DUMPSARENA

CA Identity Manager r12.x Professional

CA Technologies CAT-340

Version Demo

Total Demo Questions: 7

Total Premium Questions: 70

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

You need to import a large number of managed users to the CA Identity Minder User Store simultaneously. Having explored the various options, the Bulk Loader method seems the best option. However, which limitation do you need to be aware of before you begin?

A. It may use large amounts of memory.

B. It cannot be mapped to a workflow process.

C. It does not support the execution of identity policies.

D. It bypasses audit and security mechanisms provided by the Task Server.

ANSWER: A

Explanation:

It may use large amounts of memory. is correct because the CA Identity Manager Bulk Loader is designed for high-volume, direct loading of managed-user data, rather than processing each user through the normal interactive task flow. To improve throughput, the loader processes input records in batches and retains processing data in the Java process. Consequently, memory consumption can become substantial when the source file contains many users, the user records contain numerous attributes, or the configured batch size is high. Before a large import, an administrator should estimate the volume, ensure that the Bulk Loader host has adequate available memory, and set an appropriate JVM heap size. It is also prudent to test with a representative subset of the import file and tune batch-related settings before running the full production load. If memory pressure occurs, reducing the batch size or splitting the source data into smaller files can make the import more predictable while retaining the advantages of bulk processing. CA Identity Manager documentation covers Bulk Loader as an administrative import facility and documents its operational configuration considerations; see the CA Identity Manager documentation portal and Broadcom's Knowledge Base for version-specific Bulk Loader guidance.

QUESTION NO: 2

When you export CA IdentityMinder environment settings, you generate a ZIP file containing which files? (Choose three)

A. alias_environment.xml

B. alias_environment_roles.xml

C. alias_environment_users.xml

D. alias_environment_settings.xml

E. alias_environment_mappings.xml

ANSWER: A B D

Explanation:

CA IdentityMinder exports an environment as a ZIP archive containing a set of XML artifacts named with the environment alias. `alias_environment.xml` is the principal environment-definition artifact. It preserves the exported environment configuration so that the environment can later be recreated or moved through an import operation. `alias_environment_roles.xml` is included to carry the administrative role information associated with the environment. This lets a target system receive the role configuration required to administer the imported environment consistently. `alias_environment_settings.xml` contains the environment-level settings that accompany the environment definition and are needed to restore its configured behavior.

Together, these files represent the environment definition, its role configuration, and its settings in the export package. The alias portion is replaced by the actual environment alias selected during export, which permits multiple environment exports to be distinguished and managed safely. This export/import mechanism supports migration and backup of IdentityMinder environment configuration rather than merely copying application-server files. Broadcom's Identity Manager documentation describes environment administration and the export/import procedures in the Identity Manager documentation library. Product lifecycle and documentation access are also maintained through the Broadcom Support portal.

QUESTION NO: 3

Forward Inc. is an international logistics company with headquarters in the United Kingdom. Forward Inc. has asked you to demonstrate how CA IdentityMinder supports account provisioning. In the CA IdentityMinder configuration that you will use for your demonstration, which component is optional?

A. Provisioning Server

B. Provisioning Directory

C. IdentityMinder Server

D. SiteMinder Policy Server

ANSWER: D

Explanation:

SiteMinder Policy Server is the optional component in a CA IdentityMinder deployment used to demonstrate account provisioning. IdentityMinder can integrate with CA SiteMinder to use its centralized authentication and authorization capabilities, such as protecting IdentityMinder access through SiteMinder policies and using a SiteMinder-managed authentication experience. This integration is useful where an organization already uses SiteMinder as its web access-management platform or requires its policy-based protection model, but it is not a prerequisite for the IdentityMinder provisioning architecture itself.

For provisioning, IdentityMinder relies on its own IdentityMinder server and on the CA Identity Manager Provisioning Server, which performs provisioning operations against managed endpoint accounts. The Provisioning Directory supplies the directory repository used by the provisioning environment for its account, endpoint, and related provisioning data. Those components support the core provisioning workflow, whereas SiteMinder is an integration choice for web access management. CA IdentityMinder documentation describes SiteMinder as an optional external component and documents the provisioning architecture separately. See the CA Identity Manager documentation and Broadcom's SiteMinder documentation.

QUESTION NO: 4

Before you install the Connector Server, what should you do? (Choose two)

A. Check that the Java Virtual Machine is already installed.

B. Make sure that the time settings on all computers that will hold Connector Servers match.

C. Make sure that prerequisite packages are installed in the correct order on Red Hat 6.x systems.

D. Check that the computer already contains either the Provisioning Server or the CA IdentityMinder Server.

ANSWER: B C

Explanation:

Before Connector Server installation, the clocks on every computer hosting a Connector Server should be synchronized. Connector Server deployments rely on coordinated communication among provisioning components and managed endpoints, and matching system time helps ensure that time-sensitive authentication, logging, request processing, and certificates operate consistently. Configure the hosts to use a reliable common time source, such as an enterprise NTP service, before beginning installation.

On Red Hat Enterprise Linux 6.x, the prerequisite packages must also be installed in the documented order. The Connector Server installation prerequisites include operating-system libraries and compatibility dependencies; installing them in the prescribed sequence ensures that package dependencies are resolved correctly and that required runtime components are available when the Connector Server installer runs. This preparation should be completed and verified before installing the Connector Server, rather than remediating missing dependencies afterward. Broadcom's Identity Manager documentation provides the product installation guidance and platform-specific prerequisites; consult the applicable Connector Server and

provisioning installation section for the precise package list for the deployed release. See Broadcom Identity Manager documentation and Broadcom Support.

QUESTION NO: 5

Because of a recent acquisition by Forward Inc., which will add 1800 new users to the system, you decide to use the Bulk Loader to feed the information to CA IdentityMinder, You will need to prepare a file for the Bulk Loader, containing the relevant details. Which Bulk Loader input file guidelines do you need to follow? (Choose three)

A. The file should contain no header.

B. A field representing the action is mandatory.

C. Each file must describe a single managed object type.

D. Multivalued attributes must be separated by a hash (#) symbol.

E. Attribute names should be the physical or well-known names of the managed objects.

ANSWER: B C E

Explanation:

CA IdentityMinder Bulk Loader input is structured so that the loader can identify both the object operation and the attribute mapping for every imported record. Therefore, *A field representing the action is mandatory.* The action value directs Bulk Loader to perform the intended operation for each record, such as creating, modifying, or deleting a managed object. This enables a single controlled import process to apply the appropriate lifecycle operation to the supplied data.

Each file must describe a single managed object type. Bulk Loader processing is based on a consistent managed-object schema within an input file. Keeping one object type per file ensures that each column is interpreted against the appropriate object definition and that the requested action is applied to the intended type of object.

Attribute names should be the physical or well-known names of the managed objects. The input-file column names must map to names that IdentityMinder recognizes for the relevant managed object. Using physical directory attribute names or supported well-known names allows Bulk Loader to resolve the supplied values correctly and update the target identity-store data. See the Broadcom CA Identity Manager documentation and the Broadcom Knowledge Base for product documentation and Bulk Loader guidance.

QUESTION NO: 6

Which two components communicate using a Connector?

A. Provisioning Server and endpoint

B. Policy Server and Report Server

C. User Store and Provisioning directory

D. Report Server and Snapshot Database

ANSWER: A

Explanation:

Provisioning Server and endpoint is correct. In CA Identity Manager provisioning architecture, a connector is the software integration layer that enables the Provisioning Server to communicate with, administer, and synchronize accounts on a managed target system, known as an endpoint. The Provisioning Server sends provisioning operations—such as creating, modifying, suspending, or deleting an account—to the appropriate connector. The connector translates those operations into the native commands, APIs, protocols, or directory changes required by that particular endpoint technology.

This connector-based design lets Identity Manager manage many different endpoint types through a consistent provisioning model while allowing each target system's specific implementation details to remain within its connector. Connectors can support systems such as directories, databases, operating systems, applications, and enterprise platforms. Endpoint configuration associates a particular managed system with the applicable connector and connection settings, allowing the Provisioning Server to route account-management requests correctly. Broadcom's Identity Manager documentation describes provisioning as the capability to manage endpoint accounts through the Provisioning Server and its connector framework. See the Broadcom Identity Manager documentation and the Identity Manager product documentation downloads for provisioning architecture and connector details.

QUESTION NO: 7

When you configure the Report Server, which guideline should you follow?

A. Always restart the environment after you configure reporting.

B. Set all systems involved in reporting to the same time zone and time.

C. To avoid port conflicts with JBoss, change the default port numbers in the CRConfig.xml file.

D. Configure the connection with the Provisioning Server before you configure the connection with the Snapshot Database.

ANSWER: B

Explanation:

Set all systems involved in reporting to the same time zone and time. CA Identity Manager reporting combines information produced by several components, including the Identity Manager environment, the Report Server, the Provisioning Server, and the Snapshot Database. These systems create, store, retrieve, and correlate records using date and time values. A common, synchronized time basis is therefore necessary for report data to be interpreted consistently. If components use differing clocks or time zones, records that belong to the same activity can appear in an incorrect sequence or fall outside a report's selected date range. This is especially important for reports that compare provisioning activity with snapshot data or present historical activity over a specified interval. Configure a consistent time zone across the reporting-related hosts and use an enterprise time-synchronization service, such as NTP, so that their system clocks remain aligned. This configuration practice supports reliable report generation, accurate event ordering, and meaningful auditing. Broadcom's Identity Manager documentation is available through the CA Identity Manager documentation portal; the product's reporting and deployment guidance should be applied alongside the organization's standard time-synchronization practices.