PassQueen
a.k.a dumpsqueen.com

CA Spectrum Infrastructure Manager r9 Administrator Exam

CA Technologies CAT-080

Version Demo

Total Demo Questions: 6

Total Premium Questions: 62

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

In your distributed SpectroSERVER environment, you want to achieve cross-landscape fault isolation in a distributed SpectroSERVER without having duplicate alarms. Which feature enables you to achieve this?

A. Install tickets

B. Proxy models

C. Alarm Notifications

D. SystemEDGE agents

ANSWER: B

Explanation:

Proxy models enable cross-landscape fault isolation in a distributed CA Spectrum deployment while preventing duplicate alarm reporting. A proxy model is a representation, on one landscape, of a model whose ownership and primary monitoring remain on another landscape. This lets Spectrum build and evaluate connectivity relationships that span landscape boundaries. For example, when an upstream device or connection fails, the originating landscape can correlate the resulting condition with affected devices represented through proxies on other landscapes. The fault can therefore be isolated to the actual root cause rather than producing separate, redundant alarms for every downstream symptom across the distributed environment.

This behavior is important because each modeled entity has one authoritative source for its fault and alarm state, while the proxy supplies the cross-landscape relationship information needed for correlation. Proxy models are consequently a core distributed-SpectroSERVER design mechanism for maintaining end-to-end topology awareness and effective root-cause analysis across landscapes. Broadcom's Spectrum documentation describes distributed landscape operation and model relationships in the CA Spectrum documentation portal. Additional product documentation and knowledge resources are available through the Broadcom Knowledge Base.

QUESTION NO: 2

CA Spectrum supports the SNMPv3 standard for the encryption of messages. Which encryption algorithms for privacy does CA Spectrum support? (Choose three)

A. Triple DES (3DES)

B. Tiny Encryption Algorithm (TEA)

C. Data Encryption Standard (DES)

D. Advanced Encryption Standard (AES)

E. International Data Encryption Algorithm (IDEA)

ANSWER: A C D

Explanation:

CA Spectrum supports the SNMPv3 privacy algorithms Triple DES (3DES), Data Encryption Standard (DES), and Advanced Encryption Standard (AES). These algorithms protect the confidentiality of SNMPv3 protocol data units when a user is configured with a privacy protocol and a corresponding privacy passphrase. DES is the original SNMPv3 User-based Security Model privacy mechanism defined in the SNMPv3 security specification. AES privacy support is standardized for SNMPv3 through the AES Cipher Algorithm protocol extension, allowing stronger confidentiality protection where supported by the managed device and the Spectrum configuration. CA Spectrum also supports 3DES as an available privacy encryption choice for compatible SNMPv3 agents. In practice, the selected privacy algorithm must match the privacy protocol configured on the monitored device; otherwise, Spectrum cannot establish authenticated and encrypted SNMPv3

communication. The SNMPv3 User-based Security Model and its DES privacy processing are defined by the IETF in RFC 3414. The SNMPv3 AES privacy protocol is specified in RFC 3826.

QUESTION NO: 3

Which statements about CA Spectrum events and alarms are TRUE? (Choose three)

A. Events can be generated without creating an alarm.

B. An alarm is created when event processing determines that an alarmable condition exists.

C. An alarm can be cleared when the associated condition is resolved.

D. Every Spectrum event automatically creates an alarm.

E. Only OneClick can clear an alarm condition.

ANSWER: A B C

Explanation:

Events can be generated without creating an alarm, **an alarm is created when event processing determines that an alarmable condition exists**, and **an alarm can be cleared when the associated condition is resolved** are correct. Spectrum processes incoming management information as events and applies event configuration and correlation logic to determine whether an alarm should be created or updated.

Not every event represents a fault that requires an alarm. Events can also record informational, configuration, or operational activity. Spectrum therefore does not automatically create an alarm for every event received. See the Broadcom CA Spectrum documentation portal for event and alarm management information.

QUESTION NO: 4

When you create a new role, what does it become in the SpectroSERVER database?

A. A named model

B. A named resource

C. A named collection

D. A named community

ANSWER: A

Explanation:

A named model is correct. In CA Spectrum, security roles are not merely labels maintained outside of the product's operational data. When an administrator creates a role, SpectroSERVER represents and stores that role as a named model in its database. This model-based implementation is consistent with Spectrum's architecture: managed entities, configuration objects, and many administrative constructs are represented as models with associated attributes. The role model provides the persistent object through which Spectrum maintains the role definition and its assigned access-control privileges. Users can then be associated with the role, allowing the permissions defined for that named model to be applied consistently during OneClick and Spectrum access decisions. Because the role is a database model, it can be administered through Spectrum's security and user-management facilities and persists across normal SpectroSERVER operation and restarts. Broadcom's Spectrum documentation describes Spectrum administration, including users, roles, and security configuration, within the SpectroSERVER-managed environment. See the CA Spectrum documentation portal and Broadcom's Knowledge Base for product documentation and administrative guidance.

QUESTION NO: 5

In a Distributed SpectroSERVER environment, how do SpectroSERVERS communicate with each other?

A. They use direct communication.

B. They communicate through the OneClick Server.

C. They communicate through the Main Location Server (MLS).

ANSWER: A

Explanation:

They use direct communication. In a Distributed SpectroSERVER deployment, each SpectroSERVER maintains its own landscape and modeling database while participating in a distributed environment with the other SpectroSERVERS. The SpectroSERVER processes establish direct inter-server communications to exchange the information required for distributed landscape operation, including model and event-related data needed to present a unified management view. This peer-to-peer SpectroSERVER connectivity is a core part of CA Spectrum's distributed architecture and enables management responsibility to be divided across multiple servers without making a user-interface component part of the server-to-server data path.

The direct communication design also supports scalability: additional landscapes can be managed by separate SpectroSERVER instances while the distributed environment continues to coordinate information among them. OneClick provides access to and visualization of the distributed Spectrum environment, but the architectural communication relationship among SpectroSERVERS is direct. Broadcom's Spectrum documentation describes the distributed deployment architecture and administration concepts in its CA Spectrum documentation portal; product documentation and related knowledge resources are also available through the Broadcom Knowledge Base.

QUESTION NO: 6

For CA Spectrum to interrogate a device through SNMP during discovery, which conditions must be met? (Choose three)

A. Network reachability to the device IP address

B. Matching SNMP credentials

C. Access to the SNMP agent port

D. Prior receipt of an SNMP trap from the device

E. A reverse DNS record for the device

ANSWER: A B C

Explanation:

CA Spectrum must be able to reach the device IP address, the configured SNMP credentials must match the device configuration, and SNMP communication to the agent must be permitted. For the standard SNMP request-response operation, this normally requires access to UDP port 161. The device does not have to send traps before it can be discovered, because traps and SNMP polling are separate mechanisms.

For SNMPv3, the configured user name, authentication settings, and privacy settings, when used, must also match the agent configuration. See the Broadcom TechDocs CA Spectrum documentation portal for discovery configuration guidance.