

Prep4sureReview



Try Before You Buy

24/7 customer support, Secure shopping site

If you failed your exam after buying our products we will **refund** the full amount back to you.



Free One year updates to match real exam scenarios

Download a free sample of any of our exam questions and answers

Download

<http://www.prep4surereview.com>

Latest IT Prep4Sure materials & exam review

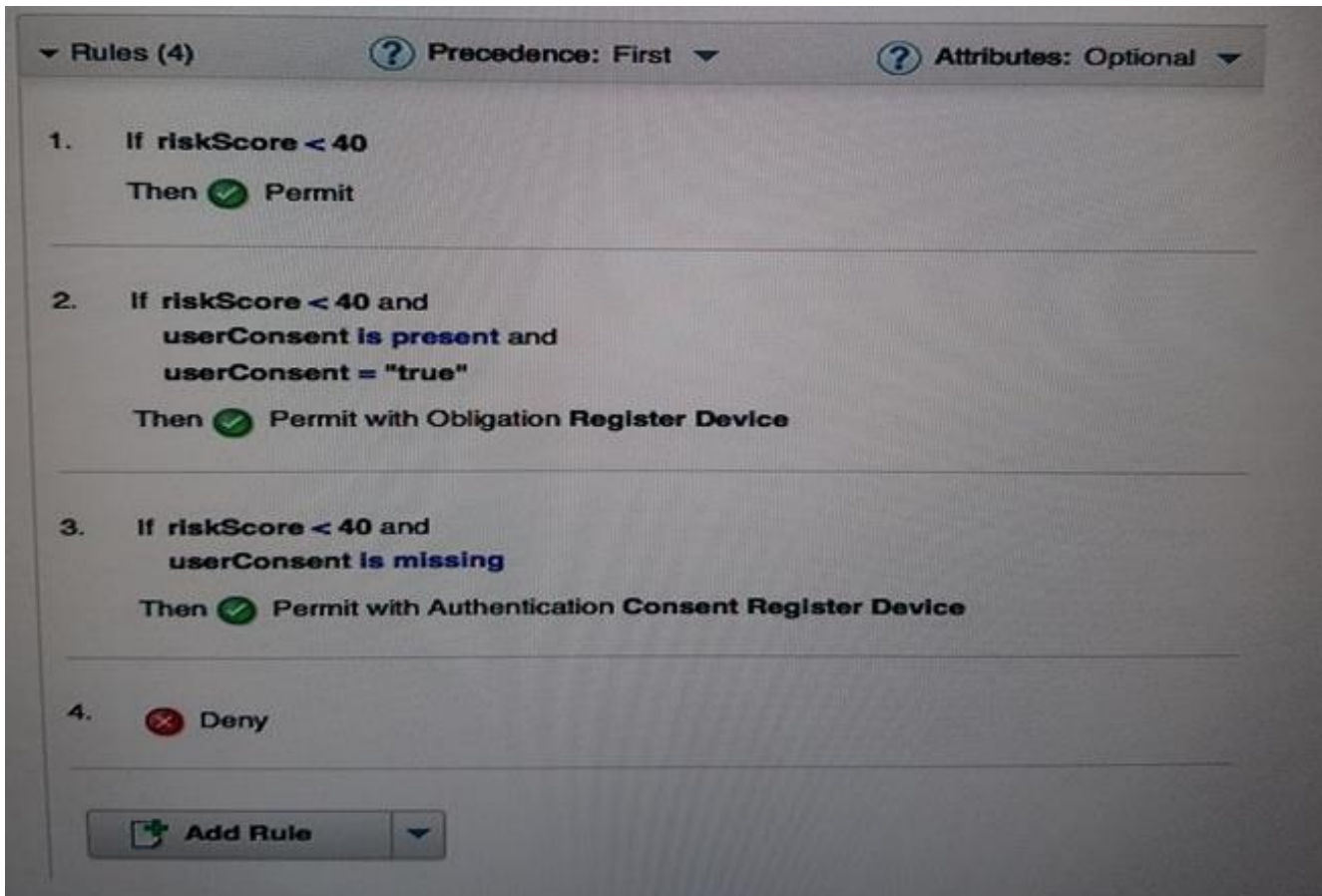
Exam : **C2150-609**

Title : IBM Security Access Manager
V9.0 Deployment

Vendor : IBM

Version : DEMO

NO.1 A deployment professional has created an Access Control Policy to protect sensitive business information:



Which Policy decision is returned for a user with a risk score of 35 and has consented to registering a device?

- A. Permit with Obligation Register Device
- B. Deny
- C. Permit
- D. Permit with Authentication Consent Register Device

Answer: B

NO.2 An IBM Security Access Manager V9.0 deployment professional executes the following steps:

1. Navigate to Edit SSL Certificate Database - embedded_ldap_keys
2. Select the embedded LDAP server certificate
3. Click Manage->Export
4. Save the resulting .cer file onto local desktop

Which task was the deployment professional performing?

- A. Renewing the embedded LDAP server certificate
- B. Creating a backup of the embedded LDAP server certificate
- C. Preparing to configure SSL for a local LDAP client to the embedded LDAP server
- D. Replacing the embedded LDAP server certificate

Answer: D

NO.3 An IBM Security Access Manager V9.0 deployment at a customer has enabled audit.authz,

audit.authn, audit,http for meeting auditing requirements and results in large volume of audit records and poses significant data management challenges to the client. The customer wants to exclude the audit events to certain static resources such as images.

What action should be taken to implement this?

- A. Disable audit.http.unsuccessful events only
- B. Define an ACL with the audithttp operation set to "no"; attach this to the static resources
- C. Define a POP with the audithttp set to "no"; attach this to the static resources
- D. Disable audit.http events only

Answer: C

NO.4 CORRECT TEXT

A customer has expressed the requirement that users accessing online banking application must first authenticate using a userid/password and successfully enter a one-time PIN which is texted to a cell phone.

Which two IBM Security Access Manager (ISAM) V9.0 modules are required to fully implement the solution? (Choose two.)

- A. ISAM Federation Module
- B. ISAM PAM Module
- C. ISAM Access Manager Platform
- D. ISAM Advanced Control Module
- E. ISAM Cloud Module

Answer: C,D

NO.5 An IBM Security Access Manager V9.0 deployment specialist is getting reports of failing requests. Analysis of a support file shows many connections to the backend server in TIME_WAIT state?

Where is the setting "sysctl.net.ipv4.tcp_tw_reuse = 1" added?

- A. In the LMI "Manage System Settings -> Network Settings -> Tuning" panel
- B. In the [server] stanza of the reverse proxy instance conf file
- C. In the LMI "Manage System Settings -> System Settings -> Advanced Tuning Parameters" panel
- D. In the [tcp] stanza of the reverse proxy instance conf file

Answer: C

NO.6 The IBM Security Access Manager (ISAM) V9.0 LMI SSL certificate is auto-generated by default. When the LMI certificate is due to expire, how is it renewed?

- A. The ISAM deployment professional must re-generate it using LMI Manage System Settings -> SSL panels.
- B. The ISAM Appliance will renew LMI certificate automatically.
- C. The ISAM deployment professional must issue reset_lmi_cert using command line interface
- D. The ISAM deployment professional must create a new self sign certificate using LMI Manage System Settings -> SSL panels.

Answer: A

NO.7 Which Hypervisor is supported for a Virtual Appliance?

- A. VirtualBox
- B. Hyper-V
- C. ESXI5.0
- D. VMware Workstation

Answer: C

NO.8 A customer is migrating from TAM v6.1 running on AIX to IBM Security Access Manager (ISAM) V9.0 hardware appliances.

Which information from the TAM v6.1 environment will be useful in sizing the new ISAM V9.0 hardware configuration?

- A. WebSEAL CDAS specifics
- B. WebSEAL request logs
- C. Number of LDAP replicas
- D. Number of objects in the protected object space

Answer: D

NO.9 A risk officer of an organization discovered that a site protected by the IBM Security Access Manager V9.0 solution might be vulnerable to common attacks like cross-site scripting (XSS) and SQL injection.

Which optional component should be configured to protect against these attacks?

- A. Advanced Access Control
- B. Secure Web Settings
- C. Web Application Firewall
- D. Federation

Answer: C

NO.10 The deployment professional (testuseri) is currently logged into the appliance, but cannot read the IBM Security Access Manager (ISAM) V9.0 event logs. Management authorization is configured as shown in the following screenshot.

The screenshot shows the IBM Security Access Manager Management Console. The top navigation bar includes Home (Appliance Dashboard), Monitor (Analysis and Diagnostics), Secure (Web Settings), and Manage (System Settings). The main content area is titled "Management Authorization" and contains two tabs: "Local User Database" and "Remote LDAP User Registry".

Under "Local User Database", there is an "Edit" button and a table with the following data:

Group name	Username
ISAMadmins	

Below this table, it says "No items to display".

Under "Remote LDAP User Registry", there is an "Edit" button and a table with the following data:

Group name	Username

Below this table, it says "No items to display".

On the left side, there is a "Roles" section with a list of roles: Global Administrator, Global Read Only Access, Policy Administration Users, Security Administrator, Security Monitoring, Security Viewer, System Administrator, and System Monitoring. The "Global Administrator" role is selected.

Below the "Role Memberships" section, there is a "Features" section with a "Save" button and "Select All" / "Set Selected" buttons. A table lists features with the following data:

Menu	Category	Feature	Permission
Monitor	Logs	Event Log	Read
Monitor	Logs	Manage Reverse Proxy Log Files	Write

What is the most likely cause of this issue?

- A. The Global Administrator role lacks the necessary privileges.
- B. There is a connectivity issue and the LDAP containing userid "testuser1" cannot be contacted.
- C. Userid "testuser1" has not been added to the ISAMadmins LDAP group.
- D. Write permission is required for the Event Log Feature.

Answer: C