PassQueen
a.k.a dumpsqueen.com

Certified NetIQ Identity Manager Administrator

Novell 050-730

Version Demo

Total Demo Questions: 14

Total Premium Questions: 142

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Identity Manager Concepts	36
Topic 2, Installing Identity Manager	6
Topic 3, Configuring Identity Manager	74
Topic 4, Managing Identity Manager	20
Topic 5, Troubleshooting Identity Manager	6
Total	142

QUESTION NO: 1

When using the Role Mapping Administrator to create a new role, you will need to select a level for the role. Which level defines lower-level privileges?

A. IT Role

B. Mapping Role

C. Systems Role

D. Business Role

E. Permission Role

ANSWER: A

Explanation:

IT Role is correct because the IT-role level represents lower-level, technical privileges within the Identity Manager role hierarchy. It is intended to model technical functions and access responsibilities, such as administration of a particular application, platform, or service. These roles bridge high-level business job functions and the individual permissions that ultimately grant resource access. Role Mapping Administrator uses the selected role level to organize mapped roles according to this hierarchy, allowing business-oriented assignments to be associated with the technical privileges needed to perform them. In this model, an IT role can be used to group and manage related access capabilities in a reusable technical role definition, supporting consistent provisioning and access governance. NetIQ's Roles-Based Provisioning documentation describes the hierarchical use of business, IT, and permission roles and their purpose in defining and assigning access. See the NetIQ Identity Manager Roles-Based Provisioning documentation and the Identity Applications Administration Guide.

QUESTION NO: 2

Which statements correctly distinguish a driver filter from schema mapping? (Choose 2.)

A. A filter controls synchronized classes and attributes.

B. Schema mapping maps class and attribute names between schemas.

C. A filter determines the target container for new objects.

D. Schema mapping replaces transformation policies for value conversion.

E. Each channel requires a separate schema mapping object.

ANSWER: A B

Explanation:

A driver filter controls the synchronization scope by specifying which object classes and attributes are allowed to participate on the Publisher and Subscriber channels. Schema mapping maps Identity Vault class and attribute names to the names used by the connected-system schema. Neither component, by itself, determines an object's target container or performs arbitrary value-format conversion; those tasks are generally handled through placement and transformation policy logic. See the NetIQ Identity Manager documentation for driver, filter, schema-mapping, and policy configuration guidance.

QUESTION NO: 3

Which actions are appropriate when troubleshooting a driver that is failing to communicate with a Remote Loader? (Choose 2.)

A. Verify that the Remote Loader service is running.

B. Verify the configured host, port, and authentication information.

C. Delete all associations for the driver.

D. Disable the driver filter.

E. Change every User object to the Group class.

ANSWER: A B

Explanation:

Verifying that the Remote Loader service is running confirms that a process is listening for the driver connection. Verifying the configured Remote Loader host, port, and authentication information helps identify connection or credential mismatches between the driver and Remote Loader. Driver trace and Remote Loader trace can then provide additional diagnostic detail. Changing the Identity Vault object's association value or disabling the driver filter does not resolve a basic Remote Loader connectivity failure. See the Remote Loader Administration Guide.

QUESTION NO: 4

Which pre-defined jobs operate at the driver set level? (Choose 2.)

A. Driver Health

B. Schedule Driver

C. Subscriber Channel Trigger

D. Random Password Generator

E. Password Expiration Notification

ANSWER: A E

Explanation:

Driver Health and **Password Expiration Notification** are predefined Identity Manager jobs whose operational scope is the Driver Set object. A Driver Set is the container for the drivers participating in an Identity Manager deployment, so jobs placed at this level can use Driver Set-wide configuration and act across the drivers or connected systems represented by that set.

The Driver Health job provides Driver Set-level monitoring of driver health and status. This makes it suitable for centralized operational oversight: its job configuration is associated with the Driver Set rather than a particular driver channel. Password Expiration Notification is also configured at the Driver Set level because it performs a coordinated password-expiration notification function for identities governed through the Driver Set. The job can be scheduled from the Driver Set's job configuration, allowing the notification process to run under a common administrative scope.

NetIQ Identity Manager documentation describes Driver Sets as the objects that contain and manage drivers and their associated configuration. It also documents predefined jobs and their assignment within the Identity Manager administration model. See the NetIQ Identity Manager 4.8 documentation and the Identity Manager Administration Guide for Driver Set and job administration details.

QUESTION NO: 5

When installing the Active Directory Driver, which options can you choose when selecting the desired form for the placement of new objects? (Choose 2.)

A. Flat

B. Level

C. Parallel

D. Mirrored

E. Structured

F. Bi-directional

G. Single Organizational Unit

ANSWER: A D

Explanation:

The Active Directory Driver configuration supports two placement forms for newly created objects: **Flat** and **Mirrored**. Flat placement puts new objects into a specified single Active Directory container. This is appropriate when the target directory does not need to reproduce the eDirectory organizational hierarchy and administrators want all provisioned objects of a given type to be created in one managed location.

Mirrored placement preserves the source container relationship by creating or using a corresponding hierarchy beneath the configured target container. This enables objects from different source containers to be placed into matching Active Directory organizational-unit paths, which is useful when the directory structure itself carries administrative, geographic, departmental, or policy significance. The driver's placement configuration therefore lets an administrator choose between a consolidated target location and a hierarchy that reflects the source tree.

These settings are part of the Active Directory Driver configuration workflow and determine where objects are created when the driver provisions them to Active Directory. See the NetIQ Identity Manager Active Directory Driver documentation and the NetIQ Identity Manager documentation library.

QUESTION NO: 6

Which XPATH operator is used to select all descendent nodes at any depth below the current stated node?

A. *

B. |

C. @

D. &

E. //

ANSWER: E

Explanation:

`//` is the XPath descendant-or-self location-path abbreviation. When used after a current context node, it traverses through that node's descendant hierarchy at any depth, rather than being limited to immediate children. For example, `book//title` selects every `title` element that is a descendant of the current `book` element, including titles nested several levels below it. In Identity Manager policy expressions, XPath is used to navigate the XML document being processed; this descendant search is useful when the required element may occur in different nested locations. Formally, `//` is shorthand for `/descendant-or-self::node()/`, which explains why it searches recursively through the XML tree beginning from the applicable context. The XPath specification defines this abbreviation and its descendant-or-self semantics, while the NetIQ Identity Manager documentation describes XPath as the mechanism used by policy conditions and actions to query XML data. See the W3C XPath path abbreviation specification and the NetIQ Identity Manager policy XPath documentation.

QUESTION NO: 7

An Identity Vault object is moved from one container to another. Which XDS operation represents this change for driver policy processing?

A. `rename`

B. `add`

C. `delete`

D. `modify`

E. `query`

ANSWER: A

Explanation:

A move or name change is represented by a `rename` operation in the XDS event vocabulary. The operation identifies the affected object and provides the information required for the driver and its policies to process the new name or location. An `add` creates an object, a `delete` removes one, and a `modify` changes attribute values rather than an object's distinguished name. See the Identity Manager Driver Development documentation.

QUESTION NO: 8

Which drivers have Remote Loader capability? (Choose 3.)

A. JDBC

B. LDAP

C. eDirectory

D. Active Directory

E. Entitlement Services

ANSWER: A B D

Explanation:

The drivers with Remote Loader capability in this question are **JDBC**, **LDAP**, and **Active Directory**. Remote Loader provides a secure mechanism for the Identity Manager engine to communicate with a driver shim running on a separate server. This architecture is especially useful when the connected application, directory, or database must be accessed from a host within a different network segment, when the required native client libraries are installed on a remote system, or when direct connectivity from the Identity Vault server is not appropriate.

The JDBC driver can use Remote Loader where database connectivity and JDBC driver libraries reside on the remote host. The LDAP driver can similarly run remotely to connect to an LDAP-compliant directory from the system with the necessary network access. The Active Directory driver is a primary Remote Loader use case because the driver can operate on a Windows server close to, or within, the Active Directory environment. In each case, the driver communicates with the Identity Manager engine through the Remote Loader protocol while maintaining the driver's normal synchronization and event-processing functions. See the NetIQ Identity Manager documentation and the Remote Loader Administration Guide.

QUESTION NO: 9

If you map the eDirectory attribute of Login Expiration Time to the Active Directory attribute of accountExpires, when does the account in Active Directory expire?

A. A day later than the time set in eDirectory

B. A day earlier than the time set in eDirectory

C. An hour later than the time set in eDirectory

D. At the same time as the time set in eDirectory

E. An hour earlier than the time set in eDirectory

ANSWER: B

Explanation:

A day earlier than the time set in eDirectory is correct because eDirectory Login Expiration Time and Active Directory accountExpires use different expiration-date semantics. eDirectory treats the configured login-expiration date as the last date on which the user may log in. Active Directory stores accountExpires as a Windows FILETIME value and evaluates the expiration at the start of the stored date. Consequently, when the same date value is transferred directly, Active Directory denies the account at midnight beginning that date, rather than allowing access through that date as eDirectory does. The practical result is that the account becomes unavailable one calendar day sooner in Active Directory.

This distinction is important when synchronizing users with the Identity Manager Active Directory driver. A mapping or transformation policy that needs equivalent end-user behavior must account for the one-day difference, rather than assuming that two date-like attributes have identical operational meaning. Microsoft documents that accountExpires is a 64-bit value representing the account-expiration time and is interpreted by Active Directory for account logon processing. See the Active Directory accountExpires attribute reference and the NetIQ Identity Manager documentation.

QUESTION NO: 10

What is the primary purpose of schema mapping in an Identity Manager driver configuration?

A. Map object and attribute names between schemas

B. Store pending synchronization events

C. Set the Remote Loader password

D. Schedule driver startup and shutdown

E. Assign approvers to a workflow

ANSWER: A

Explanation:

Schema mapping defines the correspondence between Identity Vault classes and attributes and the classes and attributes expected by the connected system. For example, it can map an Identity Vault user class or attribute name to its connected-system equivalent. This mapping enables the engine and driver shim to interpret object and attribute data consistently even when the two systems use different schema names. See the NetIQ Identity Manager documentation.

QUESTION NO: 11

What are benefits of using Policy Builder? (Choose 2.)

A. It is built on open standards.

B. It enforces password complexity.

C. It is a GUI with command line capabilities.

D. It minimizes the need for XLST stylesheets.

E. It provides a graphical interface to help data cleansing.

F. It provides a graphical interface for rapid development of policies.

ANSWER: D F

Explanation:

Policy Builder is intended to make Identity Manager policy authoring faster and more approachable by presenting policy logic in a graphical authoring environment. Therefore, **"It provides a graphical interface for rapid development of policies."** is a direct benefit: administrators can construct rules, conditions, actions, and transformations visually rather than having to hand-author every policy component. This supports faster implementation and easier maintenance of driver policies.

"It minimizes the need for XLST stylesheets." is also correct. Policy Builder provides graphical constructs for common filtering, mapping, conditional processing, and data-transformation requirements. These capabilities reduce the occasions where an administrator must create and maintain custom XSLT to manipulate XML event documents. XSLT can still be used where specialized transformations are required, but the visual policy tools address many routine integration tasks without that additional stylesheet-development overhead.

These benefits align with NetIQ Identity Manager's policy-development approach, in which policy authoring tools provide reusable graphical components for processing identity data and events. See the NetIQ Identity Manager Policy Designer documentation and the NetIQ Identity Manager documentation library.

QUESTION NO: 12

Which users have access to the team configuration page? (Choose 2.)

A. Role Manager

B. Team Manager

C. Security Administrator

D. Resource Manager

E. Provisioning Manager

ANSWER: B C

Explanation:

The correct selections are **Team Manager** and **Security Administrator**. In the Identity Manager Roles Based Provisioning Module (RBPM) User Application, the Team Configuration page is an administrative function for maintaining the organizational team structure and the settings that govern how teams are used. A Team Manager is granted access because this role is responsible for managing teams, including their membership and team-related configuration. A Security Administrator also has access because the role administers security-related configuration and delegated administrative capabilities within the User Application, which includes access to protected configuration areas such as team administration. These permissions support controlled delegation: team administration can be performed by designated team-management personnel, while security administrators retain the broader authority needed to administer and secure the application environment. NetIQ's Identity Manager documentation describes the User Application's administrative roles and the delegated administration model used for teams and security administration. See the NetIQ Identity Manager Applications Administration Guide and the Identity Manager documentation library.

QUESTION NO: 13

The User Application Security Model uses domains to create sets of configurations and permissions that can be assigned to different user types. Under the Provisioning domain, which permission allows the user to retract selected provisioning requests when they are in progress?

A. Retract PRD

B. Initiate PRD

C. Configure Delegate

D. View Running PRD

E. Configure Availability

ANSWER: A

Explanation:

Retract PRD is the Provisioning-domain permission that authorizes a user to withdraw a selected provisioning request that is currently in progress. In the Identity Manager User Application, provisioning requests are initiated and then proceed through the request-definition workflow, which can include approvals, fulfillment activities, and other processing stages. Granting this permission allows an authorized requester to stop and retract an applicable active request rather than allowing it to continue through the workflow.

This capability is useful when the original request is no longer needed, was submitted with incorrect details, or must be cancelled before fulfillment. The permission is deliberately part of the Provisioning domain because it governs an action on the lifecycle of a provisioning request. Administrators assign this permission through the User Application security model to the roles or users that need authority to manage their own active requests. NetIQ's Identity Manager documentation describes the User Application's role- and permission-based security administration model and provisioning-request functionality: NetIQ Identity Manager documentation and Identity Manager 4.0.2 documentation.

QUESTION NO: 14

Which task within Novell iManager allows administrators to view all objects that are associated with a particular Novell IDM driver?

A. Object Inspector

B. Driver Inspector

C. DriverSet Inspector

D. Driver Cache Inspector

ANSWER: B

Explanation:

Driver Inspector is the iManager task designed to examine a selected Identity Manager driver and display the eDirectory objects associated with that driver. In Identity Manager, a driver maintains associations that connect eDirectory objects to corresponding objects in the connected application. Administrators need a driver-focused view to identify the objects that have associations, inspect their association information, and perform administration in the context of the selected driver. Driver Inspector supplies that context: the administrator selects the Driver Set and driver, then uses the task to view the associated objects and relevant driver-association details. This is particularly useful for validating whether users, groups, or other objects have been linked to the connected system as intended and for investigating synchronization or provisioning issues involving a specific driver. The task is part of the Identity Manager administration functionality provided through the iManager plug-ins, rather than a general eDirectory browsing view. NetIQ Identity Manager documentation describes administration of drivers and their associated objects through the Identity Manager plug-ins for iManager. See the NetIQ Identity Manager documentation library and the NetIQ iManager documentation library for Identity Manager plug-in and driver administration guidance.