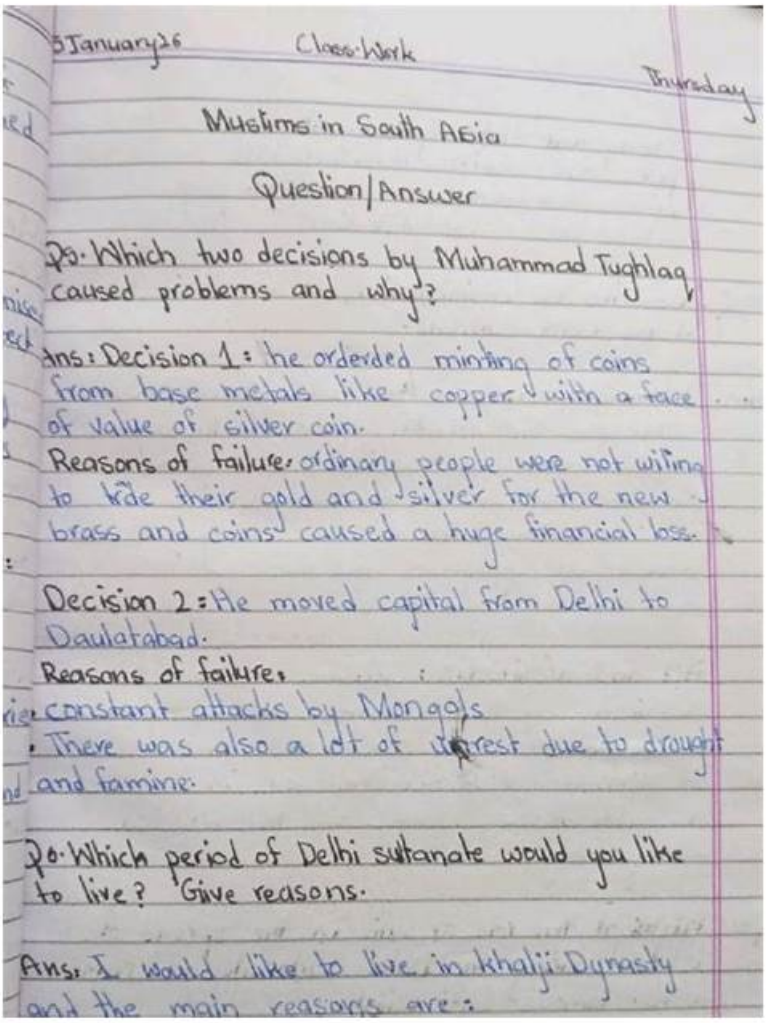
NSE5_FNC_AD_7.6 Latest Learning Material | NSE5_FNC_AD_7.6 Answers Free


5 January'26 Class-Work Thursday

Muslims in South Asia

Question/Answer

Q5. Which two decisions by Muhammad Tughlaq caused problems and why?

Ans: Decision 1: he ordered minting of coins from base metals like copper with a face of value of silver coin.
Reasons of failure: ordinary people were not willing to hide their gold and silver for the new brass and coins caused a huge financial loss.

Decision 2: He moved capital from Delhi to Daulatabad.
Reasons of failure:
- constant attacks by Mongols
- There was also a lot of unrest due to drought and famine.

Q6. Which period of Delhi sultanate would you like to live? Give reasons.

Ans: I would like to live in Khalji Dynasty and the main reasons are:

PrepAwayPDF Fortinet NSE5_FNC_AD_7.6 practice exam is the most thorough, most accurate and latest practice test. You will find that it is the only materials which can make you have confidence to overcome difficulties in the first. Fortinet NSE5_FNC_AD_7.6 exam certification are recognized in any country in the world and all countries will be treate it equally. Fortinet NSE5_FNC_AD_7.6 Certification not only helps to improve your knowledge and skills, but also helps your career have more possibility.

The NSE5_FNC_AD_7.6 exam materials is a dump, maybe many candidates will worry about how to payment and whether it is safe when pay for it. Some people may think that online shopping is not safe. Now I will tell you responsibly that our payment method of NSE5_FNC_AD_7.6 exam materials is very secure. The payment method we use is credit card payment, not only can we guarantee your security of the payment, but also we can protect your right and interests. As for the safety issue of NSE5_FNC_AD_7.6 Exam Materials you are concerned about is completely unnecessary. You can rest assured to buy and use it.

>> NSE5_FNC_AD_7.6 Latest Learning Material <<

2026 NSE5_FNC_AD_7.6 Latest Learning Material | Pass-Sure NSE5_FNC_AD_7.6 Answers Free: Fortinet NSE 5 - FortiNAC-F 7.6 Administrator

We offer you to take back your money, if you do not succeed in NSE5_FNC_AD_7.6 exam. Such a guarantee in itself is concrete evidence on the unmatched quality of our NSE5_FNC_AD_7.6 dumps. For the reason, they are approved not only by a large

number of professionals who are busy in developing their careers but also by the industry experts. Get the right reward for your potential, believing in the easiest and to the point NSE5_FNC_AD_7.6 Exam Questions that are meant to bring you a brilliant success in NSE5_FNC_AD_7.6 exams.

Fortinet NSE5_FNC_AD_7.6 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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.
Topic 2	• 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 3	• 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 4	• 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.

Fortinet NSE 5 - FortiNAC-F 7.6 Administrator Sample Questions (Q26-Q31):

NEW QUESTION # 26
Which two requirements must be met to set up an N+1 HA cluster? (Choose two.)

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

Answer: A,C

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 $N \geq 1$). 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 # 27

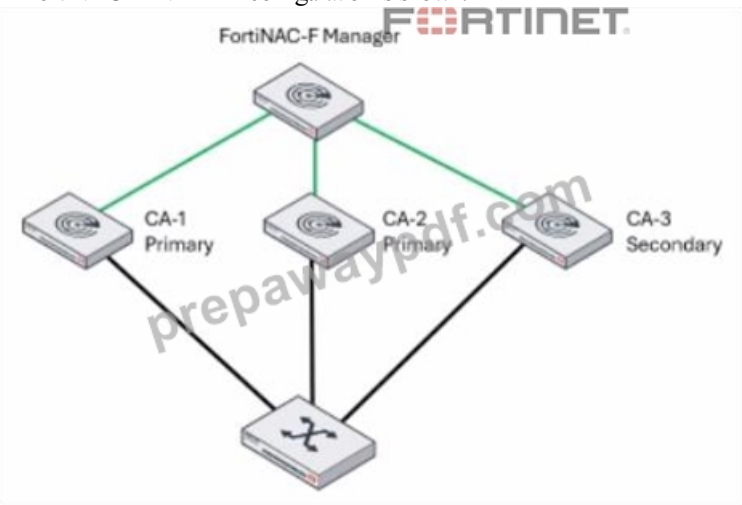
A network administrator is troubleshooting a network access issue for a specific host. The administrator suspects the host is being assigned a different network access policy than expected.
Where would the administrator look to identify which network access policy, if any, is being applied to a particular host?

- A. The Policy Logs view
- B. The Connections view
- C. The Port Properties view of the hosts port
- D. The Policy Details view for the host

Answer: D

Explanation:
When troubleshooting network access in FortiNAC-F, it is often necessary to verify exactly why a host has been granted a specific level of access. Since FortiNAC-F evaluates policies from the top down and assigns access based on the first match, an administrator needs a clear way to see the results of this evaluation for a specific live endpoint.
The Policy Details (C) view is the designated tool for this purpose. By navigating to the Hosts > Hosts (or Adapter View) in the Administration UI, an administrator can search for the specific MAC address or IP of the host in question. Right-clicking on the host record reveals a context menu from which Policy Details can be selected. This view provides a real-time "look" into the policy engine's decision for that specific host, showing the Network Access Policy that was matched, the User/Host Profile that triggered the match, and the resulting Network Access Configuration (VLAN/ACL) currently applied.
While Policy Logs (A) provide a historical record of all policy transitions across the system, they are often too high-volume to efficiently find a single host's current state. The Connections view (B) shows the physical port and basic status but lacks the granular policy logic breakdown. The Port Properties (D) view shows the configuration of the switch interface itself, which is only one component of the final access determination.
"To identify which policy is currently applied to a specific endpoint, use the Policy Details view. Navigate to Hosts > Hosts, select the host, right-click and choose Policy Details. This window displays the specific Network Access Policy, User/Host Profile, and Network Access Configuration currently in effect for that host record." - FortiNAC-F Administration Guide: Policy Details and Troubleshooting.

NEW QUESTION # 28
Refer to the exhibit.
A FortiNAC-F N+1 HA configuration is shown.



What will occur if CA-2 fails?

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

Answer: C

Explanation:
In an N+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 the FortiNAC-F 7.6.0 N+1 Failover Reference Manual, when a primary CA (such as CA-2 in 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 does not merge 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, the Secondary CA is designed to take over the functionality of any single failed primary component within 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 # 29
When FortiNAC-F is managing VPN clients connecting through FortiGate, why must the clients run a FortiNAC-F agent?

- A. To validate the endpoint policy compliance
- B. To collect user authentication details
- C. To transparently update The client IP address upon successful authentication
- D. To collect the client IP address and MAC address

Answer: D

Explanation:
When FortiNAC-F manages VPN clients through a FortiGate, the agent plays a fundamental role in device identification that standard network protocols cannot provide on their own. In a standard VPN connection, the FortiGate establishes a Layer 3 tunnel and assigns a virtual IP address to the client. While the FortiGate sends a syslog message to FortiNAC-F containing the username and this assigned IP address, it typically does not provide the hardware (MAC) address of the remote endpoint's physical or virtual adapter.
FortiNAC-F relies on the MAC address as the primary unique identifier for all host records in its database. Without the MAC address, FortiNAC-F cannot correlate the incoming VPN session with an existing host record to apply specific policies or track the device's history. By running either a Persistent or Dissolvable Agent, the endpoint retrieves its own MAC address and communicates it directly to the FortiNAC-F service interface. This allows the "IP to MAC" mapping to occur. Once FortiNAC-F has both the IP and the MAC, it can successfully identify the device, verify its status, and send the appropriate FSSO tags or group information back to the FortiGate to lift network restrictions.
Furthermore, while the agent can also perform compliance checks (Option D), the architectural requirement for the agent in a managed VPN environment is primarily driven by the need for session data correlation-specifically the collection of the IP and MAC address pairing.
"Session Data Components: * User ID (collected via RADIUS, syslog and API from the FortiGate). * Remote IP address for the remote user connection (collected via syslog and API from the FortiGate and from the FortiNAC agent). * Device IP and MAC address (collected via FortiNAC agent). ... The Agent is used to provide the MAC address of the connecting VPN user (IP to MAC)." - FortiNAC-F FortiGate VPN Integration Guide: How it Works Section.

NEW QUESTION # 30
An administrator wants to control user access to corporate resources by integrating FortiNAC-F with FortiGate using firewall tags defined on FortiNAC-F.
Where would the administrator assign the firewall tag value that will be sent to FortiGate?

- A. Device profiling rule
- B. RADIUS group attribute
- C. Security rule
- D. Logical network

Answer: D

Explanation:
Questio ns no: 9

Verified Answe r: B
Comprehensive and Detailed 250 to 300 words each Explanation with Exact Matched Extract from FortiNAC-F Administrator library and documentation for current versions (including F 7.2, 7.4, and 7.6) documents:
In FortiNAC-F, the integration with FortiGate for Security Fabric and Single Sign-On (FSSO) allows the system to communicate the access level of an endpoint directly to the firewall using firewall tags. This eliminates the need for complex VLAN steering in some environments by allowing the FortiGate to apply policies based on these dynamic tags instead of just a physical or virtual network segment.
The actual assignment of the firewall tag value occurs within a Logical Network. In the FortiNAC-F architectural model, a Logical Network acts as a container for "Access Values". When an administrator configures a Logical Network (located under Network > Logical Networks), they define what that network represents-such as "Corporate Access" or "Contractor Limited". Within that definition, they assign the specific Firewall Tag that matches the tag created on the FortiGate. Once a user or host matches a Network Access Policy, FortiNAC-F identifies the associated Logical Network and pushes the defined tag to the FortiGate via the FSSO connector.
It is important to note that while Network Access Policies (and by extension Security Rules) are the logic engines that trigger the assignment, they do not hold the tag value itself. They simply point to a Logical Network, which serves as the central repository for that specific access configuration.
"To assign firewall tags, navigate to Network > Logical Networks. Select the desired logical network and click Edit. Under the Access Value section, select Firewall Tag as the type and enter the tag name exactly as it appears on the FortiGate. When a Network Access Policy matches a host, FortiNAC sends this tag to the FortiGate as an FSSO message." - FortiNAC-F Administration Guide: Logical Networks and Security Fabric Integration.

NEW QUESTION # 31
.....

Many job-hunters want to gain the competition advantages in the labor market and become the hottest people which the companies rush to get. But if they want to realize that they must boost some valuable NSE5_FNC_AD_7.6 certificate. The NSE5_FNC_AD_7.6 certificate enjoys a high reputation among the labor market circle and is widely recognized as the proof of excellent talents and if you are one of them and you want to pass the NSE5_FNC_AD_7.6 test smoothly you can choose our NSE5_FNC_AD_7.6 practice questions.

Source

- NSE5_FNC_AD_7.6 Reliable Test Tutorial □ Book NSE5_FNC_AD_7.6 Free □ NSE5_FNC_AD_7.6 Accurate Answers □ Open （ www.pdfdumps.com ） enter 【 NSE5_FNC_AD_7.6 】 and obtain a free download □ □NSE5_FNC_AD_7.6 Actual Questions
- www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.ted.com, wanderlog.com, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes