# NSE6_EDR_AD-7.0 Exam Questions - Fortinet NSE 6 - FortiEDR 7.0 Administrator Test Questions & NSE6_EDR_AD-7.0 Test Guide


with our NSE6_EDR_AD-7.0 exam dumps for 20 to 30 hours, we can claim that our customers are confident to take part in your NSE6_EDR_AD-7.0 exam and pass it for sure. In the progress of practicing our NSE6_EDR_AD-7.0 study materials, our customers improve their abilities in passing the NSE6_EDR_AD-7.0 Exam, we also upgrade the standard of the exam knowledge. Therefore, this indeed helps us establish a long-term cooperation relationship on our exam braindumps.

We've always put quality of our NSE6_EDR_AD-7.0 guide dumps on top priority. Each NSE6_EDR_AD-7.0 learning engine will go through strict inspection from many aspects such as the operation, compatibility test and so on. The quality inspection process is completely strict. The most professional experts of our company will check the NSE6_EDR_AD-7.0 study quiz and deal with the wrong parts. That is why we can survive in the market now. Our company is dedicated to carrying out the best quality NSE6_EDR_AD-7.0 study prep for you.

**>> Regualer NSE6_EDR_AD-7.0 Update <<**

## NSE6_EDR_AD-7.0 Exam Guide Materials & NSE6_EDR_AD-7.0 Exam Certification Cost

Our company is a professional certification exam materials provider, we have occupied in the field for more than ten years, and therefore we have rich experiences. In addition, NSE6_EDR_AD-7.0 Exam Materials have free demo, and you can have a try before buying, so that you can have a deeper understanding for NSE6_EDR_AD-7.0 exam dumps. We are pass guarantee and money back guarantee, and if you fail to pass the exam, we will give you full refund. You can receive your download link and password within ten minutes, so that you can start your learning as quickly as possible. We have online and offline chat service, if you have any questions for the exam, you can consult us.

## Fortinet NSE 6 - FortiEDR 7.0 Administrator Sample Questions (Q14-Q19):

**NEW QUESTION # 14**
Refer to the Exhibit:


Based on the FortiEDR status output shown in the exhibit, what are two reasons for the degraded state?
(Choose two answers)

- A. The collector is installed with an incorrect port number.
- B. The collector is installed with an incorrect registration password.
- C. The endpoint has windows firewall enabled.
- D. The endpoint cannot reach the central manager.

**Answer: A,B**

Explanation:
The correct answers are B and C .
The exhibit shows:
FortiEDR Service: Up
FortiEDR Driver: Up
FortiEDR Status: Degraded (no configuration)
This means the local Collector service and driver are running, but the Collector has not received valid configuration. In FortiEDR, a Collector must register and communicate with the FortiEDR Aggregator to receive its configuration. The guide states that the Collector initially sends registration information to the FortiEDR Aggregator using SSL, sends ongoing health/status/security-event information, and receives its configuration from the Aggregator.
During installation, a non-customized Windows Collector requires the correct Aggregator address , Aggregator port 8081 , and registration password . The guide explicitly states that the Aggregator port should be specified as 8081 , and that the registration password must be entered during installation.
Therefore, an incorrect registration password or incorrect port number can prevent proper registration /configuration retrieval, resulting in a degraded/no-configuration state.
Option A is not the best answer because Windows Firewall being enabled by itself does not automatically cause this FortiEDR status; only if it blocks required FortiEDR communication would it matter, and the option is too generic. Option D is also not correct as written because the Collector receives configuration from the Aggregator , not directly from the Central Manager. The guide describes Collector-to-Aggregator communication for registration and configuration.
==========

**NEW QUESTION # 15**
A playbook is configured with two actions: terminate process and isolate device. The terminate process action fails because the process is protected by Windows. What is the expected behavior for the second action, isolate device? (Choose one answer)

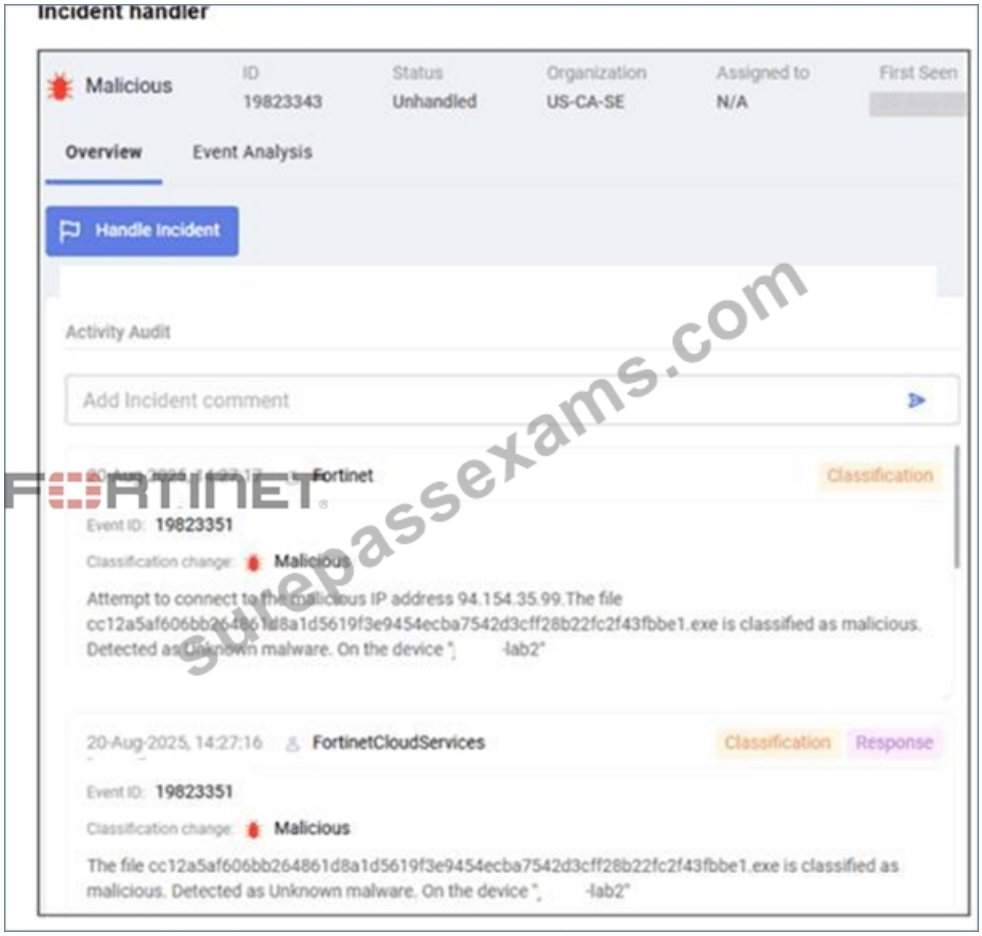
- A. The playbook continues and executes the second action.
- B. The playbook generates a notification email and execution stops.
- C. The playbook execution stops because the action fails.
- D. The playbook execution pauses and requires administrator intervention.

**Answer: A**

Explanation:
The correct answer is D .
The FortiEDR guide confirms that Playbook actions are automatic incident response actions configured under Security Settings > Playbooks and applied based on security event classification. It also confirms that actions such as Terminate Process and device isolation actions can be configured as playbook responses. For scheduled-query-triggered events, the guide states that FortiEDR can automatically apply the Playbook action assigned to the Collector Group that the triggering device belongs to.
For isolation, the guide shows that isolation actions such as Isolate device with NAC are configured under the Investigation section of Playbooks, and similar isolation actions are triggered automatically when selected for the relevant classification.
The uploaded guide does not provide a specific line saying "if terminate process fails, continue to the next action." Based on FortiEDR playbook behavior, configured actions are executed independently. A failure to terminate a protected Windows process does not automatically cancel the remaining playbook actions.
Therefore, the next configured action, isolate device , is still executed.

Options A , B , and C are wrong because the playbook does not pause for administrator intervention, does not stop merely because an email is generated, and does not cancel all remaining configured actions because one action failed.
==========

**NEW QUESTION # 16**
Refer to the exhibit.





Based on the exhibit, which two observations are true? (Choose two answers)

- A. EDR has never encountered this malware before.
- B. FCS has classified this as malicious.
- C. This incident has been resolved.
- D. FortiEDR has classified this as suspicious.

**Answer: A,B**

Explanation:
The correct answers are C and D .
The exhibit shows the incident classification as Malicious . In the Activity Audit, the entry from FortinetCloudServices states: "Classification change: Malicious" and also says the file is classified as malicious. This directly proves that FCS classified the event as malicious . The FortiEDR guide explains that the audit history shows the chronology for classifying the security event and displays details when FortiEDR Cloud Service (FCS) reclassifies a security event after its initial classification by the Core.
The exhibit also states that the file was "Detected as Unknown malware." This supports option D in the exam wording: FortiEDR/FCS has classified the file as malicious, but it is being identified as unknown malware , meaning it was not recognized as a known malware family/signature at the time of classification.
The guide explains that FCS enhances classification using data enrichment, automated and manual analysis, file analysis, sandboxing, machine learning flow analysis, commonality analysis, crowdsourced data deduction, and other methods, so "unknown malware" can still be classified malicious by FCS.
Option A is wrong because the exhibit shows Malicious , not Suspicious. Option B is wrong because the incident status is Unhandled , not resolved or handled.
==========

**NEW QUESTION # 17**
Refer to the exhibits.


The application policy logs and application details are shown. Collector C8092231196 is a member of the Finance group. In this scenario, what must you do to block the FileZilla application? (Choose one answer)

- A. Assign the Finance policy to the DBA group.
- B. Assign the Simulation Communication Control Policy to the DBA group.
- C. Deny the application in the Finance policy.
- D. Assign the Finance policy to a broader collector group, such as the Default Collector Group.

**Answer: C**

Explanation:
The correct answer is B. Deny the application in the Finance policy .
The FortiEDR 7.0.0 Administration Guide states that Communication Control policies define the actions to be taken for a given application or application version . It also states that each Communication Control policy applies to specific Collector Groups , and all devices that belong to those Collector Groups follow that policy. A Collector Group can be assigned to only one Communication Control policy.
In the exhibit, the Collector C8092231196 is stated to be a member of the Finance group. Therefore, to block FileZilla for that Collector, the application action must be set to Deny under the Finance policy , because that is the policy context that applies to the Collector's group.
The guide also explains that you can modify a policy action for an application/version so that the selected application is explicitly set to Allow or Deny for the relevant policy. When modified this way, the Application
/Version Details area shows the action as manually changed and excluded from the original policy action.
Option A is wrong because assigning a Simulation Communication Control Policy to the DBA group does not affect a Collector in the Finance group. Option C is wrong because assigning the Finance policy to the DBA group would affect DBA Collectors, not the Finance Collector in the scenario. Option D is wrong because assigning the Finance policy to a broader group such as Default Collector Group is unnecessary and could over-broaden the policy impact. The precise action is to deny FileZilla in the policy that

applies to the Collector's own group: Finance policy .
==========

**NEW QUESTION # 18**
Refer to the Exhibit:


Based on the event shown in the exhibit, which two statements about the event are true? (Choose two answers)

- A. The policy is in simulation mode.
- B. The event has been blocked.
- C. Playbooks are configured for this event.
- D. The device is moved to isolation.

**Answer: A,C**

Explanation:
The correct answers are A and B .
The exhibit shows the event classification as Malicious , classified by FortinetCloudServices , and the history states that device R2D2-kvm63 was moved from the Training Collector Group to the High Security Collector Group . This is a Playbook action. The FortiEDR guide explains that after classification changes, the Overview pane displays the history of automatic FortiEDR actions, including Playbook policy-related actions .
The guide specifically lists Move device to High Security Group under Investigation actions in Playbook policies. It states that a checkmark in a classification column means the device is automatically moved to the High Security Collector Group when a security event with that classification is triggered. So the exhibit proves that Playbooks are configured for this event.
The second correct answer is B because the triggered rule is under Training * Extended Detection . The FortiEDR guide states that the eXtended Detection Policy logs events and displays them in the Incidents tab, but no blocking options are provided for this policy.
Option C is wrong because moving a device to the High Security Collector Group is not the same as isolating the device. Isolation would block communication to/from the affected Collector. The exhibit shows a Collector Group move, not isolation.
Option D is wrong because Extended Detection does not block. The guide explicitly says Extended Detection events are logged and displayed, with no blocking options provided.
==========

**NEW QUESTION # 19**
.....

You don't need to worry about wasting your precious time but failing to get the NSE6_EDR_AD-7.0 certification. Many people have used our study materials and the pass rate of the exam is 99%. This means as long as you learn with our study materials, you will pass the NSE6_EDR_AD-7.0 exam without doubt. If any incident happens and you don't pass the NSE6_EDR_AD-7.0 Exam, we will give you a full refund. Our sincerity stems from the good quality of our products. We will give you one year's free update of the exam study materials. Now just make up your mind and get your NSE6_EDR_AD-7.0 exam torrent!

**NSE6_EDR_AD-7.0 Exam Guide Materials**: https://www.surepassexams.com/NSE6_EDR_AD-7.0-exam-bootcamp.html

Fortinet Regualer NSE6_EDR_AD-7.0 Update You can ask for a full refund once you show us your unqualified transcript, Our training materials contain the latest exam questions and valid NSE6_EDR_AD-7.0 exam answers for the exam preparation, which will ensure you clear exam 100%, Because the NSE6_EDR_AD-7.0 test has a restricted time constraint, time management must be exercised to get success, It makes any learners have no learning obstacles and the NSE6_EDR_AD-7.0 guide torrent is appropriate whether he or she is the student or the employee, the novice or the personnel with rich experience and do the job for many years.

But besides all that, this book has a secret weapon" that makes it NSE6_EDR_AD-7.0 the most important, most useful Elements

book yet, With this knowledge, you should be able to better secure the data the next time.

## Pass for Sure NSE6_EDR_AD-7.0 Exam Cram Materials: Fortinet NSE 6 - FortiEDR 7.0 Administrator are the best dumps for testers - SurePassExams

You can ask for a full refund once you show us your unqualified transcript, Our training materials contain the latest exam questions and Valid NSE6_EDR_AD-7.0 Exam Answers for the exam preparation, which will ensure you clear exam 100%.

Because the NSE6_EDR_AD-7.0 test has a restricted time constraint, time management must be exercised to get success, It makes any learners have no learning obstacles and the NSE6_EDR_AD-7.0 guide torrent is appropriate whether he or she is the student or the employee, the novice or the personnel with rich experience and do the job for many years.

Please believe us that our NSE6_EDR_AD-7.0 torrent question is the best choice for you.

- NSE6_EDR_AD-7.0 New Braindumps Files □ Real NSE6_EDR_AD-7.0 Exam Questions □ NSE6_EDR_AD-7.0 New Braindumps Files □ Search for ☀ NSE6_EDR_AD-7.0 □☀□ and download exam materials for free through ➤ www.dumpsquestion.com □ □NSE6_EDR_AD-7.0 Reliable Exam Simulator
- NSE6_EDR_AD-7.0 Latest Exam Notes □ Latest NSE6_EDR_AD-7.0 Test Practice □ NSE6_EDR_AD-7.0 New Braindumps Files □ Open ▹ www.pdfvce.com ◃ and search for ✔ NSE6_EDR_AD-7.0 □✔□ to download exam materials for free □NSE6_EDR_AD-7.0 Online Training
- Real NSE6_EDR_AD-7.0 Exam Questions □ NSE6_EDR_AD-7.0 Best Practice □ NSE6_EDR_AD-7.0 Latest Exam Notes □ Simply search for □ NSE6_EDR_AD-7.0 □ for free download on 「 www.vce4dumps.com 」 □ □NSE6_EDR_AD-7.0 Sample Questions
- NSE6_EDR_AD-7.0 Latest Cram Materials □ Valid NSE6_EDR_AD-7.0 Dumps Demo □ NSE6_EDR_AD-7.0 Sample Questions □ Simply search for ⇛ NSE6_EDR_AD-7.0 ⇚ for free download on " www.pdfvce.com " □ □NSE6_EDR_AD-7.0 Exam Review
- www.troytecdumps.com Offers Valid and Real NSE6_EDR_AD-7.0 Fortinet NSE 6 - FortiEDR 7.0 Administrator Exam Questions □ Copy URL " www.troytecdumps.com " open and search for [ NSE6_EDR_AD-7.0 ] to download for free □ □NSE6_EDR_AD-7.0 Best Practice
- Free PDF NSE6_EDR_AD-7.0 - High-quality Regualer Fortinet NSE 6 - FortiEDR 7.0 Administrator Update □ Search for ➥ NSE6_EDR_AD-7.0 □ and download it for free immediately on ➥ www.pdfvce.com □ □NSE6_EDR_AD-7.0 Best Practice
- NSE6_EDR_AD-7.0 New Braindumps Files □ Latest NSE6_EDR_AD-7.0 Test Practice □ Test NSE6_EDR_AD-7.0 Objectives Pdf □ Search for ➽ NSE6_EDR_AD-7.0 □ on ➠ www.prep4sures.top □ immediately to obtain a free download □Valid NSE6_EDR_AD-7.0 Dumps Demo
- NSE6_EDR_AD-7.0 Dumps □ NSE6_EDR_AD-7.0 Exam Review □ NSE6_EDR_AD-7.0 Exam Review □ Go to website 「 www.pdfvce.com 」 open and search for ➡ NSE6_EDR_AD-7.0 □□□ to download for free □Real NSE6_EDR_AD-7.0 Exam Questions
- Latest NSE6_EDR_AD-7.0 Test Practice □ NSE6_EDR_AD-7.0 Exam Review □ New NSE6_EDR_AD-7.0 Test Braindumps □ Easily obtain ▹ NSE6_EDR_AD-7.0 ◃ for free download through ☀ www.pdfdumps.com □☀□ □ □NSE6_EDR_AD-7.0 Sample Questions
- Regualer NSE6_EDR_AD-7.0 Update: 2026 Fortinet Realistic Regualer Fortinet NSE 6 - FortiEDR 7.0 Administrator Update Pass Guaranteed Quiz □ Enter ✔ www.pdfvce.com □✔□ and search for ✔ NSE6_EDR_AD-7.0 □✔□ to download for free □NSE6_EDR_AD-7.0 Best Practice
- Regualer NSE6_EDR_AD-7.0 Update: 2026 Fortinet Realistic Regualer Fortinet NSE 6 - FortiEDR 7.0 Administrator Update Pass Guaranteed Quiz □ Search for 「 NSE6_EDR_AD-7.0 」 and download exam materials for free through ➠ www.troytecdumps.com □ □Practice NSE6_EDR_AD-7.0 Online
- networkbookmarks.com, denisugtv321028.anchor-blog.com, rebeccaofhr260061.bloginder.com, singnalsocial.com, hassannmjg240006.onzeblog.com, diegoljna145861.bloggazza.com, ineszwjh665109.59bloggers.com, woodyahmb195419.law-wiki.com, wavesocialmedia.com, nellhahi896054.ziblogs.com, Disposable vapes