under its Gateway administration material; consult the current release documentation because supported versions and image formats can vary by release. See the VMware SD-WAN documentation portal and the VMware SD-WAN documentation library.

QUESTION NO: 3

A customer requires all branch Internet-bound traffic to be inspected by a security appliance located at the data center. Local Internet breakout must not be used for this traffic.

Which Network Service should be configured in the Business Policy?

A. Direct

B. Backhaul

C. Multi-Path

D. CoS Mapping

ANSWER: B

Explanation:

Backhaul is the appropriate Network Service because it directs matching branch traffic through the SD-WAN overlay to a hub or data-center location before the traffic reaches its destination. In this scenario, the branch Internet-bound traffic can be sent to the data-center security appliance for centralized inspection and egress.

Backhaul is commonly used when an organization requires traffic to traverse centralized security services, private data-center services, or a controlled Internet egress point. The Business Policy identifies the relevant application or destination traffic and applies the backhaul service so that the Edge does not use direct local Internet access for those flows. See the VMware SD-WAN documentation portal for Business Policy and Network Service configuration guidance.

QUESTION NO: 4

Which port is used for the high availability connection between the two Edges on a pair of Edge 510s?

A. Any port may be chosen.

B. GE1

C. SFP1

D. GE4

ANSWER: B

Explanation:

GE1 is the dedicated high-availability interface on a VMware SD-WAN Edge 510. When deploying two Edge 510 appliances as an HA pair, GE1 on one appliance is directly connected to GE1 on the peer appliance. This physical link carries the HA communication needed for peer status monitoring, configuration synchronization, and failover coordination between the active and standby Edges. Because the HA interface is hardware-model-specific, the designated port must be used rather than selecting an arbitrary available data interface. Correctly cabling GE1 to GE1 is therefore an essential part of the physical installation of an Edge 510 HA topology, before validating HA state in VMware SD-WAN Orchestrator. VMware's installation documentation describes hardware interfaces and HA deployment requirements for supported Edge platforms; see the VMware SD-WAN Installation and Upgrade Guide and the VMware SD-WAN documentation portal.

QUESTION NO: 5

A customer uses an MPLS circuit and an Internet circuit at a branch. The design requires a Business Policy that remains portable even when branches use different carriers and different physical WAN interfaces.

Which VMware SD-WAN object should be used to abstract the underlying WAN links in the policy?

A. Transport Group

B. Configuration Profile

C. Application Map

D. Gateway Role

ANSWER: A

Explanation:

Transport Group is correct because it provides a logical grouping of WAN links that can be referenced by Business Policy. The administrator can place links with a common business purpose into a Transport Group and then use that group for link-steering decisions instead of referencing individual physical interfaces or specific carriers.

This approach makes the policy more portable across sites with different access technologies and interface layouts. For example, a policy can prefer a transport group representing private WAN connectivity while allowing a different set of physical MPLS or broadband links at individual branches. See the VMware SD-WAN documentation portal for transport and Business Policy configuration guidance.

QUESTION NO: 6

Which statement is correct about VMware SD-WAN Orchestrator user roles and their associate privileges?

A. Customer Support User can view and manage then company's network

B. Standard Admin User can view but cannot manage their customer.

C. Superuser: User can view but cannot create additional admin.

D. Enterprise read only: User can view but not modify configurations.

ANSWER: D

Explanation:

Enterprise read only: User can view but not modify configurations. This accurately describes the VMware SD-WAN Orchestrator Enterprise Read Only role. The role is intended for personnel who need visibility into an enterprise's SD-WAN environment without being permitted to make operational or configuration changes. For example, a read-only user can inspect enterprise-level information, view network configuration and monitoring data, and review the status of deployed SD-WAN components. This supports common operational requirements such as audit access, reporting, troubleshooting observation, and stakeholder visibility while preserving configuration control for authorized administrators.

VMware SD-WAN Orchestrator uses role-based access control to limit actions according to the user's assigned role. Assigning Enterprise Read Only access follows the principle of least privilege: users receive the access needed to observe the environment but do not receive permissions to alter configurations, modify policies, or perform administrative changes. This separation helps protect the production SD-WAN deployment from unintended changes while allowing appropriate teams to review relevant enterprise data. See the VMware SD-WAN documentation portal at VMware SD-WAN Documentation and the Broadcom technical documentation portal at Broadcom TechDocs.

QUESTION NO: 7

An enterprise is implementing role-based access control for VMware SD-WAN Orchestrator users.

Which three practices support the principle of least privilege? (Choose three.)

A. Assign read-only access to users who only require monitoring visibility

B. Limit administrative roles to authorized operators

C. Use enterprise-scoped access where appropriate

D. Assign Superuser access to all NOC personnel

E. Share one administrator account among all operators

ANSWER: A B C

Explanation:

Assigning read-only access to users who only require monitoring visibility, **limiting administrative roles to authorized operators**, and **using enterprise-scoped access where appropriate** support least privilege. VMware SD-WAN Orchestrator roles determine what users can view and modify, allowing organizations to grant only the access required for a user's operational responsibilities.

Read-only users can review configuration and monitoring information without making changes. Administrative privileges should be limited to trusted personnel responsible for configuration and lifecycle tasks. Enterprise-scoped access prevents a user from receiving unnecessary access to other customer or enterprise environments. See the VMware SD-WAN documentation portal for user-management and role information.