PassQueen
a.k.a dumpsqueen.com

HCLSoftware Certified Associate Administrator ExamNotes/Domino 12

HCL Software Academy HCL-DOM-AADM-12

Version Demo

Total Demo Questions: 8

Total Premium Questions: 85

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

What is the main purpose of the Messaging tab in the Domino Administrator Client?

A. Configure DAOS

B. Monitor mail routing and SMTP diagnostics

C. Create and manage server groups

D. Manage server partitions

ANSWER: B

Explanation:

The correct answer is **Monitor mail routing and SMTP diagnostics**. The Messaging tab in the Domino Administrator client is the central administrative workspace for monitoring and managing Domino mail flow. It gives administrators access to routing-related views and tools, including the status of mail routing, message queues such as MAIL.BOX, and routing events. This enables an administrator to identify delayed, held, or failed messages and to assess whether the Router is processing mail normally. The tab also includes SMTP-focused diagnostic capabilities, which are important when investigating inbound or outbound SMTP delivery behavior and connectivity with other mail systems. These functions support day-to-day operational monitoring and troubleshooting of the Domino messaging environment, helping administrators detect mail-flow bottlenecks and take appropriate corrective action. HCL's Domino Administrator documentation describes the Messaging tab as the location for administering mail routing and related messaging tasks. For further details, see the HCL Domino Administrator Messaging tab documentation and the HCL guidance for monitoring mail routing.

QUESTION NO: 2

Which two advantages are provided by using organizational-unit certifiers in a Domino hierarchical naming structure? (Choose two)

A. Delegate registration administration within an organizational unit

B. Eliminate the need for DNS name resolution

C. Maintain a certificate chain to the organization certifier

D. Create mail databases automatically for all users

ANSWER: A C

Explanation:

An organizational-unit certifier can be used to **delegate registration administration** for a defined part of the organization. For example, an administrator responsible for an organizational unit can register users and servers within that unit without needing routine access to the organization certifier ID.

Organizational-unit certifiers also maintain a **certificate chain to the organization certifier**. This preserves the hierarchical trust relationship while allowing names to be organized under separate organizational units.

Organizational-unit certifiers do not replace DNS for network name resolution and do not automatically create mail databases.

QUESTION NO: 3

What security feature helps prevent unauthorized use of a user's Notes client on a shared machine?

A. Server access control

B. Replication formula restrictions

C. Smart Upgrade tracking

D. Lock ID after x minutes of inactivity

ANSWER: D

Explanation:

Lock ID after x minutes of inactivity is the appropriate security feature because it protects a Notes client session when its user leaves a shared workstation unattended. After the configured idle interval elapses, Notes locks the ID, requiring the ID password before the client can be used again. This prevents a person who subsequently approaches the workstation from opening mail, accessing applications, sending messages, or using any other resources available through the currently active Notes identity.

This protection is especially important on reception desks, shift-based workstations, training rooms, and other environments in which more than one person may physically use the same device. An administrator can standardize the behavior through policy settings rather than relying on every user to remember to lock the client manually. The timeout should be selected according to the organization's security requirements and the practical needs of users who may temporarily step away from their machines.

The setting protects the local Notes session and its ID while it is inactive, providing a direct safeguard against unauthorized walk-up use. HCL Domino administrator documentation describes the policy-based administration model and client security configuration in the HCL Domino 12.0.2 documentation and the Domino Administrator documentation.

QUESTION NO: 4

Which two types of replication modes are supported by Domino? (Choose two)

A. Time-based replication

B. Push replication

C. Pull replication

D. HTTP over DAOS

ANSWER: B C

Explanation:

Push replication and **Pull replication** are the fundamental directional replication modes supported by HCL Domino. With push replication, the initiating server sends its locally accumulated database changes to the destination server. This is useful when the initiating server is responsible for distributing updates to another replica. With pull replication, the initiating server requests and receives changes from the remote server, allowing it to obtain updates held by that replica.

These directions can also be combined in a connection document as push-pull replication, which exchanges changes in both directions during the replication session. The underlying modes remain push and pull: they determine whether the local server sends changes, requests changes, or does both. Domino replication uses replica IDs and replication histories to identify corresponding replicas and exchange only the changes required to bring replicas up to date, rather than transferring an entire database each time. Administrators configure the intended direction in server connection documents and can schedule replication according to operational requirements. See HCL's Domino replication documentation and connection document configuration guidance.

QUESTION NO: 5

Which two conditions can prevent Domino mail routing from functioning correctly? (Choose two)

A. Invalid DNS entries for the SMTP relay

B. Disabled DAOS task

C. Missing or incorrect Connection documents

D. Lack of Domino roaming profile

ANSWER: A C

Explanation:

Invalid DNS entries for the SMTP relay can stop SMTP mail routing because Domino must resolve the configured relay host or destination mail hosts to usable network addresses. The Router and SMTP components rely on DNS lookups for outbound SMTP delivery, including resolution of MX records and relay-server names. If the relevant DNS name is missing, incorrectly mapped, or otherwise cannot be resolved, messages can remain queued because Domino cannot establish the required SMTP connection. HCL documents the role of DNS in locating hosts for SMTP routing in its Internet DNS configuration guidance.

Missing or incorrect Connection documents can prevent routing between Domino servers when the routing topology requires a defined connection. Connection documents provide the Router with information such as the destination server, connection type, schedule, and route details. A valid document enables the server to establish or schedule the required Notes network connection and transfer queued mail to the next Domino hop. HCL's Connection documents documentation describes their use in defining server-to-server communications. Consequently, both accurate DNS resolution for SMTP delivery and correctly configured Domino connection information are essential routing prerequisites.

QUESTION NO: 6

Which two roles in the Server document grant privileged administrative access to the Domino server? (Choose two)

A. Run unrestricted agents

B. Full Access Administrators

C. Create replicas

D. Administrators

ANSWER: B D

Explanation:

Full Access Administrators and **Administrators** are the privileged access settings in the Security section of a Domino Server document. The Administrators field identifies the people, groups, or server names authorized to perform standard server-administration activities, such as administering the server through Domino Administrator and carrying out management operations for which administrator authority is required. This field establishes the primary administrative identities for the server.

Full Access Administrators is a distinct, more powerful emergency-administration designation. When an authorized administrator enables full-access administration, Domino grants that person access to databases on the server without being constrained by the databases' normal ACL permissions. This capability is intended for exceptional operational needs, including recovery, troubleshooting, and maintenance where ordinary database access controls would otherwise prevent an administrator from completing necessary work. Domino records and controls this elevated mode so it can be used deliberately rather than as routine access.

Together, these Server document fields define both normal administrative authority and the specially controlled full-access authority needed to administer and recover a Domino server securely. See HCL's Server security documentation and full-access administration documentation.

QUESTION NO: 7

A DAOS-enabled server is configured with a minimum attachment size of 1 MB. A user adds a 500 KB attachment to a document in a database enabled for DAOS. How is that attachment stored?

A. It is stored in the NSF database

B. It is converted into a full-text index entry

C. It is stored as an NLO file in the DAOS repository

D. It is moved to the Administration Requests database

ANSWER: A

Explanation:

The attachment remains **stored in the NSF database** because it does not meet the configured minimum attachment size for DAOS processing. DAOS stores eligible attachments as separate objects in the DAOS repository while the NSF retains references to those objects.

DAOS does not move every attachment automatically. The server-level minimum size determines whether an attachment is eligible, even when the database itself has been enabled for DAOS.

QUESTION NO: 8

What is the role of the AdminP task in a Domino domain?

A. Generate DAOS attachments

B. Route SMTP messages

C. Automate administrative requests

D. Monitor server hardware

ANSWER: C

Explanation:

AdminP, the Administration Process, automates administrative requests in an HCL Domino domain. When an authorized administrator performs supported changes in the Domino Directory—such as renaming a user, deleting a user or group, moving a mail file, or modifying group membership—Domino creates administration request documents in the Administration Requests database, `admin4.nsf`. AdminP runs on applicable servers and processes those requests according to their scheduled execution times and the servers involved. This provides a controlled, asynchronous mechanism for propagating administrative changes throughout the domain rather than requiring administrators to manually update every affected directory entry, database ACL, mail file, or replica. For example, a user rename can result in updates to references to that user in database ACLs and related administrative structures, helping preserve access and consistency after the directory change. Administration requests are replicated to the relevant servers, where AdminP completes the portions of the request appropriate to each server. Administrators can review request status and any errors in `admin4.nsf`, making the process auditable and manageable. Therefore, **Automate administrative requests** correctly states the core role of this Domino server task. See the HCL documentation on the Administration Process and Administration Requests database.