PassQueen
a.k.a dumpsqueen.com

CA Unified Infrastructure Management 8.x Proven Professional Exam

CA Technologies CAT-540

Version Demo

Total Demo Questions: 6

Total Premium Questions: 60

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Architecture	13
Topic 2, Installation and Upgrade	6
Topic 3, Configuration	30
Topic 4, Administration	5
Topic 5, Monitoring	6
Total	60

QUESTION NO: 1

You completed the nimldr installation on several Linux distributions. Now you need to enable the nimbus

service. Which Linux command should you run to enable the service?

A. systemctl enable nimbus.service

B. /etc/init.d/niminit start

C. /opt/nimsoft/bin/niminit run

D. /nimldr -I NMS_server_name_or_IP_address

ANSWER: A

Explanation:

`systemctl enable nimbus.service` is the correct command because the nimldr installation registers the CA Unified Infrastructure Management (UIM) Nimbus service with systemd on supported Linux systems. The `enable` action configures systemd so that the Nimbus service is started automatically during normal system boot. This is the required post-installation configuration step when the objective is to enable the service persistently, rather than merely launch a process for the current session. The explicit `.service` suffix identifies the systemd unit file for Nimbus and makes the command unambiguous. After enabling the unit, an administrator can use the normal systemd service-management workflow to start it immediately and check its operational state. CA UIM Linux robot installation guidance documents the use of system service integration for deployed UIM components. The systemd documentation also defines `enable` as creating the unit-file links that cause a service to be started by the relevant boot target. See the CA UIM documentation at Broadcom TechDocs and the systemctl manual.

QUESTION NO: 2

Which guidelines apply when creating Unified Service Manager (USM) groups? (Choose two.)

A. Never put more than 250 devices in one group.

B. Use the containers to create a hierarchy that applies to the customer business or infrastructure.

C. Always put the origin at the beginning of the group name so that the administrators know which customer created it.

D. In the group labels, indicate whether they are Monitoring Configuration Service (MCS) groups.

ANSWER: B D

Explanation:

Use the containers to create a hierarchy that applies to the customer business or infrastructure. USM containers and groups are intended to organize managed entities in a meaningful, navigable model. Building the hierarchy around how the customer operates—for example, by business service, geographic location, department, application, or infrastructure tier—makes the inventory easier for operators to browse and helps present monitoring information in an appropriate operational context. This structure can be tailored to the customer rather than requiring a fixed device-oriented layout.

In the group labels, indicate whether they are Monitoring Configuration Service (MCS) groups. Clearly identifying MCS-related groups in their labels helps administrators distinguish groups used for monitoring configuration and profile deployment from groups intended primarily for organizational views. This naming practice improves administration of MCS policies and reduces ambiguity when selecting target groups for configuration tasks. Broadcom's Unified Infrastructure Management documentation describes USM as the interface for organizing and managing monitored entities and documents MCS group-based configuration capabilities. See the Broadcom Unified Infrastructure Management documentation and the Monitoring Configuration Service documentation.

QUESTION NO: 3

How is a connection established when difficulties with a hub-to-hub tunnel connection occur because of a bad password?

A. Create a new certificate and password, and set up the tunnel again.

B. Clear the SSL cache and cookies.

C. Restart the primary server hub.

D. Paste the original certificate from the tunnel server again, with the same password.

ANSWER: C

Explanation:

Restart the primary server hub. In CA Unified Infrastructure Management, hub-to-hub tunnel authentication depends on the tunnel certificate and its associated password. A failed attempt using an invalid password can leave the hub's tunnel authentication/connection state unable to complete the expected handshake. Restarting the primary server hub resets the hub processes and causes the tunnel components to initialize again, allowing the configured tunnel connection to be established with the valid tunnel credentials. This is the appropriate recovery action for the specific condition described: an authentication attempt involving a bad password during tunnel connection setup. The primary hub is central to UIM domain communication, so restarting it refreshes the relevant hub and tunnel services rather than requiring an unrelated browser-cache action or a replacement certificate. CA UIM documentation describes tunnels as the mechanism used to connect hubs across network boundaries and identifies the hub as the component responsible for this communication. See the CA UIM documentation on configuring tunnels and the Hub configuration reference.

QUESTION NO: 4

You are configuring an Auto-Operator (AO) profile in the Alarm Server (NAS). Which actions can an AO profile perform when an alarm matches its criteria? (Choose two.)

A. Execute a command.

B. Send a notification.

C. Collect CPU utilization from a remote server.

D. Install a probe on a robot.

E. Create a database partition.

ANSWER: A B

Explanation:

An Auto-Operator profile can execute a command and send a notification when an alarm matches the profile criteria. AO profiles are used to automate alarm-handling responses, including initiating remediation scripts or commands and notifying an administrator or operational group through a configured notification action.

AO processing is performed by the NAS after it receives alarms. It does not collect operating-system performance data or install probes on robots. These functions belong to monitoring probes and deployment mechanisms rather than alarm automation. See the UIM alarm-management documentation.

QUESTION NO: 5

In CA UIM 8.5.1. which probes are covered by Monitoring Configuration Service (MCS) templates? (Choose three.)

A. snmpcollector

B. vmware

C. vmax

D. cdm and ntevl

E. dirscan

ANSWER: B D E

Explanation:

In CA UIM 8.5.1, Monitoring Configuration Service provides centrally managed monitoring templates for supported probes, allowing administrators to define monitoring profiles and deploy them consistently to target devices or groups. The **vmware** probe is covered by MCS templates for VMware infrastructure monitoring. The **cdm and ntevl** probes are also covered: cdm templates support system-resource monitoring, while ntevl templates provide Windows Event Log monitoring configuration. The **dirscan** probe is included for template-driven monitoring of directories and files, such as checking for expected files, file age, or directory content conditions. These supported MCS template integrations let operators standardize thresholds and policies while reducing the need to configure each robot individually. Broadcom's CA UIM documentation describes MCS as the service used to deploy monitoring configurations through profiles and templates, and its probe documentation identifies the monitoring capabilities supplied by these probes. See the CA Unified Infrastructure Management 8.5.1 documentation and the CA UIM documentation portal.

QUESTION NO: 6

You need to define a proxy connection between an Apache server and a UMP server when you:

A. use sticky sessions in a load-balancing configuration.

B. set up access to the UMP through a DMZ.

C. configure the UMP to use SSL communication exclusively.

D. implement multiple UMP servers.

ANSWER: B

Explanation:

You define a proxy connection between Apache HTTP Server and Unified Management Portal when you set up access to the UMP through a DMZ. In this topology, Apache acts as a reverse proxy at the network boundary: users connect to the Apache server, while Apache forwards the approved UMP requests to the UMP application server on the protected internal network. This avoids directly exposing the UMP server to clients located outside the trusted network and provides a controlled point at which access, routing, and HTTPS settings can be managed. The proxy configuration maps the externally reachable Apache endpoint to the internal UMP address and must preserve the application paths and request handling required by UMP. This deployment pattern is specifically intended to make UMP available across a demilitarized zone while retaining separation between the external-facing web tier and the internal UIM environment. Broadcom's knowledge article for this procedure describes configuring Apache HTTP Server as a proxy for access to UMP in a DMZ: How to set up access to UMP in the DMZ using Apache HTTP Server as a proxy. UIM product documentation is available from the Broadcom TechDocs UIM documentation portal.