VMware NSX-T Data Center 3.1 Security

VMware 5V0-41.21

Version Demo

Total Demo Questions: 9

Total Premium Questions: 91

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, VMware Products and Solutions	40
Topic 2, Planning and Designing	1
Topic 3, Installing, Configuring, and Setup	34
Topic 4, Performance-tuning, Optimization, and Upgrades	1
Topic 5, Troubleshooting and Repairing	6
Topic 6, Administrative and Operational Tasks	9
Total	91

QUESTION NO: 1

There has been a confirmed case of virus infection on multiple VMs managed by Endpoint Protection. A security administrator wants to create a group to quarantine infected VMs in the future.

What criteria will be used to build this group?

A. NSX Tags

B. Segment

C. vSphere Tags

D. VM Name

ANSWER: A

Explanation:

NSX Tags is the appropriate criterion for building a dynamic quarantine group in this Endpoint Protection scenario. NSX-T integrates with supported endpoint-protection solutions through Guest Introspection and the Endpoint Protection framework. When the endpoint-protection solution detects an infection, it can communicate the VM's security state to NSX-T and associate an NSX security tag with the affected workload. An administrator can then define a group whose membership criterion matches that NSX tag, such as an infection- or quarantine-related tag supplied by the endpoint-protection solution.

This approach makes the quarantine workflow dynamic and repeatable. Any VM subsequently identified as infected receives the relevant NSX tag and is automatically included in the quarantine group. Security policy can then use that group as its source or destination, applying restrictive distributed firewall rules to isolate the affected workload while maintaining a consistent operational process. The group is therefore driven by the security context published to NSX-T rather than by a manually maintained list of virtual machines.

VMware documents NSX-T's Endpoint Protection and Guest Introspection capabilities in the NSX-T Data Center 3.1 Administration Guide and describes security groups and tag-based membership in the NSX-T Data Center Security documentation.

QUESTION NO: 2

What is one of the main use-cases of NSX-T Endpoint Protection?

A. Use Network Security Services of a third party vendor

B. Agentless Antivirus

C. East-West Firewalling

D. North-South Firewalling

ANSWER: B

Explanation:

Agentless Antivirus is a primary use case for NSX-T Data Center Endpoint Protection. The feature uses NSX Guest Introspection and the vSphere Endpoint/Guest Introspection framework to enable a supported third-party security solution to inspect and protect workloads without installing a full antivirus scanning agent inside every protected virtual machine. Instead, a lightweight guest component communicates with an external security virtual appliance, which performs the intensive inspection and malware-scanning work.

This architecture reduces the CPU, memory, storage, and operational overhead that can result when each virtual machine runs an independent antivirus engine. It also helps avoid simultaneous scan activity across many desktops or servers, commonly called an antivirus storm, because scanning can be centralized and coordinated by the security partner appliance. NSX-T provides the virtualization-aware integration and policy enforcement capabilities, while the partner solution supplies the antimalware intelligence, scanning engine, signatures, and remediation workflow. This makes agentless antivirus

especially useful in dense virtualized environments where consistent workload protection and efficient resource usage are required.

VMware describes Guest Introspection as the mechanism that enables partner security services for guest virtual machines in the NSX documentation. See the NSX-T Data Center Guest Introspection documentation and the NSX Guest Introspection administration guide.

QUESTION NO: 3

An organization is using VMware Identity Manager (vIDM) to authenticate NSX-T Data Center users Which two selections are prerequisites before configuring the service? (Choose two.)

A. Validate vIDM functionality

B. Assign a role to users

C. Time Synchronization

D. Configure vIDM Integration

E. Certificate Thumbprint from vIDM

ANSWER: C E

Explanation:

Time Synchronization is required because NSX-T Data Center and VMware Identity Manager rely on time-sensitive TLS and token-based authentication operations. Their clocks must be synchronized, normally through a common NTP source, before the integration is configured. This prevents authentication failures caused by invalid or apparently expired certificates and tokens.

Certificate Thumbprint from vIDM is also required to establish trusted TLS communication with the VMware Identity Manager service. During the NSX-T Data Center configuration, the administrator supplies the VMware Identity Manager appliance details and validates its server certificate using the certificate thumbprint. Obtaining and confirming that thumbprint in advance ensures NSX Manager can securely verify the identity of the vIDM endpoint rather than trusting an unverified server.

These are setup prerequisites for connecting NSX-T Data Center to an already deployed VMware Identity Manager environment. VMware documents the requirement to synchronize time and to provide the VMware Identity Manager certificate thumbprint as part of configuring the integration. See the VMware NSX-T Data Center administration documentation and the NSX-T 3.1 Identity Manager integration guidance.

QUESTION NO: 4

Which are two use-cases for the NSX Distributed Firewall' (Choose two.)

A. Zero-Trust with segmentation

B. Security Analytics

C. Lateral Movement of Attacks prevention

D. Software defined networking

E. Network Visualization

ANSWER: A C

Explanation:

Zero-Trust with segmentation and **Lateral Movement of Attacks prevention** are core use cases for the NSX Distributed Firewall. The distributed firewall is enforced directly at the virtual NIC of protected workloads, allowing security policy to be applied close to each application rather than only at a centralized network perimeter. This supports a zero-trust model by enabling granular, least-privilege controls between workloads, application tiers, and environments. Policies can use workload context such as groups, tags, and identity-related attributes, which makes micro-segmentation practical even when workloads move or their IP addresses change.

The same workload-level enforcement is designed to limit lateral movement after an initial compromise. By allowing only explicitly required east-west communications, such as the approved flows between web, application, and database tiers, the distributed firewall reduces an attacker's ability to reach additional systems within the data center. NSX Distributed Firewall rules can be applied consistently across hosts and workloads, helping contain a threat to a smaller security segment while maintaining required application connectivity. VMware describes distributed firewall capabilities and workload-level policy enforcement in its NSX Distributed Firewall documentation and discusses micro-segmentation and zero-trust architecture in the NSX Security Reference Architecture.

QUESTION NO: 5

An administrator needs to create a Distributed Firewall policy that is evaluated before policies in the Infrastructure, Environment, and Application categories.

Which category should be used?

A. Emergency

B. Infrastructure

C. Environment

D. Application

ANSWER: A

Explanation:

The Emergency category has the highest precedence among the user-configurable Distributed Firewall policy categories. Rules in this category are evaluated before Infrastructure, Environment, and Application category rules. It is intended for urgent, broadly applicable security controls that must take priority over normal application policy.

Policy category selection affects evaluation order and should be planned carefully to avoid unintentionally overriding required connectivity. VMware documents Distributed Firewall policy categories and ordering in the NSX-T Data Center Firewall Administration documentation.

QUESTION NO: 6

What type of IDS/IPS system deployment allows an administrator to block a known attack?

A. A system deployed in SPAN port mode.

B. A system deployed inline with ALERT and DROP action.

C. A system deployed inline with ALERT action.

D. A system deployed in TERM mode.

ANSWER: B

Explanation:

A system deployed inline with ALERT and DROP action allows an administrator to block a known attack because inline IDS/IPS inspects traffic while it is traversing the protected network path and can enforce a prevention decision before the traffic reaches its destination. NSX-T IDS/IPS signatures identify traffic patterns associated with known threats. When a

signature is matched, the ALERT action records the event and makes it visible for monitoring and investigation, while the DROP action actively discards the matching packets. Using both actions therefore provides operational visibility into the detection and the enforcement capability required to stop the identified attack. This is the essential distinction of an intrusion-prevention deployment: the inspection engine is placed directly in the traffic flow and is configured with a blocking action. In NSX-T Data Center, IDS/IPS profiles and rules define the signatures and actions that are applied to protected workloads, enabling administrators to use signature-based detection together with packet dropping for prevention. VMware's NSX-T documentation describes IDS/IPS configuration, profiles, and rule actions in the NSX-T Data Center 3.1 Administration Guide. Additional product documentation is available through the VMware NSX technical documentation portal.

QUESTION NO: 7

Which two traffic types are supported by NSX Service Insertion? (Choose two.)

A. East-West traffic

B. North-South traffic

C. vMotion traffic

D. NSX Manager management traffic

E. ESXi host storage traffic

ANSWER: A B

Explanation:

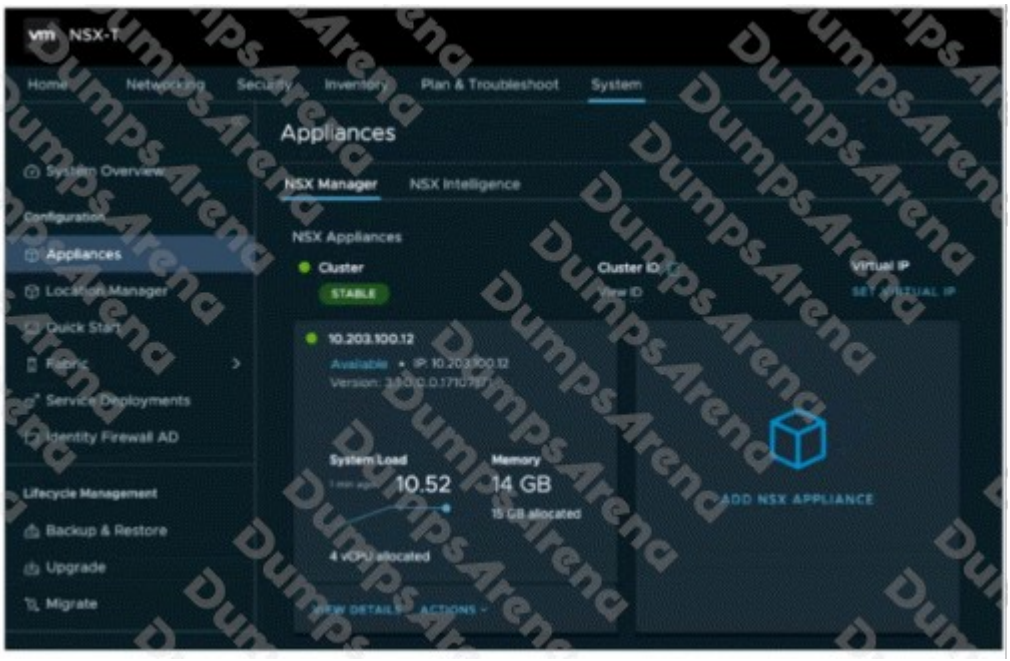
East-West traffic is supported by NSX Service Insertion. Traffic exchanged between internal workloads can be redirected to a registered partner service for inspection and enforcement close to the virtual machine interface.

North-South traffic is also supported. Traffic entering or leaving the NSX environment can be redirected through a partner service, commonly at a gateway-related insertion point, to provide centralized inspection for external connectivity.

vMotion and management traffic are infrastructure traffic types and are not service-insertion traffic categories. See the VMware NSX-T Data Center Service Insertion documentation.

QUESTION NO: 8

Refer to the exhibit.



Referencing the exhibit, what is the VMware recommended number of NSX Manager Nodes to additionally deploy to form an NSX-T Manager Cluster?

A. 4

B. 3

C. 2

D. 5

ANSWER: C

Explanation:

The correct answer is **2**. An NSX-T Manager cluster is recommended to contain three NSX Manager nodes for production deployment. Where the exhibit represents an already deployed initial NSX Manager appliance, two further NSX Manager nodes must be deployed and added to that appliance to reach the recommended three-node cluster size. A three-node management cluster provides the intended availability and quorum model: cluster services can continue operating when one manager node becomes unavailable, while the remaining nodes retain a majority. VMware documents the process as deploying the first NSX Manager appliance and then deploying and joining two additional appliances to create the NSX Manager cluster. The additional nodes should be installed with compatible versions and configured with the required network connectivity before they are joined through the NSX Manager management interface. This design is the standard production architecture for the NSX-T management plane and supports resilient management services. See the VMware NSX installation documentation at Deploy the NSX Manager Appliances and the NSX Manager cluster administration documentation.

QUESTION NO: 9

Which two statements are true about NSX Intelligence? (Choose two.)

A. NSX Intelligence assists to build service insertion with Partner SVM.

B. NSX Intelligence supports planning of distributed firewall rules and policy.

C. NSX Intelligence can help to visualize network physical infrastructure.

D. NSX Intelligence can be used in conjunction with vRealize Network Insight.

E. NSX Intelligence supports planning of NSX-T Edge Firewall rules and policy.

ANSWER: A B

Explanation:

NSX Intelligence assists to build service insertion with Partner SVM because its application-discovery and traffic-flow analysis capabilities help an administrator understand how workloads communicate before creating security controls. This visibility can be used when planning service insertion policies that steer applicable traffic to a supported partner service virtual machine (SVM). The resulting policy design can account for the application context, the workloads involved, and the traffic that requires inspection by the inserted network-security service.

NSX Intelligence supports planning of distributed firewall rules and policy because a primary function of the product is to analyze observed workload traffic, identify application relationships, and generate policy recommendations. Administrators can review these recommendations in the NSX Intelligence user interface, refine the proposed groups and services as needed, and use them as the basis for distributed firewall policy. This supports a staged microsegmentation process: first observe and visualize communications, then plan the policy, validate the intended controls, and finally publish the appropriate distributed firewall rules. VMware's NSX Intelligence documentation describes these security-planning and policy-recommendation workflows, including support for distributed firewall and service insertion policy planning. See the NSX Intelligence documentation and the NSX-T Data Center Administration Guide.