



# C2150-609<sup>Q&As</sup>

IBM Security Access Manager V9.0 Deployment

## Pass IBM C2150-609 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4itsure.com/c2150-609.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by IBM Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





### QUESTION 1

A customer has an IBM Security Access Manager V9.0 appliance cluster spanning two data centers A and B. Data center A has the Primary Master and two Restricted nodes. Data center B has a Secondary Master and two Restricted Nodes.

A Load Balancer with redundancy across data centers provides sticky load balancing to reverse proxies in both data centers.

What is true if a disaster recovery testing scenario takes down all appliances in data center A?

- A. The Secondary Master will automatically be promoted to Primary Master
- B. Reverse Proxies in Data Center B will service all end-users with no intervention
- C. The Secondary Master has to be promoted to Primary for Data Center B to service end-users
- D. Reverse Proxies in Data Center B need to be recycled sequentially to handle users assigned Data Center A reverse proxies.

Correct Answer: A

---

### QUESTION 2

A deployment professional has created an Access Control Policy to protect sensitive business information, but is not obtaining the desired result.



▼ Rules (4)    ? Precedence: First ▼    ? Attributes: Optional ▼

1. If **riskScore < 40**  
Then Permit
2. If **riskScore < 40**  
    **userConsent is present** and  
    **userConsent = "true"**  
Then Permit with Obligation **Register Device**
3. If **riskScore < 40**  
    **userConsent is missing**  
Then Permit with Authentication **Consent Register Device**
4. Deny

Add Rule ▼

Considering the rule precedence, which decision is returned for a user with a risk score of 40 and an ipAddress not considered malware?

- A. Deny
- B. Permit
- C. Deny after Authentication One-Time-Password
- D. Permit after Authentication One-Time-Password

Correct Answer: A

### QUESTION 3

The deployment professional (testuser1) 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.



IBM Security Access Manager

testuser1 Help Language IBM

Home Appliance Dashboard Monitor Analysis and Diagnostics Secure Web Settings Manage System Settings

Management Authorization Management Authorization Users Groups

Roles

Enable Authorization Roles

New Delete

Roles

- Global Administrator
- Global Read Only Access
- Policy Administration Users
- Security Administrator
- Security Monitoring
- Security Viewer
- System Administrator
- System Monitoring

Role Memberships

Local User Database Remote LDAP User Registry

Edit Edit

Group name	Username
ISAMadmins	No items to display

Features

Save Select All Set Selected

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

What is the most likely cause of this issue?

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

Correct Answer: A

#### QUESTION 4

A customer has configured the IBM Security Access Manager V9.0 appliance authentication to an external LDAP server. The customer wants to allow support staff with LDAP accounts that are members of the HelpDesk group to view appliance and audit logs.

Where should the deployment professional configure a new role and map it to the HelpDesk LDAP group for the support staff?

- A. Manage System Settings-> Management Delegation
- B. Manage System Settings-> Administrator Settings
- C. Manage System Settings-> Management Authorization
- D. Manage System Settings-> Management Authentication

Correct Answer: B



### QUESTION 5

The IBM Security Access Manager (ISAM) V9.0 deployment professional is attempting to strike the correct balance between ease of administration/configuration and security, and wants to limit where in the environment security policy can be changed.

On which ISAM component is the Secure Web Settings -> Policy Administration tool automatically disabled?

- A. Runtime cluster restricted node
- B. Master External Reference Entity
- C. Distributed Session Cache primary node
- D. Runtime cluster Standby Policy Server node

Correct Answer: B

[C2150-609 VCE Dumps](#)

[C2150-609 Practice Test](#)

[C2150-609 Exam Questions](#)