VMware
6V0-22.25

VMware vDefend Security for VCF 5.x Administrator
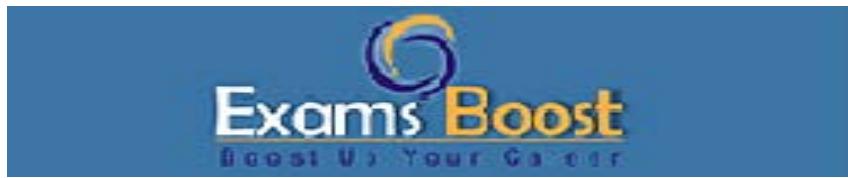
For More Information – Visit link below:

https://www.examsboost.com/

Product Version

Latest Version: 6.0

Question: 1

A security administrator suspects that a service insertion policy is not working as expected. Which NSX Manager feature can be used to validate the health status of the associated service instance?

A. Policy Traceflow
B. Host Profiles Dashboard
C. Service Deployment Status under the NSX Inventory
D. ESXi Hardware Status tab

Answer: C

Question: 2

Which of the following is NOT a characteristic that describes VMware vDefend Security?

A. Elastic scalability
B. Application unaware
C. No network changes needed
D. Supports Policy automation

Answer: B

Question: 3

What role is required to start and stop vDefend Intelligence data collection?

A. Auditor
B. Cloud Administrator
C. Enterprise Administrator
D. Security Administrator

Answer: C

Question: 4

How does the vDefend firewall architecture support horizontal scalability in private cloud environments?

A. By using a single centralized rule engine for all traffic
B. By distributing packet inspection only at the DMZ
C. By assigning firewall processing to NSX edge nodes
D. By embedding the enforcement logic into every hypervisor host

Answer: D

Question: 5

What file types can vDefend Gateway Malware Detection analyze?
(Select all that apply)

A. Benign
B. Suspicious
C. Malicious
D. Unknown

Answer: A,B,C

Question: 6

When NSX Malware Prevention detects a suspicious file, what is the typical default behavior?

A. Move the file to a backup location
B. Block the file and generate a security alert
C. Automatically shut down the infected VM
D. Forward the file to the tenant's email for verification

Answer: B

Question: 7

Which of the statements below are true about the Time-Based Firewall Policy capability?
(Select all that apply)

A. Cannot be combined with VDI, RDSH, and IDFW
B. Require all time-based rules to be defined in UTC time zone
C. Can be applied at the vDefend Distributed Firewall and Gateway Firewall
D. Can apply a different Security Policy based on day and time

Question: 8

Which scripting or automation platform is commonly used alongside NSX-T for automating vDefend firewall rule deployment?

A. Chef
B. Python with REST API
C. Hadoop
D. Ansible Playbooks for storage arrays

Answer: B

Question: 9

Which NSX component is responsible for correlating malware events and providing detailed threat visibility?

A. NSX Edge Gateway
B. NSX Malware Prevention Engine
C. NSX Manager Security Dashboard
D. vCenter Alarm Manager

Answer: C

Question: 10

In the context of securing a private cloud, which two are considered best practices when designing workload isolation strategies?
(Choose two)

A. Use VLANs as the only method of segmentation
B. Group workloads by function and apply role-based security policies
C. Allow all traffic within a cluster to avoid unnecessary latency
D. Employ security groups tied to VM tags or attributes
E. Disable logging on security rule sets for performance reasons

Answer: B,D

Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ **90 Days Free Updates**

- ✓ **Money Back Pass Guarantee**

- ✓ **Instant Download or Email Attachment**

- ✓ **24/7 Live Chat Support**

- ✓ **PDF file could be used at any Platform**

- ✓ **50,000 Happy Customer**