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 : **C2150-624**

Title : IBM Security QRadar SIEM V7.2.8 Fundamental Administration

Version : DEMO

1.Administrators on versions of IBM Security QRadar SIEM older than V7.2.4 must use a specific upgrade path to transition to newer software versions. These requirements are outlined in what technical document?
A. Fix Level Recommendation Tool
B. IBM latest firmware release notes
C. QRadar Software upgrade progress technical note
D. IBM System Security Interoperation Center (SSIC)
Answer: C
Explanation:
Most of the upgrades of IBM products are available in technical notes. IBM security Qradar SIEM upgrade process and information can be obtained through technical notes that IBM publishes on the web.
Reference http://www-01.ibm.com/support/docview.wss?uid=swg27038118

2.What is a precaution an Administrator should take before beginning an upgrade of IBM Security QRadar SIEM V7.2.8?
A. Close all open offenses.
B. Purge old data and events.
C. Check and close all open messages.
D. Confirm that a backup of the data is complete.
Answer: D
Explanation:
The first precaution listed in the IBM document states that the administrator should backup data before preparing for software upgrade. Backup of the current settings is important because if anything bad happens during the upgrade, you can always revert back to the original settings.
Reference http://www-01.ibm.com/support/docview.wss?uid=swg27048793

3.After downloading the <QRadar_patchupdate>.sfs file from Fix Central, what is the next step to upgrade IBM Security QRadar SIEM V7.2.8?
A. Log in to the console as the Admin user-> Admin tab -> Advanced Menu -> Clean SIM Model.
B. Log in to the console as the Admin user-> Admin tab -> Advanced Menu -> Upgrade option.
C. Use SSH to log in to the system as the root user -> Run the patch installer with the following command: /media/updates/upgrade_qradar.
D. Use SSH to log in to the system as the root user -> Copy the patch file to the /tmp directory or to another location that has sufficient disk space.
Answer: D
Explanation:
Download the fix pack to install QRadar 7.2.8 Patch 1 from the IBM Fix Central website: http://www.ibm.com/support/fixcentral/swg/quickorder?parent=IBM%2BSecurity&product=ibm/Other+software/IBM+Security+QRadar+SIEM&release=7.2.0&platform=Linux&function=fixId&fixids=7.2.8-QRADARQRSIEM-20161118202122&includeRequisites=1&includeSupersedes=0&downloadMethod=http&source=fc
Using SSH, log in to your system as the root user.
Copy the fix pack to the /tmp directory on the QRadar Console. Note: If space in the /tmp directory is limited, copy the fix pack to another location that has sufficient space.

To create the /media/updates directory, type the following command: mkdir -p /media/updates
Reference http://www-01.ibm.com/support/docview.wss?uid=swg27049111

4.An Administrator working with IBM Security QRadar SIEM V7.2.8 needs to enable the PCI report template.
What is the procedure to accomplish this task?
A. Admin Tab -> Reports -> Templates -> Compliance -> PCI -> Select “Enable”
B. Report Tab -> Enable “Show all templates” -> Group List -> Compliance -> PCI
C. Reports Tab -> Clear “Hide Inactive Reports” box -> Group List -> Compliance -> PCI
D. Admin Tab -> Reports -> Templates -> Compliance -> PCI -> uncheck “Hide Template”
Answer: C
Explanation:
1. Click the Reports tab.
2. Clear the Hide Inactive Reports check box.
3. In the Group list, select Compliance > PCI. 4. Select all report templates on the list:A. Click the first report on the list.
b. Select all report templates by holding down the Shift key, while you click
the last report on the list.
5. In the Actions list, select Toggle Scheduling. 6. Access generated reports:A. From the list in the Generated Reports column, select the time stamp of the
report that you want to view.
b. In the Format column, click the icon for report format that you want to view.
Reference ftp://ftp.software.ibm.com/software/security/products/qradar/documents/7.2.8/en/
b_qradar_gs_guide.pdf

5.An IBM Security QRadar SIEM V7.2.8 Administrator assigned to a company that is looking to add QRadar into their current network. The company has requirements for 250,000 FPM, 15,000 EPS and FIPS.
Which QRadar appliance solution will support this requirement?
A. QRadar 3128-C with Basic License
B. QRadar 2100-C with Basic License
C. QRadar 3128-C with Upgraded License
D. QRadar 2100-C with Upgraded License
Answer: C
Explanation:
The upgraded license of Qradar 3128-C has 300k FPM and 15000 EPS and FIPs. Therefore the Qradar 3128-C with upgraded license is the best choice for the company.
Reference https://www.ibm.com/support/knowledgecenter/SS42VS_7.2.8/com.ibm.qradar.doc/c_hwg_3128_allone.html