

Book FCP_FSA_AD-5.0 Free | FCP_FSA_AD-5.0 Exam PDF



FCP_FSA_AD-5.0 exam tests are a high-quality product recognized by hundreds of industry experts. Over the years, FCP_FSA_AD-5.0 exam questions have helped tens of thousands of candidates successfully pass professional qualification exams, and help them reach the peak of their career. It can be said that FCP_FSA_AD-5.0 test guide is the key to help you open your dream door. We have enough confidence in our products, so we can give a 100% refund guarantee to our customers. FCP_FSA_AD-5.0 Exam Questions promise that if you fail to pass the exam successfully after purchasing our product, we are willing to provide you with a 100% full refund.

ITdumpsfree FCP - FortiSandbox 5.0 Administrator (FCP_FSA_AD-5.0) practice test material covers all the key topics and areas of knowledge necessary to master the Fortinet Certification Exam. Experienced industry professionals design the FCP_FSA_AD-5.0 exam questions and are regularly updated to reflect the latest changes in the FCP - FortiSandbox 5.0 Administrator (FCP_FSA_AD-5.0) exam. In addition, ITdumpsfree offers three different formats of practice material which are discussed below.

>> **Book FCP_FSA_AD-5.0 Free** <<

FCP_FSA_AD-5.0 Exam PDF, Simulated FCP_FSA_AD-5.0 Test

You only need 20-30 hours to learn our FCP_FSA_AD-5.0 test braindumps and then you can attend the exam and you have a very high possibility to pass the exam. For many people whether they are the in-service staff or the students they are busy in their job, family lives and other things. But you buy our FCP_FSA_AD-5.0 prep torrent you can mainly spend your time energy and time on your job, the learning or family lives and spare little time every day to learn our FCP - FortiSandbox 5.0 Administrator exam torrent. Our answers and questions are compiled elaborately and easy to be mastered. Because our FCP_FSA_AD-5.0 Test Braindumps are highly efficient and the passing rate is very high you can pass the exam fluently and easily with little time and energy needed.

Fortinet FCP - FortiSandbox 5.0 Administrator Sample Questions (Q22-Q27):

NEW QUESTION # 22

There is a connectivity problem between FortiSandbox and the FortiGuard distribution servers. You observe that a firewall located

between FortiSandbox and the internet allows traffic on ports TCP/4443, UDP/8888, and UDP/53. What is the cause of the issue? (Choose one answer)

- A. They must allow UDP 443 out
- B. They must allow TCP 8890 out
- C. They must allow UDP 514 out
- **D. They must allow TCP 443 out**

Answer: D

Explanation:

From the Deployment and System Settings lesson, the Study Guide states:

"The test-network command checks FortiGuard services as its last set of validation tests. These include the FortiGuard distribution network (FDN) accessibility, FDN contract expiration, web filtering service, and the community cloud service. All these FortiGuard services should be reachable and valid for FortiSandbox to be effective."

"The diagnose-debug fldn command provides details around FortiSandbox and the FortiGuard Distribution Network (FDN) communication and updates." FortiGuard Distribution Network (FDN) communication requires TCP/443 for HTTPS-based update and licensing communication. The current firewall rules allow TCP/4443 (API/management), UDP/8888 (FortiGuard queries), and UDP/53 (DNS), but TCP/443 is missing - which is the standard port required for FortiGuard FDN connectivity and license validation.

NEW QUESTION # 23

When configuring wildcard administrator authentication, which two account types can you use? (Choose two answers)

- **A. LDAP**
- B. TACACS
- C. Local
- **D. RADIUS**

Answer: A,D

Explanation:

From the Deployment and System Settings lesson, the Study Guide explicitly states:

"The default administrator account has a blank password. You should change this as soon as possible for all Fortinet devices. Aside from local accounts, FortiSandbox also supports LDAP, SAML SSO, and RADIUS." This confirms the supported remote authentication types for FortiSandbox administrator accounts are:

LDAP (Option A) ✓

RADIUS (Option B) ✓

SAML SSO (not listed as an option)

TACACS (Option C) and Local (Option D) are not listed as wildcard administrator authentication types in the Study Guide. Local accounts are standard administrator accounts, not wildcard authentication, and TACACS is not mentioned as a supported authentication method.

NEW QUESTION # 24

You are asked to create some custom VMs to better represent your security environment. In which two FortiSandbox deployments is this supported? (Choose two answers)

- A. Azure non-nested mode
- B. FortiSandbox Cloud
- **C. Private cloud**
- **D. Device-based**

Answer: C,D

Explanation:

From the Scanning and Rating Components lesson, the Study Guide explicitly states:

"FortiSandbox allows you to modify the number of CPUs and memory assigned to a custom VM. This feature is supported on hardware models and private cloud VMs." Hardware models = Device-based (Option C) Private cloud VMs = Private cloud (Option A) Azure non-nested mode and FortiSandbox Cloud do not support custom VM creation as per the Study Guide.

NEW QUESTION # 25

Refer to the CLI configuration below.

```
set device-authorization -a
```

How will FortiSandbox authorize new FortiClient devices after this command? (Choose one answer)

- A. When a new FortiClient registers, it inherits authorization status from the managing EMS or FortiGate.
- B. When a new device other than FortiClient registers, FortiSandbox will authorize it automatically.
- **C. When a new FortiClient registers, FortiSandbox will authorize it automatically.**
- D. When a Fabric device is not authorized, FortiSandbox will authorize it automatically.

Answer: C

Explanation:

The Study Guide explains the default behavior first: "You must authorize FortiClient EMS on FortiSandbox. FortiSandbox automatically authorizes all FortiClient endpoints managed by an authorized FortiClient EMS." It then adds the key point for this question: "To change the default FortiClient authorization behavior, use the command shown on this slide to authorize FortiClient endpoints using FortiSandbox CLI. By default, FortiClient inherits its authorization status from the managing EMS or FortiGate." Because the question specifically shows the CLI command `set device-authorization -a`, it is asking about the behavior after changing the default. The default inheritance model described in option A applies before the override. After this command, FortiSandbox is set to authorize FortiClient endpoints directly and automatically, which makes C the correct answer. Option B is incorrect because the command is specifically about FortiClient endpoints, not other devices in general. Option D is too broad and does not match the Study Guide's explanation, which is limited to FortiClient authorization behavior.

NEW QUESTION # 26

How can you limit an administrator's access to scan jobs on FortiSandbox based on the system that submitted the scan request? (Choose one answer)

- A. By configuring device groups to assign to users
- **B. By configuring administrator profiles that define job access**
- C. By configuring access in the log server configuration settings
- D. By configuring netshare groups to define access

Answer: B

Explanation:

The correct answer is B. The Study Guide states that FortiSandbox has default administrative profiles and specifically says: "The Read Only profile is intended to be used for system-wide monitoring and reporting tasks, whereas the Device profile is intended to be used for monitoring alerts and reporting for a specific device." That wording directly matches the question requirement to limit access based on the system that submitted the scan request. In other words, FortiSandbox uses administrator profiles to control whether an admin can view broad system-wide activity or only jobs and alerts related to a specific submitting device. This eliminates the other options. The Study Guide does not describe device groups, log server settings, or netshare groups as the mechanism for restricting admin visibility of scan jobs by submitter. Instead, access control is tied to the admin profile model. The Device profile is the exact fit because it narrows monitoring and reporting to a particular device context rather than the entire system. Therefore, the way to limit an administrator's access to scan jobs by the submitting system is by configuring administrator profiles that define job access.

NEW QUESTION # 27

.....

The pass rate is 98.65% for FCP_FSA_AD-5.0 study guide, and you can pass the exam just one time. In order to build up your confidence for the exam, we are pass guarantee and money back guarantee. If you fail to pass the exam by using FCP_FSA_AD-5.0 exam braindumps of us, we will give you full refund. Besides, FCP_FSA_AD-5.0 learning materials are edited and verified by professional specialists, and therefore the quality can be guaranteed, and you can use them at ease. We have online and offline service. If you have any questions for FCP_FSA_AD-5.0 Exam Materials, you can consult us, and we will give you reply as quick as possible.

FCP_FSA_AD-5.0 Exam PDF: https://www.itdumpsfree.com/FCP_FSA_AD-5.0-exam-passed.html

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.spatial.io, thehvacademy.com, Disposable vapes