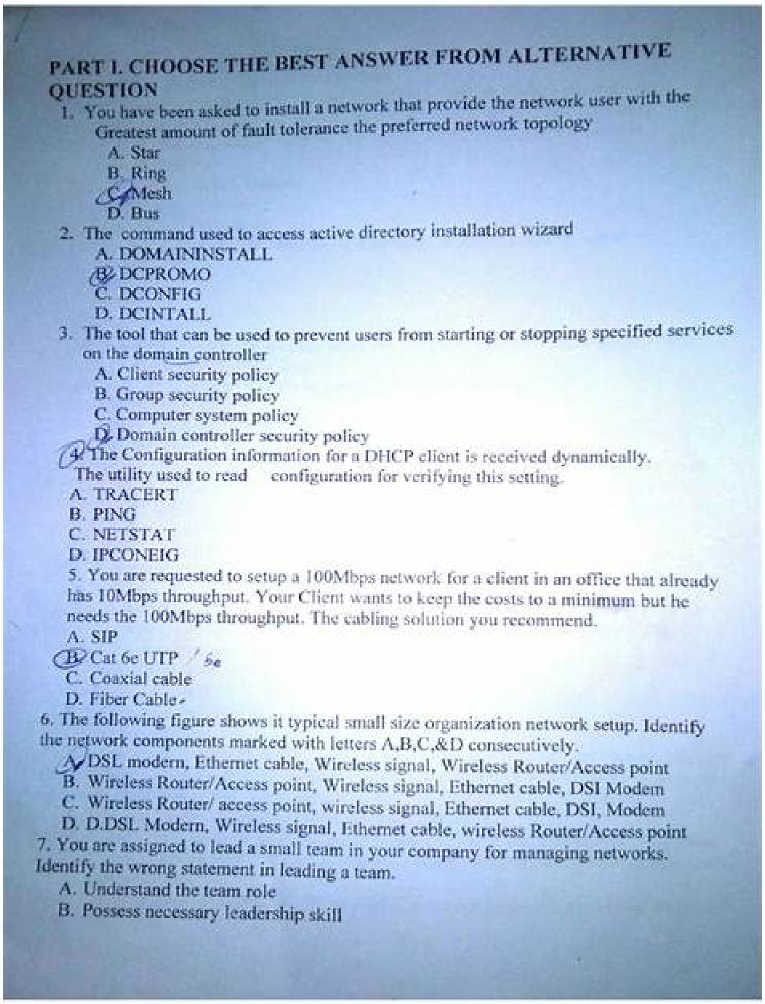
NSE5_FNC_AD_7.6 Training Material | Exam NSE5_FNC_AD_7.6 Outline



PART I. CHOOSE THE BEST ANSWER FROM ALTERNATIVE QUESTION

1. You have been asked to install a network that provide the network user with the Greatest amount of fault tolerance the preferred network topology
   A. Star
   B. Ring
   [✓ C. Mesh]
   D. Bus
2. The command used to access active directory installation wizard
   A. DOMAININSTALL
   [✓ B. DCPROMO]
   C. DCONFIG
   D. DCINTALL
3. The tool that can be used to prevent users from starting or stopping specified services on the domain controller
   A. Client security policy
   B. Group security policy
   C. Computer system policy
   [✓ D. Domain controller security policy]
4. The Configuration information for a DHCP client is received dynamically. The utility used to read configuration for verifying this setting.
   A. TRACERT
   B. PING
   C. NETSTAT
   D. IPCONEIG
5. You are requested to setup a 100Mbps network for a client in an office that already has 10Mbps throughput. Your Client wants to keep the costs to a minimum but he needs the 100Mbps throughput. The cabling solution you recommend.
   A. SIP
   [✓ B. Cat 6e UTP] / 5e
   C. Coaxial cable
   D. Fiber Cable
6. The following figure shows it typical small size organization network setup. Identify the network components marked with letters A,B,C,&D consecutively.
   [✓ A. DSL modern, Ethernet cable, Wireless signal, Wireless Router/Access point]
   B. Wireless Router/Access point, Wireless signal, Ethernet cable, DSI Modem
   C. Wireless Router/ access point, wireless signal, Ethernet cable, DSI, Modem
   D. D.DSL Modern, Wireless signal, Ethernet cable, wireless Router/Access point
7. You are assigned to lead a small team in your company for managing networks. Identify the wrong statement in leading a team.
   A. Understand the team role
   B. Possess necessary leadership skill

No doubt the Fortinet NSE 5 - FortiNAC-F 7.6 Administrator (NSE5_FNC_AD_7.6) certification is one of the most challenging certification exams in the market. This Fortinet NSE 5 - FortiNAC-F 7.6 Administrator (NSE5_FNC_AD_7.6) certification exam gives always a tough time to Fortinet NSE 5 - FortiNAC-F 7.6 Administrator (NSE5_FNC_AD_7.6) exam candidates. The PassReview understands this hurdle and offers recommended and real Fortinet NSE5_FNC_AD_7.6 Exam Practice questions in three different formats. These formats hold high demand in the market and offer a great solution for quick and complete Fortinet NSE 5 - FortiNAC-F 7.6 Administrator (NSE5_FNC_AD_7.6) exam preparation.

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.

Helpful Product Features of Fortinet NSE5_FNC_AD_7.6 Desktop Practice Exam Software

Our NSE5_FNC_AD_7.6 training guide boosts three versions which include PDF version, PC version and APP online version. The NSE5_FNC_AD_7.6 test guide is highly efficient and the forms of the answers and questions are the same. Different version boosts their own feature and using method, and the client can choose the most convenient method. For example, PDF format of NSE5_FNC_AD_7.6 Guide Torrent is printable and boosts instant access to download. You can learn at any time, and you can update the NSE5_FNC_AD_7.6 exam questions freely in any day of one year.

Fortinet NSE 5 - FortiNAC-F 7.6 Administrator Sample Questions (Q19-Q24):

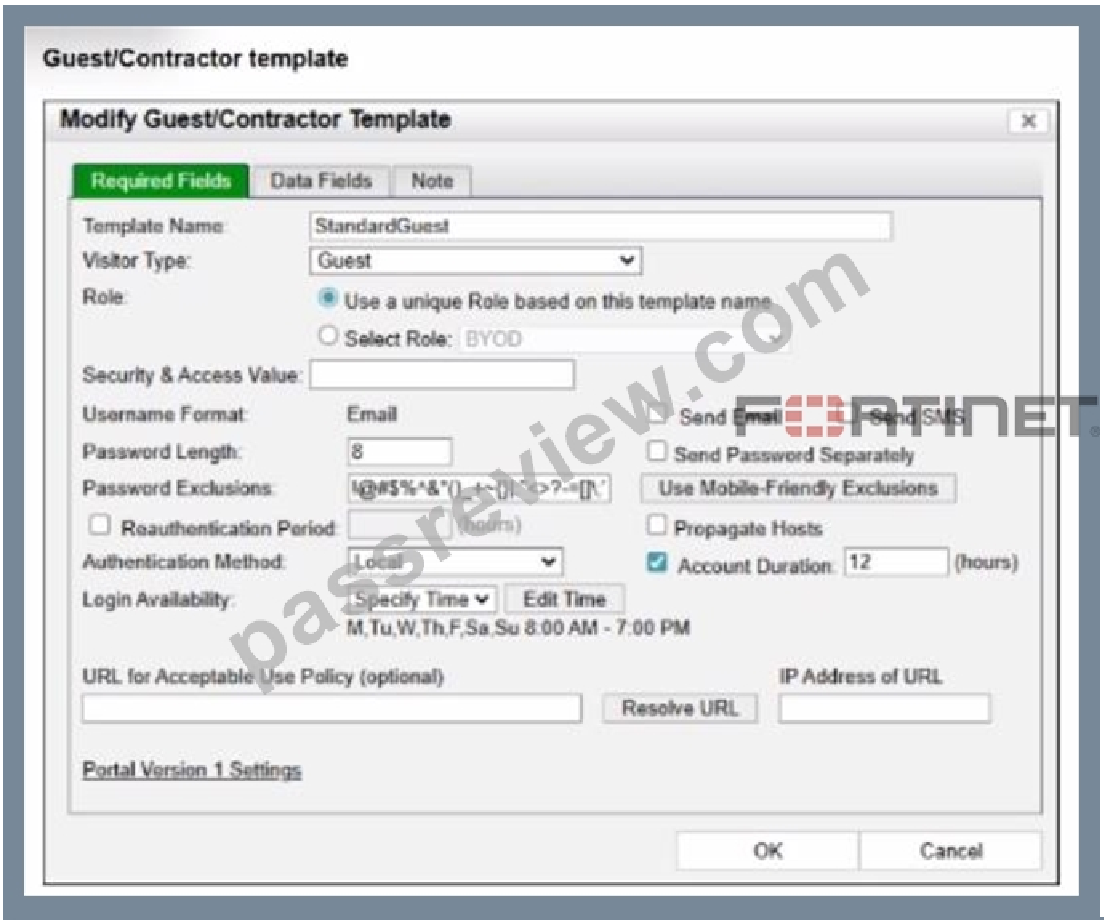
NEW QUESTION # 19
An administrator wants FortiNAC-F to return a group of user-defined RADIUS attributes in RADIUS responses.
Which condition must be true to achieve this?

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

Answer: D

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 # 20
Refer to the exhibits.



Guest/Contractor template

Modify Guest/Contractor Template

Template Name: StandardGuest

Visitor Type: Guest

Role: ● Use a unique Role based on this template name
○ Select Role: BYOD

Security & Access Value:

Username Format: Email ☐ Send Email ☐ Send SMS

Password Length: 8 ☐ Send Password Separately

Password Exclusions: !@#$%^&*()_+~{}|:"<>?-=[]\' Use Mobile-Friendly Exclusions

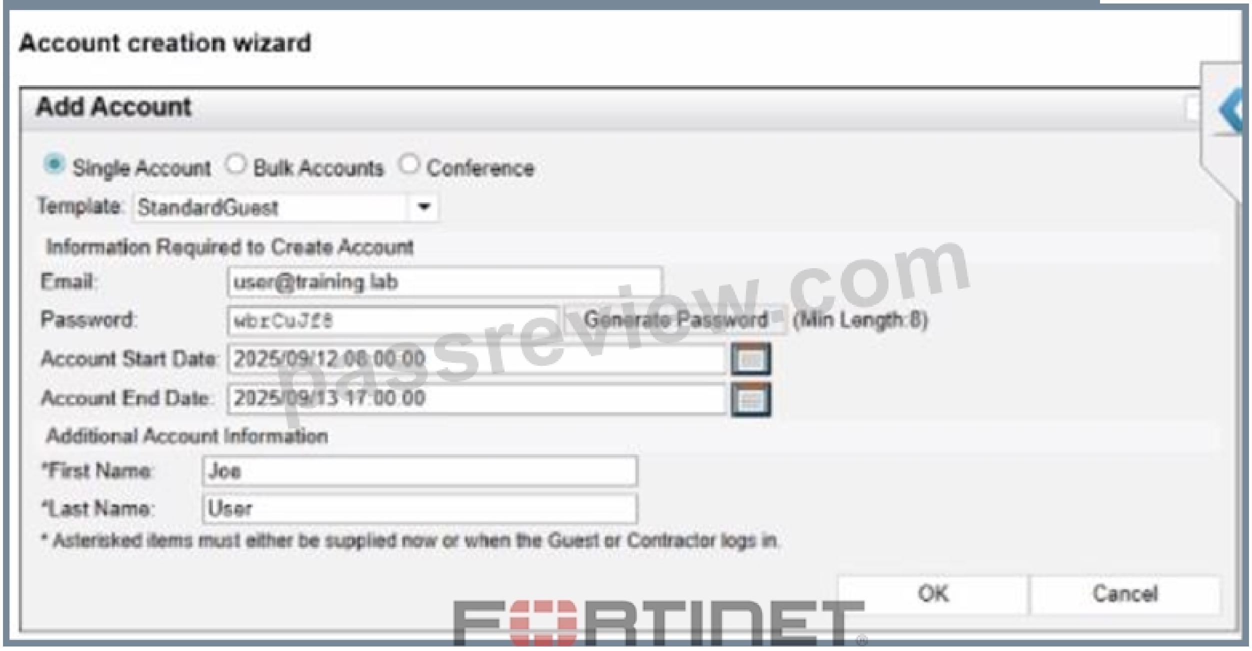
☐ Reauthentication Period: (hours) ☐ Propagate Hosts

Authentication Method: Local ☑ Account Duration: 12 (hours)

Login Availability: Specify Time Edit Time
M,Tu,W,Th,F,Sa,Su 8:00 AM - 7:00 PM

URL for Acceptable Use Policy (optional) Resolve URL IP Address of URL

Portal Version 1 Settings



Account creation wizard

Add Account

● Single Account ○ Bulk Accounts ○ Conference

Template: StandardGuest

Information Required to Create Account

Email: user@training.lab

Password: wbrCuJf8 Generate Password (Min Length:8)

Account Start Date: 2025/09/12 08:00:00

Account End Date: 2025/09/13 17:00:00

Additional Account Information

*First Name: Joe

*Last Name: User

* Asterisked items must either be supplied now or when the Guest or Contractor logs in.

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

Answer: A

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 # 21
How can an administrator configure FortiNAC-F to normalize incoming syslog event levels across vendors?

- A. Configure event to alarm mappings.
- B. Configure the security rule settings.
- C. Configure severity mappings.
- D. Configure the vendor OUI settings.

Answer: C

Explanation:
FortiNAC-F serves as a central manager for security events originating from a diverse ecosystem of third-party security appliances, such as FortiGate, Check Point, and Cisco. Each vendor utilizes its own internal scale for severity levels within syslog messages (e.g., Check Point uses a 1-5 scale, while others may use 0-7). To provide a consistent response regardless of the source, FortiNAC-F uses Severity Mappings to normalize these incoming values.
According to the FortiNAC-F Administration Guide, severity mappings allow the administrator to translate vendor-specific threat levels into standardized FortiNAC Security Levels (such as High, Medium, or Low Violation). When a syslog message arrives, the parser extracts the vendor's severity code, and the system immediately references the Security Event Severity Level Mappings table to determine how that event should be categorized internally. This normalization is vital because it allows a single Security Alarm to be configured to respond to any "High Violation" event, whether it was reported as a "Critical" by one vendor or a "Level 5" by another. Without these mappings, the administrator would have to create separate, redundant security rules for every vendor to account for their different naming conventions and numerical scales.
"Each vendor defines its own severity levels for syslog messages. The following table shows the equivalent FortiNAC security level... To normalize these events, configure the Severity Level Mappings found in the device integration guides. This allows FortiNAC to generate a consistent security event that can then trigger an alarm regardless of the reporting vendor's specific terminology." - FortiNAC-F Administration Guide: Vendor Severity Levels and Syslog Management.

NEW QUESTION # 22
When configuring FortiNAC-F to manage FortiGate VPN users, an endpoint compliance policy must be created for the integration. Why is the endpoint compliance policy necessary for this type of integration?

- A. To validate the VPN client being used
- B. To validate the VPN user credentials
- C. To confirm the installed endpoint certificate
- D. To designate the required agent type

Answer: D

Explanation:

The integration of FortiNAC-F with FortiGate VPN requires a specific policy workflow to bridge the gap between initial user authentication and full network access. When a user connects to the VPN, the FortiGate typically provides the User ID and IP address, but FortiNAC-F requires a MAC address to uniquely identify and manage the endpoint's record.
According to the FortiGate VPN Integration Guide, the Endpoint Compliance Policy is a mandatory component of this setup because it is used to designate the required agent type. Because a VPN connection is Layer 3, FortiNAC cannot "see" the MAC address through traditional SNMP or L2 polling. The compliance policy instructs the system to present a Captive Portal to the remote user, requiring them to download and run either the Persistent or Dissolvable Agent. The agent then reports the device's MAC address back to FortiNAC, allowing the system to correlate the VPN session with a host record.
Once the agent is running and the MAC is known, FortiNAC-F can evaluate the device's security posture (if scanning is configured) and send the necessary FSSO tags back to the FortiGate to lift the initial network restrictions. Without the compliance policy to enforce the agent requirement, the connection would remain in an isolated "IP-only" state with no unique hardware identity.
"The Endpoint Compliance Policy is necessary to control the agent requirement for VPN users. Create a default VPN Endpoint Compliance Policy to distribute an agent via captive portal for isolated machines. This policy allows the administrator to designate the required agent type (Persistent or Dissolvable) that will be used to collect the hardware (MAC) address and perform health scans on the remote endpoint." - FortiNAC FortiGate VPN Integration Guide: Default Endpoint Compliance Policy (Optional) Section.

NEW QUESTION # 23

An administrator manages a corporate environment where all users log into the corporate domain each time they connect to the network. The administrator wants to leverage login scripts to use a FortiNAC-F agent to enhance endpoint visibility Which agent can be deployed as part of a login script?

- A. Dissolvable
- B. Persistent
- C. Mobile
- D. Passive

Answer: B

Explanation:
In a corporate domain environment where "enhanced endpoint visibility" is required, the Persistent Agent is the recommended choice. Unlike the Dissolvable Agent, which is temporary and intended for one-time compliance scans during registration, the Persistent Agent is an "install-and-stay-resident" application.
The Persistent Agent is specifically designed to be distributed through automated enterprise methods, including login scripts, Group Policy Objects (GPO), or third-party software management tools. When deployed via a login script, the agent can be configured to silently install and immediately begin communicating with the FortiNAC-F service interface. Once active, it provides continuous visibility by reporting host details such as logged-on users, installed applications, and adapter information. It also listens for Windows session events (logon/logoff) to trigger automatic single-sign-on (SSO) registration in FortiNAC-F, ensuring that as soon as a user connects to the domain, their device is identified and assigned the correct network access policy.
"The Persistent Agent can be distributed to Windows domain machines via login script or by any other software distribution method your organization might use. The Persistent Agent remains installed on the host at all times. Once the agent is installed it runs in the background and communicates with FortiNAC at intervals established by the FortiNAC administrator." - FortiNAC-F Administration Guide: Persistent Agent Overview.

NEW QUESTION # 24

......

It is all due to the top features of Fortinet NSE 5 - FortiNAC-F 7.6 Administrator NSE5_FNC_AD_7.6 exam dumps. These features are three Fortinet NSE 5 - FortiNAC-F 7.6 Administrator exam questions formats, free exam dumps download facility, three months updated Salesforce NSE5_FNC_AD_7.6 exam dumps download facility, affordable price and 100 exams passing money back guarantee. All these Fortinet NSE 5 - FortiNAC-F 7.6 Administrator dumps features are designed to assist you in Fortinet NSE 5 - FortiNAC-F 7.6 Administrator NSE5_FNC_AD_7.6 Exam Preparation and enable you to pass the exam with flying colors.

Exam NSE5_FNC_AD_7.6 Outline: https://www.passreview.com/NSE5_FNC_AD_7.6_exam-braindumps.html

- NSE5_FNC_AD_7.6 Reliable Exam Pattern □ Test NSE5_FNC_AD_7.6 Discount Voucher □ Valid NSE5_FNC_AD_7.6 Study Notes □ Easily obtain { NSE5_FNC_AD_7.6 } for free download through ➠ www.practicevce.com □ □Valid NSE5_FNC_AD_7.6 Study Notes

- Certification NSE5_FNC_AD_7.6 Book Torrent □ NSE5_FNC_AD_7.6 Exam Simulator Free □ NSE5_FNC_AD_7.6 Latest Exam Notes □ Search for （NSE5_FNC_AD_7.6） and easily obtain a free download on ▷ www.pdfvce.com ◁ □NSE5_FNC_AD_7.6 Reliable Exam Pattern
- NSE5_FNC_AD_7.6 Valid Test Review □ NSE5_FNC_AD_7.6 Reliable Exam Pattern □ NSE5_FNC_AD_7.6 Exam Simulator Free □ Easily obtain free download of 「NSE5_FNC_AD_7.6」 by searching on ▷ www.examcollectionpass.com ◁ □Valid NSE5_FNC_AD_7.6 Exam Pass4sure
- To Prepare for the Fortinet Exam, Get Fortinet NSE5_FNC_AD_7.6 Dumps □ Easily obtain { NSE5_FNC_AD_7.6 } for free download through " www.pdfvce.com " □NSE5_FNC_AD_7.6 Latest Exam Labs
- Pass Guaranteed 2026 Useful Fortinet NSE5_FNC_AD_7.6: Fortinet NSE 5 - FortiNAC-F 7.6 Administrator Training Material □ Search for （NSE5_FNC_AD_7.6） and download it for free on ➥ www.dumpsmaterials.com □ website □NSE5_FNC_AD_7.6 Latest Exam Notes
- Take Your Exam Preparation to the Next Level with NSE5_FNC_AD_7.6 Web-Based Practice Test □ Simply search for □ NSE5_FNC_AD_7.6 □ for free download on 【 www.pdfvce.com 】 □NSE5_FNC_AD_7.6 Reliable Exam Pattern
- 100% Pass Quiz NSE5_FNC_AD_7.6 - Fantastic Fortinet NSE 5 - FortiNAC-F 7.6 Administrator Training Material □ Open 《 www.vceengine.com 》 enter ▶ NSE5_FNC_AD_7.6 ◀ and obtain a free download □New NSE5_FNC_AD_7.6 Test Sample
- Fortinet NSE5_FNC_AD_7.6 Practice Test Software for Desktop □ Download 【 NSE5_FNC_AD_7.6 】 for free by simply entering ➽ www.pdfvce.com □ website □NSE5_FNC_AD_7.6 Valid Test Review
- Customizable NSE5_FNC_AD_7.6 Exam Mode □ Reliable NSE5_FNC_AD_7.6 Exam Preparation □ NSE5_FNC_AD_7.6 Exam Simulator Free □ Open ➥ www.vce4dumps.com □ enter □ NSE5_FNC_AD_7.6 □ and obtain a free download □New NSE5_FNC_AD_7.6 Test Sample
- Fortinet NSE5_FNC_AD_7.6 Practice Test Software for Desktop □ Copy URL ⇛ www.pdfvce.com ⇚ open and search for ➤ NSE5_FNC_AD_7.6 □ to download for free □NSE5_FNC_AD_7.6 Pass4sure Study Materials
- New NSE5_FNC_AD_7.6 Test Sample □ NSE5_FNC_AD_7.6 Valid Test Review □ NSE5_FNC_AD_7.6 Latest Exam Notes □ Download ➡ NSE5_FNC_AD_7.6 □□□ for free by simply searching on ➽ www.vce4dumps.com □ ❣ Test NSE5_FNC_AD_7.6 Discount Voucher
- mpgimer.edu.in, demo.webdive.in, sseducationcenter.com, pct.edu.pk, hashnode.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.pmll.com.ng, pct.edu.pk, www.stes.tyc.edu.tw, Disposable vapes