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_FAZ-7.0**

Title : Fortinet NSE 5 - FortiAnalyzer 7.0

Version : DEMO

1.Which log type does the FortiAnalyzer indicators of compromise feature use to identify infected hosts?
A. Antivirus logs
B. Web filter logs
C. IPS logs
D. Application control logs
Answer: B
Explanation:
Reference:
https://help.fortinet.com/fa/faz50hlp/60/6-0-2/Content/FortiAnalyzer_Admin_Guide/3600_FortiView/0200_Using_FortiView/1200_Compromised_hosts_page.htm?TocPath=FortiView%7CUsing%20FortiView%7C_____6

2.The admin administrator is failing to register a FortiClient EMS on the FortiAnalyzer device.
What can be the reason for this failure?
A. FortiAnalyzer is in an HA cluster.
B. ADOM mode should be set to advanced, in order to register the FortiClient EMS device.
C. ADOMs are not enabled on FortiAnalyzer.
D. A separate license is required on FortiAnalyzer in order to register the FortiClient EMS device.
Answer: C
Explanation:
Reference:
https://help.fortinet.com/fa/faz50hlp/56/5-6-2/FMG-FAZ/0800_ADOMs/0015_FortiClient%20and%20ADOMs.htm

3.Which two statements are true regarding FortiAnalyzer operating modes? (Choose two.)
A. When in collector mode, FortiAnalyzer collects logs from multiple devices and forwards these logs in the original binary format.
B. Collector mode is the default operating mode.
C. When in collector mode. FortiAnalyzer supports event management and reporting features.
D. By deploying different FortiAnalyzer devices with collector and analyzer mode in a network, you can improve the overall performance of log receiving, analysis, and reporting
Answer: A,D
Explanation:
Reference:
https://docs.fortinet.com/document/fortianalyzer/7.0.0/administration-guide/227478/collector-mode
https://docs.fortinet.com/document/fortianalyzer/7.0.0/administration-guide/312644/analyzer-collector-collaboration

4.Which two settings must you configure on FortiAnalyzer to allow non-local administrators to authenticate to FortiAnalyzer with any user account in a single LDAP group? (Choose two.)
A. A local wildcard administrator account
B. A remote LDAP server
C. A trusted host profile that restricts access to the LDAP group
D. An administrator group

Answer: A,B
Explanation:
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD38567

5.If you upgrade the FortiAnalyzer firmware, which report element can be affected?
A. Custom datasets
B. Report scheduling
C. Report settings
D. Output profiles
Answer: A
Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/upgrade-guide/669300/checking-reports