Question 1

While a search runs on the Network Activity tab, the direction of a set of flows is seen as R2R. The source IP of this set of flows is an internal email server.

What does this situation suggest about the QRadar configuration?

Options:

A- QRadar might be having performance issues.

B- The email server is offline or down.

C- The email server is not included in the network hierarchy.

D- The flow pipeline is choked because of high incoming flows.

Answer:

C

Question 2

The Server Discovery process updates building blocks based on which of these?

Options:

A- Port-based filtering

B- Malware detection

C- CMDB integration

D- MAC address filtering

Answer:

C

Question 3

Question Type: **MultipleChoice**

Which log file helps in QRadar troubleshooting?

A- aql.log

B- ariel-query.log

C- sim-audit.log

D- qradar.error

Answer:

C

Question 4

Question Type: **MultipleChoice**

A QRadar deployment uses multiple domains to provide data separation between different departments in the organization.

When the tenants and users are configured, which constraints are enforced?

Options:

A- A tenant can contain multiple domains; each domain may be in multiple tenants.

B- A tenant can contain only one domain; each tenant can only have a single user.

C- A tenant can contain multiple domains; each domain may only be in a single tenant.

D- A tenant can contain only one domain; each tenant can have multiple users.

Answer:

C

Question 5

Question Type: **MultipleChoice**

Before the creation of a new application instance with QRadar Assistant, with what entity must every application be associated?

Options:

A- An authorization token

B- A user role

C- A security profile

D- A tenant

Answer:

A

Question 6

Question Type: **MultipleChoice**

What can content management scripts be used to accomplish?

Options:

A- Update QRadar.

B- Export content from a QRadar deployment.

C- Debug the default configuration in QRadar.

D- Extract the list of offenses in QRadar.

Answer:

C