DUMPSBOSS.

CA AppLogic r3 Administrator Exam

CA Technologies CAT-280

Version Demo

Total Demo Questions: 7

Total Premium Questions: 74

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

A grid controller becomes intermittently non-responsive. Before escalating the issue, which information should you collect? (Choose three)

A. Controller log files from the period of the failure

B. Grid messages reported near the time of the failure

C. Server status information for the grid servers

D. Delete the controller logs to create space for new messages.

E. Reboot every grid server before collecting diagnostic information.

ANSWER: A B C

Explanation:

Controller logs provide details about grid-management operations and controller failures. Grid messages can reveal warnings, alerts, and operational events that correspond to the reported time period, while server-status information identifies whether a grid server is unavailable or otherwise contributing to the condition.

Collecting this information before restarting or changing components helps preserve evidence needed to diagnose the issue. Deleting logs removes useful diagnostic data, and rebooting every grid server is not an appropriate first troubleshooting action for an intermittent controller issue. Broadcom support resources are available through the Broadcom Knowledge Base.

QUESTION NO: 2

Which CA AppLogic runtime subsystem is responsible for handling the infrastructure required by each application?

A. Disposable Infrastructure Manager

B. Grid Controller

C. Global Volume Store

D. Backbone Fabric Controller

ANSWER: A

Explanation:

The **Disposable Infrastructure Manager** handles the infrastructure required by each CA AppLogic application. It manages the disposable infrastructure resources that support an application while allowing the application definition to remain independent of the individual physical grid servers on which it runs.

This differs from the Distributed Kernel, which abstracts and virtualizes grid hardware and provides core system services, and from the Grid Controller, which provides the central management functions for the grid. CA AppLogic architecture information is available in the CA 3Tera AppLogic Architecture documentation.

QUESTION NO: 3

You want to integrate your grid application with a legacy system. To do this, the legacy system must share network access with your grid's:

A. Controller

B. Public switch

C. Private switch

D. Power management network switch

ANSWER: B

Explanation:

Public switch is correct because CA AppLogic separates grid networking into public and private network domains. The public network is the externally reachable network used for connections between an application running in the grid and systems outside the grid, including enterprise resources, users, and legacy applications. To integrate a grid application with a legacy system, the legacy host therefore needs network connectivity to the same public-side network infrastructure as the grid so that application interfaces can be addressed and traffic can be routed between the two environments.

This arrangement allows application components to expose or consume services through their configured public interfaces while retaining the grid's internal private network for component-to-component communication. The public switch is consequently the appropriate shared network point for an external legacy system that must communicate with the grid application. Network connectivity, addressing, routes, and any relevant firewall rules must also permit the required application ports and protocols between the legacy system and the grid's public interfaces.

CA AppLogic is documented as a platform for deploying and operating distributed applications, with networking as a fundamental part of grid and application configuration. See the CA AppLogic documentation and the Broadcom CA Technologies education resources.

QUESTION NO: 4

Many CA AppLogic subsystems and appliances can create event messages to provide information, warnings, or alerts. Which utility can you use to generate events within a running component?

A. iso2class

B. image2class

C. Data Director

D. VME user mode

ANSWER: D

Explanation:

VME user mode is the correct utility because it provides the mechanism for a running CA AppLogic component to create and submit event messages. Appliances and components use this event facility to report operational conditions such as informational status, warnings, and alert-level situations to the CA AppLogic platform. This enables the application infrastructure to surface meaningful runtime state without requiring an administrator to inspect the component manually.

In practical use, the component invokes the VME user-mode interface from its running environment and supplies the event details, including the relevant severity and message content. The platform can then record and expose the event through its normal monitoring and management interfaces. This makes VME user mode appropriate for appliance authors who need their components to communicate significant lifecycle, health, or service conditions while deployed in a grid.

CA AppLogic documentation describes the platform's appliance and operational-management capabilities, including facilities used by appliances at runtime. See the CA 3Tera AppLogic documentation and Broadcom's technical knowledge base for product documentation and operational guidance.

QUESTION NO: 5

You are preparing a production CA AppLogic application for high availability (HA). Which actions should you perform? (Choose three)

A. Place redundant critical appliance instances on separate grid servers.

B. Maintain sufficient unused grid capacity for recovery after a server failure.

C. Test the application during planned server and switch outage scenarios.

D. Place all critical appliance instances on the same grid server.

E. Delete virtual-volume streams before performing HA tests.

ANSWER: A B C

Explanation:

High availability requires that critical application components are not dependent on one physical grid server or one network path. Critical appliance instances should be placed on separate servers where the application design supports redundancy, and the grid must retain enough available capacity to restart or recover workloads after a server failure.

Testing server and switch failures before production use verifies that the configured redundancy, placement, network paths, and recovery capacity provide the expected result. Placing all critical components on one server creates a single point of failure, and deleting volume streams is not an HA preparation activity. See the CA 3Tera AppLogic Bookshelf for grid architecture information.

QUESTION NO: 6

You need to enable your grid servers to PXE boot on the Backbone Fabric Controller (BFC) network. Which steps do you need to perform? (Choose two)

A. In System Security, set AC power recovery to OFF.

B. On the power controller setup screen, set IPMI over LAN to off.

C. In the boot settings, enable the backbone NIC to boot before the disk.

D. Enable backbone Network Interface Cards (NICs) to PXE boot in the BIOS.

ANSWER: C D

Explanation:

PXE booting a grid server through the Backbone Fabric Controller network requires both a firmware-level PXE capability setting and an appropriate boot-device priority. “Enable backbone Network Interface Cards (NICs) to PXE boot in the BIOS.” enables the network adapter’s preboot execution environment, allowing the server firmware to initialize the backbone-facing NIC and obtain the network bootstrap information needed to start from the BFC-managed network.

“In the boot settings, enable the backbone NIC to boot before the disk.” ensures that, once PXE is enabled, the server actually attempts a network boot before falling back to its local operating-system disk. This ordering is essential for grid-server provisioning and recovery workflows: the BFC can supply the required boot path only when the backbone NIC is selected early enough in the firmware boot sequence. Together, these settings make the backbone interface available for PXE and prioritize it as the startup device. CA AppLogic administration documentation describes the BFC as the management and provisioning component for grid infrastructure; see the CA AppLogic documentation portal. General PXE firmware behavior and boot configuration are also described in the UEFI Specification.

QUESTION NO: 7

You want to integrate a CA AppLogic grid with an external directory service. To provide an encrypted connection to the global directory server, which protocol can you select?

A. Secure Shell (SSH)

B. Secure Sockets Layer (SSL)

C. Transport Layer Security (TLS)

D. Internet Protocol Security (IPsec)

ANSWER: C

Explanation:

Transport Layer Security (TLS) is the appropriate protocol for encrypting the connection between a CA AppLogic grid and an external global directory service. Directory integrations commonly use the Lightweight Directory Access Protocol, and TLS protects the directory traffic while it travels across the network. This protection is important because authentication exchanges can include credentials and directory queries can expose user, group, and authorization information. TLS provides server authentication through certificates and establishes an encrypted session before sensitive directory data is exchanged. In a directory-service deployment, TLS may be negotiated using the LDAP StartTLS operation or used as part of a secure LDAP listener configuration, depending on the server and grid configuration. The directory server must present a certificate that the grid can validate, and the relevant certificate authority chain should be trusted by the grid. This matches standard LDAP security guidance: RFC 4513 specifies TLS as the mechanism used to provide confidentiality and integrity protection for LDAP connections, while RFC 4511 defines the LDAP protocol framework and its extension model. See RFC 4513: LDAP Authentication Methods and Security Mechanisms and RFC 4511: Lightweight Directory Access Protocol.