NSE5_FNC_AD_7.6 Valid Study Questions | Latest NSE5_FNC_AD_7.6 Test Voucher

P.S. Free & New NSE5_FNC_AD_7.6 dumps are available on Google Drive shared by VCEEngine: https://drive.google.com/open?id=1_bf41mfGVN9H_mpahXjSh7RR7XTErWOP

Test your knowledge of the Fortinet NSE 5 - FortiNAC-F 7.6 Administrator (NSE5_FNC_AD_7.6) exam dumps with VCEEngine Fortinet NSE 5 - FortiNAC-F 7.6 Administrator (NSE5_FNC_AD_7.6) practice questions. The software is designed to help with Fortinet NSE 5 - FortiNAC-F 7.6 Administrator (NSE5_FNC_AD_7.6) exam dumps preparation. Fortinet NSE5_FNC_AD_7.6 practice test software can be used on devices that range from mobile devices to desktop computers.

Fortinet NSE5_FNC_AD_7.6 Exam Overview:

Certification Vendor:	Fortinet
Exam Name:	Fortinet NSE 5 - FortiNAC-F 7.6 Administrator
Exam Number:	NSE5_FNC_AD_7.6
Related Certifications:	Fortinet Certified Professional (FCP) Network Security NSE 4 Network Security Fortinet Certified Associate (FCA)
Real Exam Qty:	30-40
Certificate Validity Period:	2 years
Exam Price:	USD 200
Exam Duration:	60 minutes
Available Languages:	English
Exam Format:	Scenario-based questions, Multiple-choice, Multiple-response
Recommended Training:	FortiNAC Administrator Training (Fortinet Official Course)
Exam Registration:	Pearson VUE Fortinet Exams Fortinet Training Institute
Sample Questions:	Fortinet NSE5_FNC_AD_7.6 Sample Questions
Exam Way:	Online proctored or Pearson VUE test center delivery
Pre Condition:	Recommended knowledge of networking fundamentals and Fortinet NSE 4 level concepts.
Official Syllabus URL:	https://training.fortinet.com

>> NSE5_FNC_AD_7.6 Valid Study Questions <<

Free PDF Quiz Fortinet - Perfect NSE5_FNC_AD_7.6 - Fortinet NSE 5 -

FortiNAC-F 7.6 Administrator Valid Study Questions

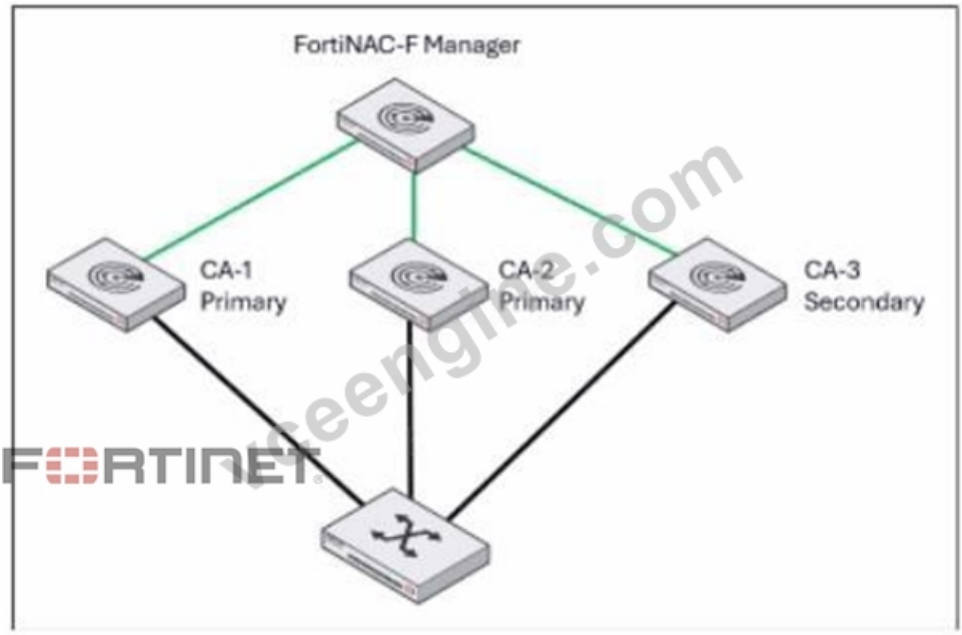
Generally speaking, you can achieve your basic goal within a week with our Fortinet NSE 5 - FortiNAC-F 7.6 Administrator NSE5_FNC_AD_7.6 study guide. Besides, for new updates happened in this line, our experts continuously bring out new ideas in this Fortinet NSE5_FNC_AD_7.6 Exam for you. The new supplemental updates will be sent to your mailbox if there is and be free.

Fortinet NSE5_FNC_AD_7.6 Exam Syllabus Topics:

Topic	Details
Topic 1	• Concepts and Initial Configuration: This domain covers organizing infrastructure devices within FortiNAC-F and understanding isolation networks for quarantining non-compliant devices. It includes using the configuration wizard for initial system setup and deployment.
Topic 2	• Integration: This domain addresses connecting FortiNAC-F with other systems using Syslog and SNMP traps, managing multiple instances through FortiNAC-F Manager, and integrating Mobile Device Management for extending access control to mobile devices.
Topic 3	• Deployment and Provisioning: This domain focuses on configuring security automation for automatic event responses, implementing access control policies, setting up high availability for system redundancy, and creating security policies to enforce network security requirements.
Topic 4	• Network Visibility and Monitoring: This domain covers managing guest and contractor access, utilizing logging options for tracking network events, configuring device profiling for automatic device identification and classification, and troubleshooting network device connection issues.

Fortinet NSE 5 - FortiNAC-F 7.6 Administrator Sample Questions (Q42-Q47):

NEW QUESTION # 42
Refer to the exhibit.
A FortiNAC-F N+1 HA configuration is shown.



What will occur if CA-2 fails?

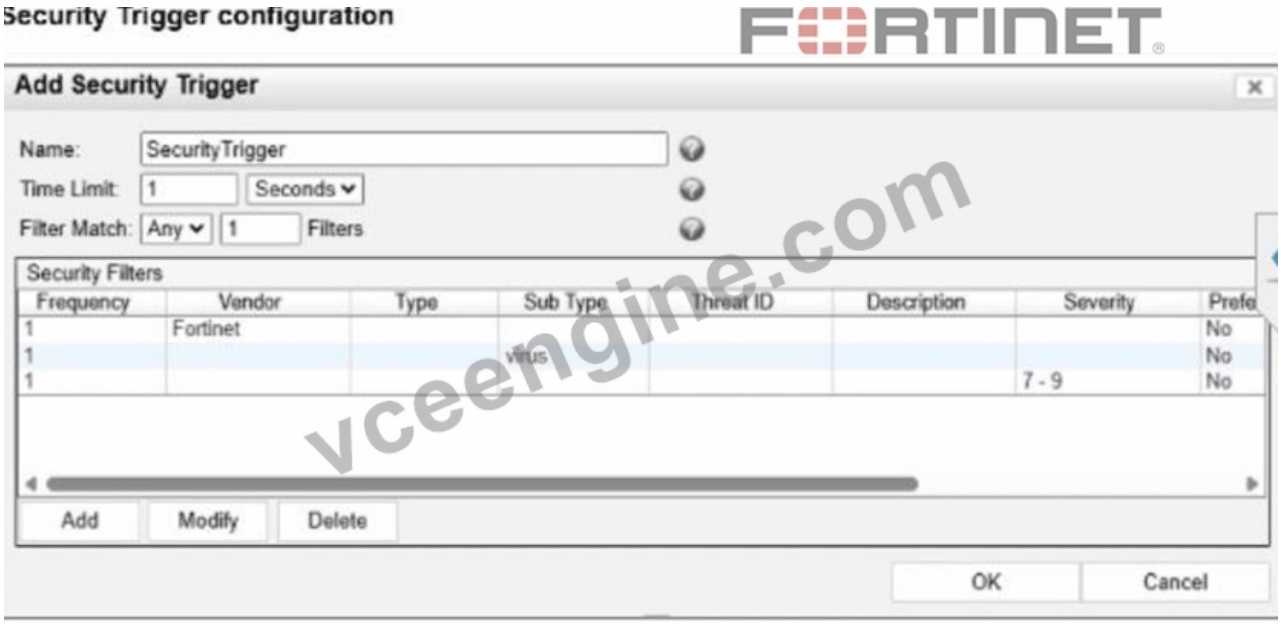
- A. CA-1 and CA-3 will operate as a 1+1 HA cluster with CA-3 acting as a hot standby.
- B. CA-3 will continue to operate as a secondary in an N+1 HA configuration.
- C. CA-3 will be promoted to a primary and FortiNAC-F manager will load balance between CA-1 and CA-3.

- D. CA-3 will be promoted to a primary and share management responsibilities with CA-1.

Answer: B

Explanation:
In anN+1 High Availability (HA)configuration, a single secondary Control and Application (CA) server provides backup for multiple primary CA servers. The FortiNAC-F Manager (FortiNAC-M) acts as the centralized orchestrator for this cluster, monitoring the health of all participating nodes.
According to theFortiNAC-F 7.6.0 N+1 Failover Reference Manual, when a primary CA (such asCA-2in the exhibit) fails, the secondary CA (CA-3) is automatically promoted by the Manager to take over the specific workload and database functions of that failed primary. Crucially, the documentation specifies that even after this promotion, the system architecture maintains its N+1 logic. The secondary CA effectively " assumes the identity " of the failed primary while continuing to operate within the N+1 framework established by the Manager.
It doesnotmerge with CA-1 to form a traditional 1+1 active/passive cluster (A), nor does it engage in load balancing (D), as FortiNAC-F HA is designed for redundancy and failover rather than active traffic distribution. Furthermore, CA-3 does not " share " management with CA-1 (C); it independently handles the tasks originally assigned to CA-2. Throughout this failover state, the Manager continues to oversee the group, and CA-3 remains the designated secondary unit currently acting in a primary capacity for the downed node until CA-2 is restored.
" In an N+1 Failover Group, theSecondary CAis designed to take over the functionality ofany single failed primary componentwithin the group. The FortiNAC Manager monitors the primaries and initiates the failover to the secondary... Once failover occurs, the secondary continues to operate as the backup unit for the failed primary while remaining part of the managed N+1 HA configuration. " -FortiNAC-F 7.6.0 N+1 Failover Reference Manual: Failover Behavior Section.

NEW QUESTION # 43
Refer to the exhibits.



Given the current configuration, what would happen if a contractor triggered two of the defined security filters?

- A. Two security events would be generated, but no security alarm would be generated
- B. A security event and a security alarm would be generated.
- C. A security alarm and two security events would be generated.
- D. Three security events and one security alarm would be generated.

Answer: C

Explanation:
The correct answer is B . In the trigger exhibit, the Filter Match setting is configured as Any 1 Filters , meaning the security trigger is satisfied when any one of the defined filters matches within the configured time window. The contractor triggers two of the defined filters, so two separate security events are generated because FortiNAC-F creates a security event whenever a security filter matches. The study guide confirms that each matched filter generates a security event, and when a trigger contains multiple filters, multiple matched filters can be associated with the resulting alarm.
The security rule exhibit also shows User/Host Profile: Match Contractors . Because the triggering user is a contractor, the user/host profile condition is satisfied. Once the trigger is satisfied and the user/host profile matches, FortiNAC-F generates a security alarm . The fact that Action is set to None does not stop the alarm from being generated; it only means no automated or manual response action is executed from that rule.
Option A is wrong because the contractor profile matches, so an alarm is generated. Option C is wrong because only two filters were triggered, not three. Option D is wrong because two filters matched, so two events are generated, not one.

NEW QUESTION # 44
Which two requirements must be met to set up an N+1 HA cluster? (Choose two.)

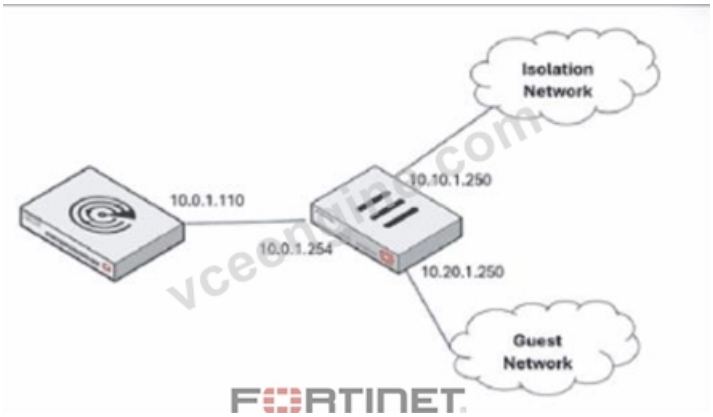
- A. A FortiNAC-F manager
- B. A FortiNAC-F device designated as a secondary
- C. A dedicated VLAN for primary and secondary synchronization
- D. At least two FortiNAC-F devices designated as primary

Answer: A,B

Explanation:
The N+1 High Availability (HA) architecture was introduced in FortiNAC-F version 7.6 to provide a more scalable and flexible redundancy model compared to the traditional 1+1 active/passive setup. In an N+1 configuration, a single secondary (standby) appliance can provide coverage for multiple primary (active) Control and Application (CA) appliances.
To set up an N+1 HA cluster, there are two fundamental structural requirements:
A FortiNAC-F Manager (FortiNAC-M): Unlike standard 1+1 HA, which can be configured directly between two CAs, N+1 management is centralized. The FortiNAC-M acts as the orchestrator that manages the failover groups, monitors the health of the primaries, and coordinates the promotion of the secondary server if a primary fails.
A FortiNAC-F device designated as a Secondary: The cluster must have one appliance explicitly configured with the Secondary

failover role. This device remains in a standby state, receiving database replications from all N primaries in its group until it is called upon to take over the functions of a failed unit.
While a cluster can support multiple primaries (D), it does not strictly require "at least two" to function as an N+1 group; it simply requires N primaries (where N ≥ 1). Additionally, N+1 is typically a Layer 3 managed solution via the Manager, meaning it does not mandate a "dedicated VLAN" for synchronization like some Layer 2 HA deployments.
"In FortiNAC-F 7.6, FortiNAC-M functions as a manager to manage the N+1 Failover Groups... enabling N+M high availability for CAs. To create an N+1 Failover group, you should add the secondary CA to the FortiNAC-M first, then add the primary CAs. The secondary CA is designed to take over the functionality of any single failed primary component." - FortiNAC-F 7.6.0 N+1 Failover Reference Manual.

NEW QUESTION # 45
Refer to the exhibit.



An administrator is configuring FortiNAC-F (or the onboarding of guest users. Which IP address would be used for the gateway defined in the DHCP scope?

- A. 10.10.1.250
- B. 10.0.1.110
- C. 10.0.1.254
- D. 10.20.1.250

Answer: D

Explanation:
The correct answer is D . The question is about guest onboarding , and the exhibit shows the Guest Network using gateway 10.20.1.250 . In a Layer 3 captive network design, FortiNAC-F provides DHCP and DNS services to isolated or captive-network hosts, but the DHCP scope must still give the endpoint the correct default gateway for the network where that endpoint is placed. The study guide specifically warns that, when configuring Layer 3 captive network scopes, the administrator must think from the isolated host's perspective for the IP pool and gateway configuration . It also states that each captive network interface configuration includes an IP address, subnet mask, default gateway, and one or more DHCP scopes.
Option A , 10.0.1.254 , is the infrastructure gateway on the FortiNAC-F service/production-side segment, not the guest network gateway. Option B , 10.0.1.110 , is the FortiNAC-F interface address shown in the diagram, not the default gateway for guest clients. Option C , 10.10.1.250 , is the gateway for the Isolation Network , not the Guest Network . Since the administrator is configuring guest onboarding, the DHCP scope for guest users must hand out 10.20.1.250 as the gateway.

NEW QUESTION # 46
What must an administrator configure to allow FortiNAC-F to process incoming syslog messages that are not supported by default?

- A. A Log Receiver
- B. A Security Action
- C. A Syslog Service Connector
- D. A Security Event Parser

Answer: D

Explanation:
FortiNAC-F provides a robust engine for processing security notifications from third-party devices. For standard integrations, such

as FortiGate or Check Point, the system comes pre-loaded with templates to interpret incoming data. However, when an administrator needs FortiNAC-F to process syslog messages from a vendor or device that is not supported by default, they must configure a Security Event Parser.
The Security Event Parser acts as the translation layer. It uses regular expressions (Regex) or specific field mappings to identify key data points within a raw syslog string, such as the source IP address, the threat type, and the severity. Without a parser, FortiNAC-F may receive the syslog message but will be unable to "understand" its contents, meaning it cannot generate the necessary Security Event required to trigger automated responses. Once a parser is created, the system can extract the host's IP address from the message, resolve it to a MAC address via L3 polling, and then apply the appropriate security rules. This allows for the integration of any security appliance capable of sending RFC-compliant syslog messages.
"FortiNAC parses the information based on pre-defined security event parsers stored in FortiNAC's database... If the incoming message format is not recognized, a new Security Event Parser must be created to define how the system should extract data fields from the raw syslog message. This enables FortiNAC to generate a security event and take action based on the alarm configuration." - FortiNAC-F Administration Guide: Security Event Parsers.

NEW QUESTION # 47
.....