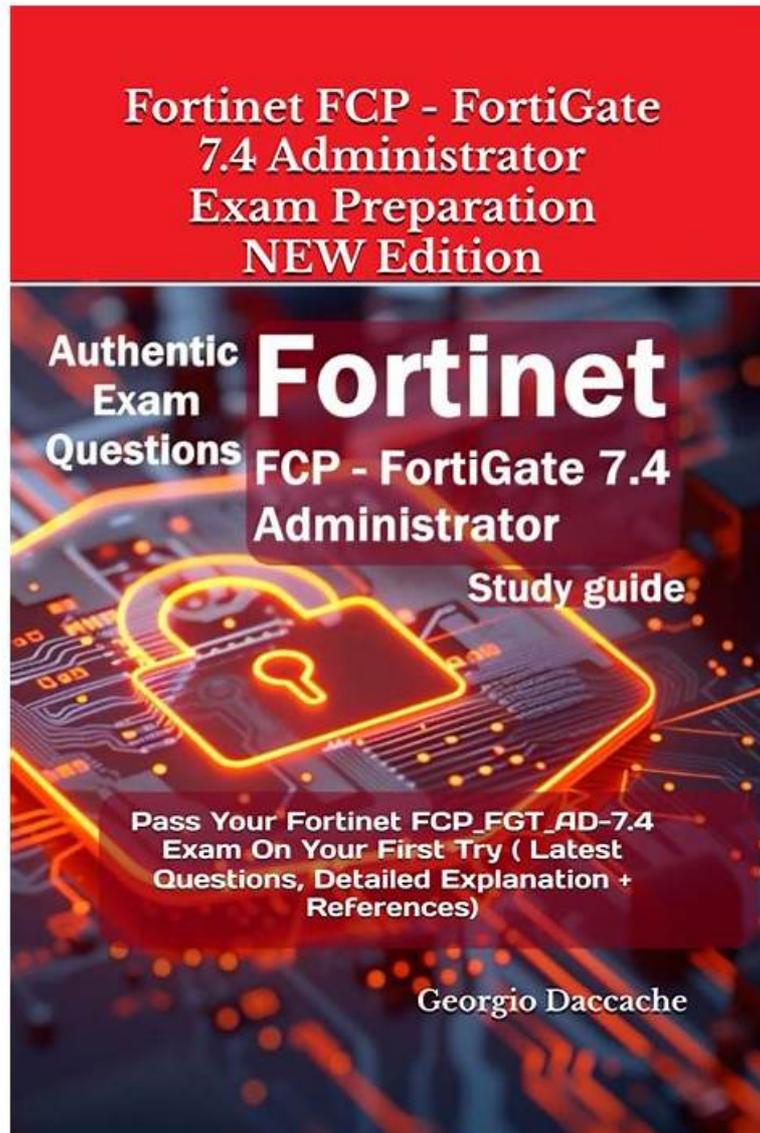


FCP_FCT_AD-7.4 Vce Exam, FCP_FCT_AD-7.4 Detailed Study Plan



DumpsQuestion can provide professional and high quality products. It is the industry leader in providing IT certification information. To select DumpsQuestion is to choose success. DumpsQuestion's Fortinet FCP_FCT_AD-7.4 Exam Training materials is your magic weapon to success. With it, you will pass the exam and achieve excellent results, towards your ideal place.

The web-based Fortinet FCP_FCT_AD-7.4 mock test is compatible with many systems. This version of the Fortinet FCP_FCT_AD-7.4 practice exam requires an active internet connection. It does not require any additional plugins or software installation to operate. Furthermore, others also support the FCP_FCT_AD-7.4 web-based practice exam. Features of the FCP_FCT_AD-7.4 desktop practice exam software are web-based as well.

>> FCP_FCT_AD-7.4 Vce Exam <<

FCP_FCT_AD-7.4 Detailed Study Plan | FCP_FCT_AD-7.4 Reliable Test Cram

You can save too much precious time because FCP_FCT_AD-7.4 actual dumps help you to prepare for the FCP_FCT_AD-7.4 certification tests in a very short time. Using DumpsQuestion FCP_FCT_AD-7.4 exam preparation material you will be aware of the

final Fortinet FCP_FCT_AD-7.4 exam pattern and the kind of FCP_FCT_AD-7.4 Exam Questions. Fortinet FCP_FCT_AD-7.4 valid dumps will remove your FCP_FCT_AD-7.4 exam fear and you will take the actual Fortinet FCP_FCT_AD-7.4 test with confidence. You will perform well in the FCP - FortiClient EMS 7.4 Administrator, FCP_FCT_AD-7.4 exam and produce the best results.

Fortinet FCP - FortiClient EMS 7.4 Administrator Sample Questions (Q21-Q26):

NEW QUESTION # 21

A company must integrate the FortiClient EMS with their existing identity management infrastructure for user authentication, and implement and enforce administrative access with multi-factor authentication (MFA).

Which two authentication methods can they use in this scenario? (Choose two answers)

- A. TACACS
- B. RADIUS
- C. SAML
- D. LDAPS

Answer: B,C

Explanation:

According to the FortiClient EMS 7.4 Administration Guide, for an organization to integrate with an identity management infrastructure while enforcing administrative access with Multi-Factor Authentication (MFA), the primary supported methods for remote administrator authentication are RADIUS and SAML.

1. RADIUS (Answer B)

* Identity Integration: FortiClient EMS allows administrators to add RADIUS servers as an authentication source under the Administration > Authentication Servers section.

* MFA Support: RADIUS is a standard protocol for enforcing MFA. In this scenario, FortiClient EMS acts as a RADIUS client to an external MFA provider (such as FortiAuthenticator, RSA Authentication Manager, or Duo).

* Workflow: When an administrator attempts to log in to the EMS console, EMS sends an Access-Request to the RADIUS server. If the provider requires MFA, it can challenge the user (via push notification or token code) before sending an Access-Accept back to EMS.

2. SAML (Answer D)

* Modern Identity Management: SAML (Security Assertion Markup Language) is the preferred method for integrating with modern cloud and on-premises Identity Providers (IdPs) like Microsoft Entra ID (formerly Azure AD), Okta, AD FS, or FortiAuthenticator.

* Native MFA Enforcement: By using SAML SSO, the authentication and MFA process are handled entirely by the IdP. The EMS server acts as the Service Provider (SP). When an admin logs in, they are redirected to the IdP, where the company's existing MFA policies (Conditional Access, etc.) are enforced before the user is granted access back to the EMS console.

* EMS Configuration: The curriculum details specific SAML SSO configurations for various IdPs under the SAML SSO section of the Administration Guide.

3. Why Other Options are Incorrect/Insufficient

* A. LDAPS: While FortiClient EMS supports importing users from Active Directory (AD DS) via LDAP

/LDAPS for endpoint management and basic admin login, standard LDAPS does not natively support or enforce an MFA challenge-response workflow in the same integrated way that RADIUS or SAML does for administrative console access.

* C. TACACS: TACACS+ is primarily used for device administration on networking equipment (like FortiGate) and is not a listed or standard method for administrative authentication within the FortiClient EMS software documentation.

NEW QUESTION # 22

An administrator installs FortiClient on Windows Server.

What is the default behavior of real-time protection control?

- A. Real-time protection is disabled
- B. Real-time protection must update AV signature database
- C. Real-time protection must update the signature database from FortiSandbox
- D. Real-time protection sends malicious files to FortiSandbox when the file is not detected locally

Answer: A

Explanation:

When FortiClient is installed on a Windows Server, the default behavior for real-time protection control is:

* Real-time protection is disabled:By default, FortiClient does not enable real-time protection on server installations to avoid potential performance impacts and because servers typically have different security requirements compared to client endpoints. Thus, real-time protection is disabled by default on Windows Server installations.

References

* FortiClient EMS 7.2 Study Guide, Real-time Protection Section

* Fortinet Documentation on FortiClient Default Settings for Server Installations

NEW QUESTION # 23

A FortiClient EMS administrator has enabled the compliance rule for the sales department Which Fortinet device will enforce compliance with dynamic access control?

- A. FortiGate
- B. FortiClient
- C. FortiAnalyzer
- D. FortiClient EMS

Answer: A

Explanation:

* Understanding Compliance Rules:

* The compliance rule for the sales department needs to be enforced dynamically.

* Enforcing Compliance:

* FortiGate is responsible for enforcing compliance by integrating with FortiClient EMS to apply dynamic access control based on compliance status.

* Conclusion:

* The Fortinet device that will enforce compliance with dynamic access control is the FortiGate.

References:

Compliance and enforcement documentation from FortiGate and FortiClient EMS study guides.

NEW QUESTION # 24

Which two statements about ZTNA destinations are true? (Choose two.)

- A. FortiClient ZTNA destination authentication is enabled by default.
- B. FortiClient ZTNA destinations use an existing VPN tunnel to create a secure connection.
- C. FortiClient ZTNA destination encryption is disabled by default.
- D. FortiClient ZTNA destinations provides access through TCP forwarding.
- E. FortiClient ZTNA destinations do not support a wildcard FQDN.

Answer: C,E

NEW QUESTION # 25

Which statement about the FortiClient enterprise management server is true?

- A. It provides centralized management of multiple endpoints running FortiClient software.
- B. It receives the configuration information of endpoints from FortiGate.
- C. It enforces compliance on the endpoints using tags
- D. It receives the CA certificate from FortiGate to validate client certificates.

Answer: C

NEW QUESTION # 26

.....

With the high pass rate as 98% to 100%, we can proudly claim that we are unmatched in the market for our accurate and latest FCP_FCT_AD-7.4 exam dumps. You will never doubt about our strength on bringing you success and the according FCP_FCT_AD-7.4 Certification that you intent to get. We have testified more and more candidates' triumph with our

