



주제 4	<ul style="list-style-type: none"> <li>• Foundational Concepts: Covers the core purpose of identity security, key IdentityIQ terminology, system components, and how rules, tasks, workflows, and business modeling fit into the platform.</li> </ul>
------	---

>> IdentityIQ-Associate시험대비 공부하기 <<

## IdentityIQ-Associate시험대비 공부하기최신버전 인증덤프

ExamPassdump에서 제공해드리는 IT인증시험대비 덤프를 사용해보신적이 있으신지요? 만약에 다른 과목을 사용해 보신 분이라면 SailPoint IdentityIQ-Associate덤프도 바로 구매할것입니다. 첫번째 구매에서 패스하셨다면 덤프에 신뢰가 있을것이고 불합격받으셨다하더라도 바로 환불해드리는 약속을 지켜드렸기때문입니다. 처음으로 저희 사이트에 오신 분이라면SailPoint IdentityIQ-Associate덤프로 첫구매에 도전해보지 않으실래요? 저희 덤프로 쉬운 자격증 취득이 가능할것입니다.

### 최신 Identity Security Engineer IdentityIQ-Associate 무료샘플문제 (Q65-Q70):

**질문 # 65**

Is this statement true about group factories and/or populations?  
New groups are created as a result of executing a task.

- A. Yes
- B. No

**정답: A**

**설명:**

The statement is true. In SailPoint IdentityIQ, group factories are used to generate identity groups dynamically based on identity attribute values or configured grouping logic. A group factory defines the rule or attribute basis for grouping identities, but the actual creation or refresh of the resulting groups occurs when the appropriate task is executed. For example, a group factory might be configured to create groups by department, location, cost center, or business unit. When the task runs, IdentityIQ evaluates identities against the factory definition and creates or updates the corresponding groups.

This differs from populations, which are typically defined sets of identities used for targeting, filtering, reporting, or governance scoping. Group factories are more generation-oriented because they can produce multiple group objects from identity data. The task execution step is important because it materializes the groups so they can be used in IdentityIQ operations.

Therefore, new groups can be created as a result of executing a task tied to group factory processing.

Reference topics: Identity Modeling - groups and populations, group factories, identity grouping, and task- driven group creation.

**질문 # 66**

Is this statement true for the use of applications?  
They are defined in IdentityIQ to represent the systems from which identities are read.

- A. No
- B. Yes

**정답: A**

**설명:**

The statement is not technically accurate. In SailPoint IdentityIQ, applications are defined to represent external systems, platforms, directories, databases, or resources from which account, group, entitlement, and attribute data are aggregated, and in some cases to which provisioning changes are written. IdentityIQ does not generally "read identities" directly from applications. Instead, it reads account records and associated attributes from applications, then uses identity correlation, authoritative-source logic, and identity refresh processing to construct or update IdentityCubes.

This distinction is fundamental. An application may be an authoritative source, such as an HR system, where account attributes contribute heavily to identity creation and lifecycle state. However, the object read from the source is still an account or source record, not an IdentityIQ identity object. The identity is modeled inside IdentityIQ after aggregation and correlation occur.

Therefore, the more precise statement is that applications represent systems from which IdentityIQ reads account and access data,

not systems from which IdentityIQ simply reads identities. Reference topics: Applications, application definition, account aggregation, authoritative applications, correlation, IdentityCube creation, and Identity Modeling.

**질문 # 67**

Is this a purpose of identity governance and administration (IGA)?  
Recording which data a user downloads

- A. No
- B. Yes

**정답: A**

**설명:**

Recording which data a user downloads is not a core purpose of Identity Governance and Administration in SailPoint IdentityIQ. IGA is concerned with governing identities, accounts, access, entitlements, roles, policy violations, certifications, access requests, and provisioning. Its central objective is to answer questions such as who a user is, what access they have, whether that access is appropriate, who approved it, and whether access complies with defined business and security policies.

Tracking the specific files, records, or data objects downloaded by a user is typically associated with data activity monitoring, data loss prevention, security information and event management, or user behavior analytics. IdentityIQ may integrate with other systems and can govern access to applications or repositories that contain sensitive data, but it does not primarily function as a tool for recording every data download event.

In IdentityIQ terms, the governance focus is identity security: access visibility, access certification, policy enforcement, role modeling, lifecycle management, and provisioning controls. Reference topics: Foundational Concepts, purpose of identity security, common IdentityIQ terms, governance model, certifications, policies, and provisioning.

**질문 # 68**

Is this statement true for the use of tasks?  
They can be used to confirm that the correct access is included in a role.

- A. No
- B. Yes

**정답: A**

**설명:**

No. In SailPoint IdentityIQ, tasks are used to execute defined system operations, often as background or scheduled processes.

Common task usage includes account aggregation, identity refresh, entitlement aggregation, maintenance activities, report execution, role processing, and other repeatable administrative operations. A task may calculate, update, import, refresh, or process data, but it does not itself perform the governance decision of confirming whether access in a role is correct.

Confirming that the correct access is included in a role is a governance review function, most closely associated with role certification, especially role composition certification. In that process, a role owner or designated certifier reviews the access profiles, entitlements, permissions, or requirements contained in a role and decides whether they are appropriate. The confirmation requires business judgment and reviewer action, not merely task execution.

A task may support role governance indirectly by refreshing role data or generating background processing, but the validation of role contents belongs to certifications and access governance. Therefore, this statement is not accurate for the use of tasks. Reference topics: Foundational Concepts, tasks versus workflows, Governance, role composition certification, Access Modeling, and role governance.

**질문 # 69**

Does this correctly describe Lifecycle Manager?  
Technology that automates the collection and provisioning of identity access data for enterprise applications, cloud offerings, and infrastructure components such as operating systems, directories, and databases

- A. No
- B. Yes

**정답: A**

