

# IT 认证电子书



质 量 更 高 服 务 更 好

半年免费升级服务

<http://www.itrenzheng.com>

**Exam : NSE5\_FCT-6.2**

**Title : Fortinet NSE 5 - FortiClient  
EMS 6.2**

**Version : DEMO**

1.Refer to the exhibit.

The screenshot displays the FortiClient configuration interface for endpoint protection. It shows two rules configured for Windows endpoints. The first rule, 'Running Process', is set to 'Required' and specifically targets 'Calculator.exe'. The second rule, 'Vulnerable Devices', is set to 'Medium' severity. Both rules are assigned to 'All' endpoints and are tagged under 'Sales Department Compliance'.

Rule Name	Type	Rule	Running Process	Severity Level	Assign to	Tag endpoint as
Running Process	Windows	Running Process	Required Calculator.exe		All	Sales Department Compliance
Vulnerable Devices	Windows	Vulnerable Devices		Medium	All	Sales Department Compliance

Based on the settings shown in the exhibit, which two actions must the administrator take to make the endpoint compliant? (Choose two)

- A. Integrate FortiSandbox for infected file analysis.
- B. Enable the webfilter profile
- C. Patch applications that have vulnerability rated as high or above.
- D. Run Calculator application on the endpoint.

**Answer:** C,D

2.What action does FortiClient anti-exploit detection take when it detects exploits?

- A. Terminates the compromised application process
- B. Patches the compromised application process
- C. Blocks memory allocation to the compromised application process
- D. Deletes the compromised application process



**Answer:** A

3.Refer to the exhibits.

## Security Fabric Settings

☒ FortiGate TelemetrySecurity Fabric role **Serve as Fabric Root** Join Existing Fabric



Fabric name Fabric

Topology  FGVM010000052731 (Fabric Root)Allow other FortiGates to join ☒  port3 Pre-authorized FortiGates None  EditSAML Single Sign-On  ☐Management IP/FQDN  **Use WAN IP** SpecifyManagement Port **Use Admin Port** Specify☒ FortiAnalyzer Logging

IP address 10.0.1.250

Test Connectivity

Logging to ADOM root

Storage usage  0% 144.55 MiB / 50.00 GiBAnalytics usage  0% 91.02 MiB / 35.00 GiB

(Number of days stored: 55/60)

Archive usage  0% 53.53 MiB / 15.00 GiB

(Number of days stored: 54/365)

Upload option  **Real Time** Every Minute Every 5 Minutes

SSL encrypt log transmission

Allow access to FortiGate REST API

Verify FortiAnalyzer certificate  FAZ-VMTM19008187☒ FortiClient Endpoint Management System (EMS)Name EMSServer 

IP/Domain Name 10.0.1.100

Serial Number FCTEMS0000100991

Admin User admin

Password .....  Change

The screenshot shows the 'Security Fabric' settings for an EMS server. The 'Hostname' field is set to 'EMSServer'. The 'Listen on IP' dropdown is set to '10.0.1.100'. The 'Use FQDN' checkbox is checked. The 'FQDN' field is set to 'myemsserver'. The 'Remote HTTPS access' checkbox is unchecked. The 'SSL certificate' field shows 'No certificate imported'.

Based on the FortiGate Security Fabric settings shown in the exhibits, what must an administrator do on the EMS server to successfully quarantine an endpoint.

When it is detected as a compromised host (IoC)?

- A. The administrator must enable remote HTTPS access to EMS.
- B. The administrator must enable FQDN on EMS.
- C. The administrator must authorize FortiGate on FortiAnalyzer.
- D. The administrator must enable SSH access to EMS.

**Answer: A**

4.Refer to the exhibit.

The screenshot shows the 'AntiVirus Protection' settings in FortiClient. The 'Realtime Protection' is set to 'OFF'. The 'Dynamic Threat Detection' is set to 'OFF'. The 'Block malicious websites' is set to 'ON'. The 'Threats Detected' is 75. The 'Scan Schedule' is 'Weekly Scan at 19:30 on Sunday'. The 'Last Scan' is '4/23/2019'. There is a 'Scan Now' button.

Based on the settings shown in the exhibit what action will FortiClient take when it detects that a user is trying to download an infected file?

- A. Blocks the infected files as it is downloading
- B. Quarantines the infected files and logs all access attempts
- C. Sends the infected file to FortiGuard for analysis
- D. Allows the infected file to download without scan

**Answer: D**

5.An administrator deploys a FortiClient installation through the Microsoft AD group policy After installation is complete all the custom configuration is missing.

What could have caused this problem?

- A. The FortiClient exe file is included in the distribution package
- B. The FortiClient MST file is missing from the distribution package
- C. FortiClient does not have permission to access the distribution package.
- D. The FortiClient package is not assigned to the group

**Answer: D**