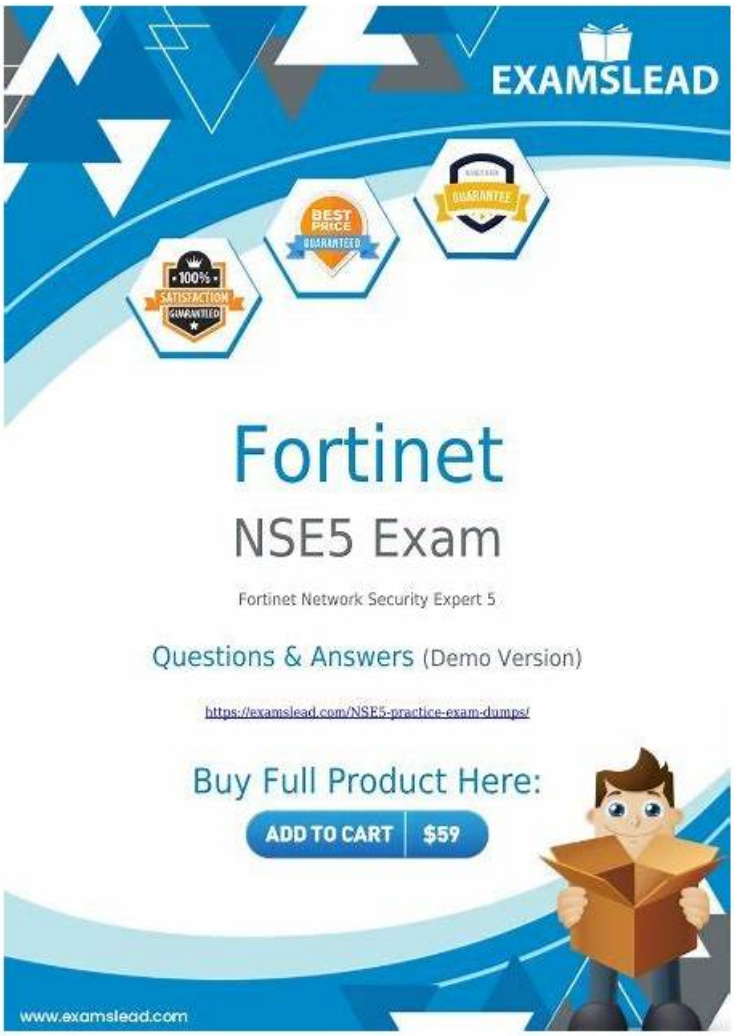
# Get Trustable NSE5_FNC_AD_7.6 Valid Exam Cram and Pass Exam in First Attempt




As you know, we are now facing very great competitive pressure. We need to have more strength to get what we want, and NSE5_FNC_AD_7.6 exam dumps may give you these things. After you use our study materials, you can get NSE5_FNC_AD_7.6 certification, which will better show your ability, among many competitors, you will be very prominent. Using NSE5_FNC_AD_7.6 Exam Prep is an important step for you to improve your soft power. I hope that you can spend a little time understanding what our study materials have to attract customers compared to other products in the industry.

## 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 | • 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 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 | • 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. |



## NSE5_FNC_AD_7.6 Certification Dump, Latest NSE5_FNC_AD_7.6 Exam Test

We have created a number of reports and learning functions for evaluating your proficiency for the Fortinet NSE 5 - FortiNAC-F 7.6 Administrator (NSE5_FNC_AD_7.6) exam dumps. In preparation, you can optimize Fortinet NSE 5 - FortiNAC-F 7.6 Administrator (NSE5_FNC_AD_7.6) practice exam time and question type by utilizing our Fortinet NSE5_FNC_AD_7.6 Practice Test software. ActualTorrent makes it easy to download Fortinet NSE5_FNC_AD_7.6 exam questions immediately after purchase. You will receive a registration code and download instructions via email.

## Fortinet NSE 5 - FortiNAC-F 7.6 Administrator Sample Questions (Q23-Q28):

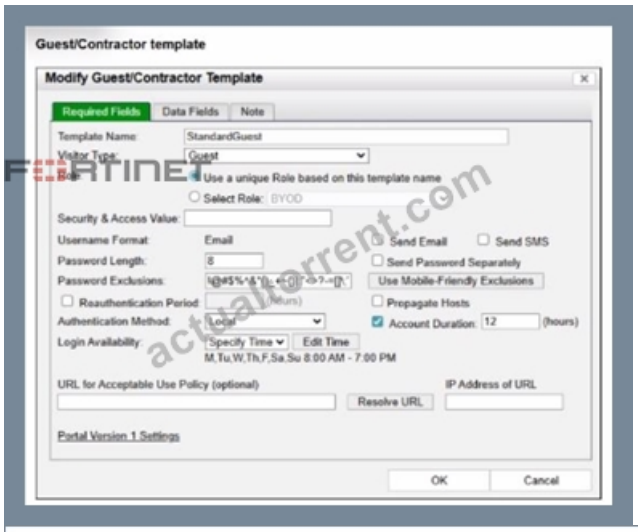
**NEW QUESTION # 23**
While discovering network infrastructure devices, a switch appears in the inventory topology with a question mark (?) on the icon. What would cause this?

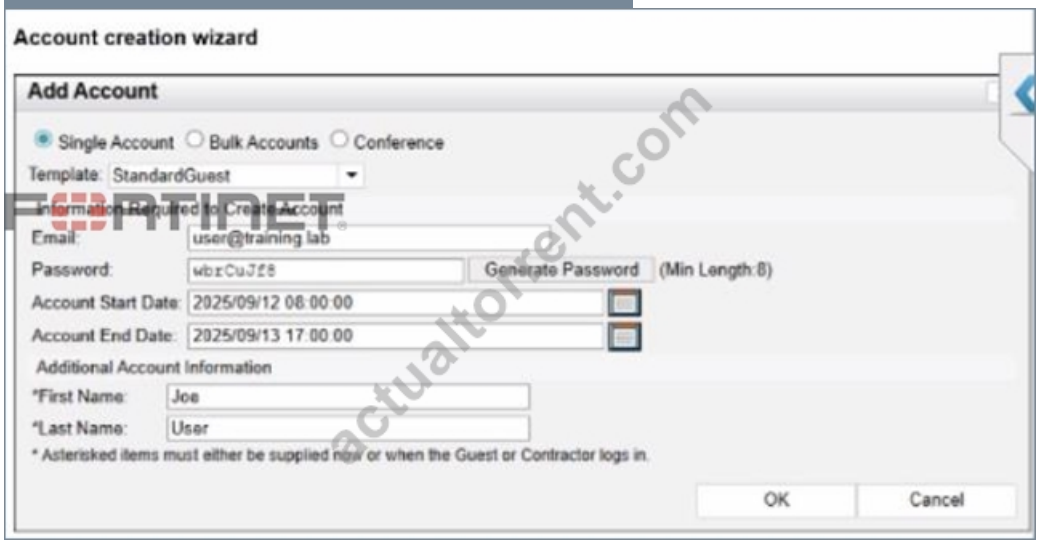
- A. A read-only SNMP community siring was used.
- B. The SNMP ObjectlD is not recognized by FortiNAC-F.
- C. The wrong SNMP community string was entered during discovery.
- D. SNMP is not enabled on the switch.

**Answer: B**

Explanation:
In FortiNAC-F, the Inventory topology uses specific icons to represent the status and model of discovered network infrastructure. When a switch or other network device is discovered via SNMP, FortiNAC-F retrieves its System ObjectID (sysObjectID) to identify the specific make and model. This OID is then compared against the internal database of supported device mappings.
A question mark (?) icon appearing on a discovered switch indicates that while the discovery process successfully communicated with the device (meaning SNMP credentials were correct), the SNMP ObjectID is not recognized or mapped in the current version of FortiNAC-F. This essentially means the device is "unsupported" by the current software out-of-the-box. Because the OID is unknown, FortiNAC-F does not know which CLI or SNMP command set to use for critical functions like L2 polling (host visibility) or VLAN switching (enforcement). To resolve this, an administrator can manually "Set Device Mapping" to a similar existing model or a "Generic SNMP Device" if only basic L3 visibility is required.
"Discovered devices displaying a '?' icon indicate the currently running version does not have a mapping for that device's System OID (device is not supported). Device mappings are used to manage the device by performing functions such as L2/L3 Polling, Reading, and Switching VLANs." - Fortinet Technical Tip: Options for devices unable to be modeled in Inventory.

**NEW QUESTION # 24**
Refer to the exhibits.




Based on the given configurations and settings, on which date and time would a guest account created at 8:00 AM on 2025/09/12 expire?

- A. 2025/09/12 at 8:00 PM
- B. 2025/09/13 at 17:00:00
- C. 2025/09/12 at 17:00:00
- D. 2025/09/12 at 7:00 PM

**Answer: B**

Explanation:
Questio ns no: 22
Verified Answe r: D
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 expiration of a guest or contractor account is determined by the configuration settings within the Account Creation Wizard and the associated Guest/Contractor Template. While a template can define a default "Account Duration" (as seen in the 12-hour setting in the second exhibit), the Account Creation Wizard allows an administrator to manually specify or override the start and end parameters for a specific user session.
According to the FortiNAC-F Administration Guide regarding guest management, the Account End Date field in the creation wizard is the definitive timestamp for when the account object will be disabled or deleted from the system. In the provided exhibit (Account Creation Wizard), the administrator has explicitly set the Account Start Date to 2025/09/12 08:00:00 and the Account End Date to 2025/09/13 17:00:00.
Even though the template indicates an "Account Duration" of 12 hours, this value typically serves as a pre-populated default. When a manual date and time are entered into the wizard, those specific values take precedence for that individual account. The account will remain active and valid until 5:00 PM (17:00:00) on the following day, 2025/09/13. It is also important to note the "Login Availability" from the template (8:00 AM - 7:00 PM); while the account exists until the 13th at 17:00:00, the user would only be able to authenticate during the active hours defined by the login schedule on both days.

"When creating an account, the administrator can select a template to provide default settings. However, specific values such as the Account End Date can be modified within the Account Creation Wizard. The date and time specified in the 'Account End Date' field determines the absolute expiration of the account. Once this time is reached, the account is moved to an expired state and the user's network access is revoked." - FortiNAC-F Administration Guide: Guest and Contractor Account Management.

**NEW QUESTION # 25**
An administrator wants FortiNAC-F to return a group of user-defined RADIUS attributes in RADIUS responses.
Which condition must be true to achieve this?

- A. Inbound RADIUS requests must contain the Calling-Station-ID attribute.
- B. The requesting device must support RFC 5176.
- C. The device models in the inventory view must be configured for proxy-based authentication.
- D. RADIUS accounting must be enabled on the FortiNAC-F RADIUS server configuration.

**Answer: A**

Explanation:
In FortiNAC-F, the RADIUS Attribute Groups feature allows administrators to return customized RADIUS attributes (such as specific VLAN IDs, filter IDs, or vendor-specific attributes) in an Access-Accept packet sent back to a network device. This is particularly useful for supporting "Generic RADIUS" devices that are not natively supported but can be managed using standard AVPairs.
According to the FortiNAC-F Generic RADIUS Wired Cookbook and the RADIUS Attribute Groups section of the Administration Guide, there is one critical prerequisite for this feature to function: the inbound RADIUS request must contain the Calling-Station-ID attribute. The Calling-Station-ID typically contains the MAC address of the connecting endpoint. Because FortiNAC-F is a host-centric system, it uses the MAC address as the unique identifier to look up the host record, evaluate the associated Network Access Policy, and determine which Logical Network (and thus which Attribute Group) should be applied. If the incoming request lacks this attribute, FortiNAC-F cannot reliably identify the host and, as a safety mechanism, will not include any user-defined RADIUS attributes in the response. This ensures that unauthorized or unidentifiable devices do not receive privileged access through misapplied attributes.
"Configure a set of attributes that must be included in the RADIUS Access-Accept packet returned by FortiNAC... Requirement: Inbound RADIUS request must contain Calling-Station-Id. Otherwise, FortiNAC will not include the RADIUS attributes. This attribute is used to identify the host and its current state within the FortiNAC database." - FortiNAC-F 7.6.0 Generic RADIUS Wired Cookbook: Configure RADIUS Attribute Groups.

**NEW QUESTION # 26**
Where should you configure MAC notification traps on a supported switch?

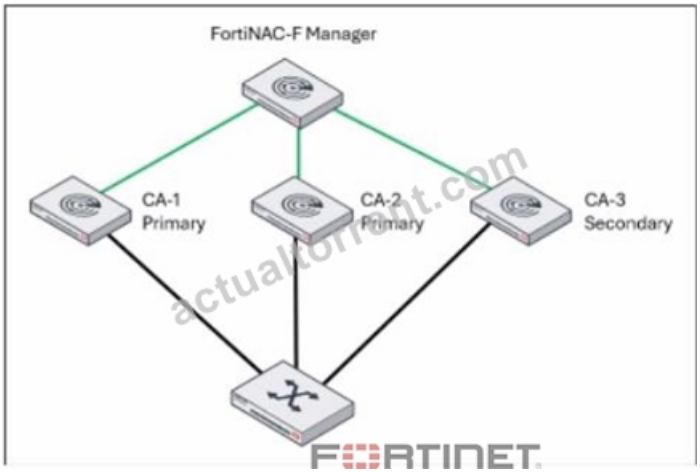
- A. Only on ports that generate linkup and linkdown traps
- B. On all ports on the switch
- C. On all ports except uplink ports
- D. Only on ports defined as learned uplinks

**Answer: C**

Explanation:
In FortiNAC-F, MAC notification traps (also known as MAC Move or MAC Change traps) are essential for achieving real-time visibility of endpoint connections and disconnections. When a device connects to a switch port, the switch generates an SNMP trap that informs FortiNAC-F of the new MAC address on that specific interface. This allows FortiNAC-F to immediately initiate the profiling and policy evaluation process without waiting for the next scheduled L2 poll.
According to the FortiNAC-F Administration Guide and Switch Integration documentation, MAC notification traps should be configured on all ports except uplink ports. Uplink ports are the interfaces that connect one switch to another or to the core network. Because these ports see the MAC addresses of every device on the downstream switches, enabling MAC notification on uplinks would cause the switch to send a massive volume of redundant traps to FortiNAC-F every time any device anywhere in the downstream branch moves or reconnects. This can overwhelm the FortiNAC-F process queue and degrade system performance. By only enabling these traps on "edge" or "access" ports-where individual endpoints like PCs, printers, and VoIP phones connect-FortiNAC-F receives precise data regarding exactly where a device is physically located. Uplinks should be identified in the FortiNAC-F inventory as "Uplink" or "Learned Uplink," which tells the system to ignore MAC data seen on those specific ports.
"To ensure accurate host tracking and optimal system performance, SNMP MAC notification traps must be enabled on all access (downlink) ports. Do not enable MAC notification traps on uplink ports, as this will result in excessive and unnecessary trap

processing. Uplink ports should be excluded to prevent the system from attempting to map multiple downstream MAC addresses to a single infrastructure interface." - FortiNAC-F Administration Guide: SNMP Configuration for Network Devices.

**NEW QUESTION # 27**
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-1 and CA-3 will operate as a 1+1 HA cluster with CA-3 acting as a hot standby.
- D. CA-3 will continue to operate as a secondary in an N+1 HA configuration.

**Answer: D**

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 # 28**
.....

- High Pass-Rate NSE5_FNC_AD_7.6 Valid Exam Cram - Leading Offer in Qualification Exams - Reliable NSE5_FNC_AD_7.6 Certification Dump □ Easily obtain free download of ⇛ NSE5_FNC_AD_7.6 ⇚ by searching on ✔ www.practicevce.com □✔□ □Sample NSE5_FNC_AD_7.6 Questions Answers
- High Pass-Rate NSE5_FNC_AD_7.6 Valid Exam Cram - Leading Offer in Qualification Exams - Reliable NSE5_FNC_AD_7.6 Certification Dump □ Download " NSE5_FNC_AD_7.6 " for free by simply searching on ⇛ www.pdfvce.com ⇚ □NSE5_FNC_AD_7.6 Reliable Test Duration
- Valid NSE5_FNC_AD_7.6 Exam Pdf □ NSE5_FNC_AD_7.6 Latest Braindumps Sheet □ NSE5_FNC_AD_7.6 Valid Exam Practice □ Search on ➽ www.practicevce.com □ for ➽ NSE5_FNC_AD_7.6 □ to obtain exam materials for free download □NSE5_FNC_AD_7.6 Latest Exam Preparation
- Valid NSE5_FNC_AD_7.6 Exam Test ✈ New NSE5_FNC_AD_7.6 Test Answers □ Valid NSE5_FNC_AD_7.6 Exam Pdf □ Search for 「 NSE5_FNC_AD_7.6 」 on ☀ www.pdfvce.com □☀□ immediately to obtain a free download □NSE5_FNC_AD_7.6 Online Test
- Reliable and Guarantee Refund of Fortinet NSE5_FNC_AD_7.6 Exam Questions □ The page for free download of □ NSE5_FNC_AD_7.6 □ on ✔ www.practicevce.com □✔□ will open immediately □Sample NSE5_FNC_AD_7.6 Questions Answers
- Test NSE5_FNC_AD_7.6 Dumps.zip □ NSE5_FNC_AD_7.6 Valid Exam Testking □ NSE5_FNC_AD_7.6 Dump Check □ Open website ➥ www.pdfvce.com □ and search for □ NSE5_FNC_AD_7.6 □ for free download □ □NSE5_FNC_AD_7.6 Valid Exam Testking
- NSE5_FNC_AD_7.6 Exam Questions in PDF Format □ Download { NSE5_FNC_AD_7.6 } for free by simply entering ⇛ www.dumpsquestion.com ⇚ website □NSE5_FNC_AD_7.6 Relevant Exam Dumps
- 100% Pass Quiz NSE5_FNC_AD_7.6 - Professional Fortinet NSE 5 - FortiNAC-F 7.6 Administrator Valid Exam Cram □ □ Search on □ www.pdfvce.com □ for ➡ NSE5_FNC_AD_7.6 □□□ to obtain exam materials for free download □ □NSE5_FNC_AD_7.6 Valid Exam Testking
- 100% Pass Quiz NSE5_FNC_AD_7.6 - Professional Fortinet NSE 5 - FortiNAC-F 7.6 Administrator Valid Exam Cram □ □ Search on ➽ www.troytecdumps.com □ for □ NSE5_FNC_AD_7.6 □ to obtain exam materials for free download □ □Test NSE5_FNC_AD_7.6 Dumps.zip
- Take NSE5_FNC_AD_7.6 Practice Exam Questions (Desktop - Web-Based) □ Open website { www.pdfvce.com } and search for ➤ NSE5_FNC_AD_7.6 □ for free download □NSE5_FNC_AD_7.6 Latest Exam Preparation
- NSE5_FNC_AD_7.6 Online Test □ Reliable NSE5_FNC_AD_7.6 Test Labs □ NSE5_FNC_AD_7.6 Online Test □ □ Download 【 NSE5_FNC_AD_7.6 】 for free by simply entering 【 www.verifieddumps.com 】 website □ □NSE5_FNC_AD_7.6 Reliable Exam Guide
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, 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, 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, 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, Disposable vapes