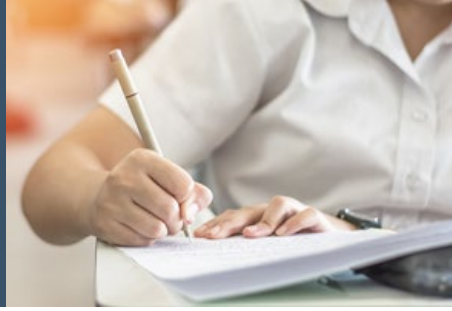
IBM Security Engineer
Study Guide



This study guide will help prepare you for the IBM **Security Engineer** Certification Examination.

What's in the Study Guide

This study guide covers:

- Manage Access Controls and Authorization in IBM Cloud

How to Use this Study Guide

1) **Read the content.**

2) **Take notes.**

3) **Answer practice questions.**

Preparation

Thorough study is essential to a successful outcome on the exam.

- Clear your schedule.
- Find a quiet place to study.
- Focus on the content.

- Open the associated on-line course for reference.
- Locate the Study Guide.
- Download the Study Guide.

- Print a copy of the Study Guide.
- Take notes.

Modules and Objectives

Modules

1. Manage Access Controls and Authorization in IBM Cloud

Objectives

- Implement IAM on IBM Cloud services
- Implement authentication with App ID
- Manage access to IBM Cloud resources
- Report and audit user activity for security insights

Module 1: Manage Access Controls and Authorization in IBM Cloud Introduction and Objectives

In Module 1 of the Study Guide the subject matter:

- Explains how to implement IAM on IBM Cloud services.
- Implement authentication with App ID.
- Manage access to IBM Cloud resources.
- Report and audit user activity for security insights.

Lessons

- Identity and Access Management on IBM Cloud Services
- App ID Authentication
- Managing Access for Classic Infrastructure
- User Activity for Security Insights
- Module Summary
- Knowledge Check Questions

Objectives

- Implement IAM on IBM Cloud services
- Implement authentication with App ID
- Manage access to IBM Cloud resources
- Report and audit user activity for security insights

Module 1: Manage Access Controls and Authorization in IBM Cloud
IBM Cloud IAM roles

IBM Cloud IAM Roles
All services that are organized in a resource group in your account are managed by using IBM Cloud Identity and Access Management (IAM). Account owners are automatically assigned the account administrator role.

Platform management roles
With platform management roles, users can be assigned varying levels of permission for performing platform actions within the account and on a service. Some services might map specific actions to the platform management roles that are related to the management of the service rather than to the access of the service. As an example, see the following table that details the Kubernetes Service service actions that are mapped to these roles.

Platform management role	Actions	Example actions for Kubernetes Service
Viewer	Can view service instances, but can't modify them	• List clusters • View details for a cluster
Editor	Perform all platform actions except for managing the account and assigning access policies	• Bind a service to a cluster • Create a webhook
Operator	Perform platform actions required to configure and operate service instances, such as viewing a service's dashboard	• Add or remove worker nodes • Restart or reload worker nodes • Bind a service to a cluster
Administrator	Perform all platform actions based on the resource this role is being assigned, including assigning access policies to other users	• Remove a cluster • Create a cluster • Update user access policies • All actions a viewer, editor, and operator can perform

Module 1: Manage Access Controls and Authorization in IBM Cloud
IBM Cloud IAM roles

IBM Cloud IAM Roles Cont'd

Service access roles

Service access roles enable users to be assigned different levels of permission for calling the service's API and accessing the UI for the service. The following table provides example actions that can be taken depending on the assigned roles based on using the Object Storage service.

Service Access Role	Actions	Example actions for Object Storage service
Reader	Perform read-only actions within a service, such as viewing service-specific resources	List and download objects
Writer	Permissions beyond the reader role, including creating and editing service-specific resources	Create and destroy buckets and objects
Manager	Permissions beyond the writer role to complete privileged actions as defined by the service, plus create and edit service-specific resources	Manage all aspects of data storage, create, and destroy buckets and objects

Module 1: Manage Access Controls and Authorization in IBM Cloud
Managing authentication

Managing Authentication

Identity providers (IdP's) add a level of security for your mobile and web apps, through authentication. With IBM Cloud® App ID, you can configure one or several identity providers to create a custom sign-in experience for your users.

App ID interacts with identity providers by using various protocols such as OpenID Connect, SAML, and more. For example, OpenID Connect is the protocol that is used with many social providers such as Facebook, Google.

Enterprise providers such as Azure Active Directory or Active Directory Federation Service, generally use SAML as their identity protocol.

For Cloud Directory, the service uses SCIM to verify identity information.

Configuring token lifetime

App ID uses tokens to identify users and secure your resources.

Token type	Description
Access	The length of time for which access tokens are valid. The smaller the value, the more protection that you have in cases of token theft.
Refresh	The length of time for which refresh tokens are valid. The smaller the number, the more frequently a user must sign themselves in.
Anonymous	The length of time for which anonymous tokens are valid. Anonymous tokens are assigned to users the moment they begin interacting with your app. When a user signs in, the information in the anonymous token is then transferred to the token associated with the user.

Module 1: Manage Access Controls and Authorization in IBM Cloud
Securing your Data in App ID

Securing your Data in App ID

To ensure that you can securely manage your data when you use IBM Cloud® App ID, it is important to know exactly what data is stored and encrypted and how you can delete any stored personal data.

How your data is stored and encrypted in App ID

App ID stores and encrypts user profile attributes. You can add a higher level of encryption control to your data at rest (when it is stored) by enabling integration with a _Key Management Service_ (KMS).

Managing your own keys

App ID uses envelope encryption to implement both provider-managed and customer-managed keys. Envelope encryption describes encrypting one encryption key with another encryption key. The key used to encrypt the actual data is known as a data encryption key (DEK). The DEK itself is never stored but is wrapped by a second key that is known as the key encryption key (KEK) to create a wrapped DEK. To decrypt data, the wrapped DEK is unwrapped to get the DEK. This process is possible only by accessing the KEK, which in this case is your root key that is stored in your KMS.

Key Protect keys are secured by FIPS 140-2 Level 3 certified cloud-based hardware security modules (HSMs), and Hyper Protect Crypto Services keys are secured by FIPS 140-2 Level 4 certified cloud-based HSMs.

Module 1: Manage Access Controls and Authorization in IBM Cloud
Managing Classic Infrastructure Access

Managing Classic Infrastructure Access

When you invite a user to your account, you can select from three classic infrastructure permission sets that assign bulk access: View only, Basic user, Super user.

Classic infrastructure permissions

Support center account management access is recommended for users working with classic infrastructure resources. To perform many tasks when working with classic infrastructure resources, such as creating or deleting a virtual server instance, users must have access to work with support cases.

Assigning classic infrastructure permissions

You must be assigned the Manage users classic infrastructure permission and be an ancestor of the user within the classic infrastructure user hierarchy. Account owners have full access to the account, so they do not see the permissions on the page. Individual users can't edit their own permissions, and they also don't see permissions on the page.

When a classic infrastructure user invites another user to the account, the classic infrastructure user becomes the parent user. When a child of a parent invites other users to the account, those users become descendants of the original parent, who is now considered their ancestor.

Module 1: Manage Access Controls and Authorization in IBM Cloud
Auditing Access To Resources

Auditing Access To Resources

If you want to determine which users, access groups, service IDs, and services can access a specific resource, you can download a report from the Resource list in your account. Auditing who has access to a specific resource can be helpful to ensure that you're using the principle of least privilege. This means that you're giving the least amount of access that is required to only the users who need it. Each report gives you a list of what entities have access at that time. You can use the report to determine who has access that doesn't need it, and then you can take action to reduce the number of access policies and inflated access across the account.

Report types

There are two report formats that you can choose from: JSON or CSV. The CSV report is in an easier to read format, but it doesn't include all of the information that is available in the JSON report.

Module 1: Manage Access Controls and Authorization in IBM Cloud
Available Activity Insights Rule Packages

Available Activity Insights Rule Packages

Activity Insights compares your user and application activity against predefined rule packages to identify suspicious behavior.

Key Protect

Key Protect helps you provision encrypted keys for apps across IBM Cloud services.

Rule	Finding Type	Description
kms secrets delete - high risk API	ata-kms-key-deleted	Reports when a key is deleted.
kms.secrets.unwrap outside change control window - indicative API	ata-kms-key-unwrap-ccw	Reports when a key is unwrapped between 1700 and 0800 (next day).
The following is a service instance rule instantiated for KMS. high risk API.	ata-kms-service	Reports when one of the following are observed: A KMS instance is created. A KMS instance is renamed or service plan changed. A KMS instance is deleted. An API key is created for a KMS instance through the Service credentials section of the service instance UI. An API key that is associated with a KMS instance is deleted from the Service credentials section of the service instance UI. When binding a KMS instance to an application. When unbinding a KMS instance to an application.

Module 1: Manage Access Controls and Authorization in IBM Cloud
Available Activity Insights Rule Packages

Available Activity Insights Rule Packages Cont'd

Kubernetes Service

Kubernetes Service helps you to deploy highly available containerized apps in a way that allows you to automate, isolate, secure, manage, and monitor your workloads across zones and regions.

Rule	Finding Type	Description
Very high risk Kubernetes Service activity	ata-iks-high-risk	Reports when one of the following behaviors are observed: A public or private ALB is created in the cluster. An existing IBM Cloud infrastructure subnet is added to a cluster.
Kubernetes Service change to logging detected	ata-iks-logging-change	Reports when changes to logging settings occur. These changes include the following: A logging filter is created. A logging filter is updated.
Indicative IKS API exceed threshold within time window	ata-iks-indicative-api-threshold	Reports when within 30 minutes more than 10 worker nodes are updated.
Indicative IKS API outside of change control window	ata-iks-indicative-api-ccw	Reports when a worker node is updated between 1700 and 0800 (next day).
Service instance high risk API	ata-iks-service	Reports when one of the following are observed: A Kubernetes Service instance is created. A Kubernetes Service instance is renamed or service plan changed.

Module 1: Manage Access Controls and Authorization in IBM Cloud
What is Security Insights?

What is Security Insights?

With IBM Cloud® Security and Compliance Center, you can take advantage of built-in insights to analyze your user activity and network communication in order to identify unauthorized or suspicious behavior in your IBM Cloud resources or applications.

How does Security Insights work?

Activity Insights

- By comparing user activity that is logged by Activity Tracker against predefined rule packages, you can identify suspicious behavior as it relates to your IBM Cloud resources, which can help to prevent malicious attacks on your applications.

Network Insights

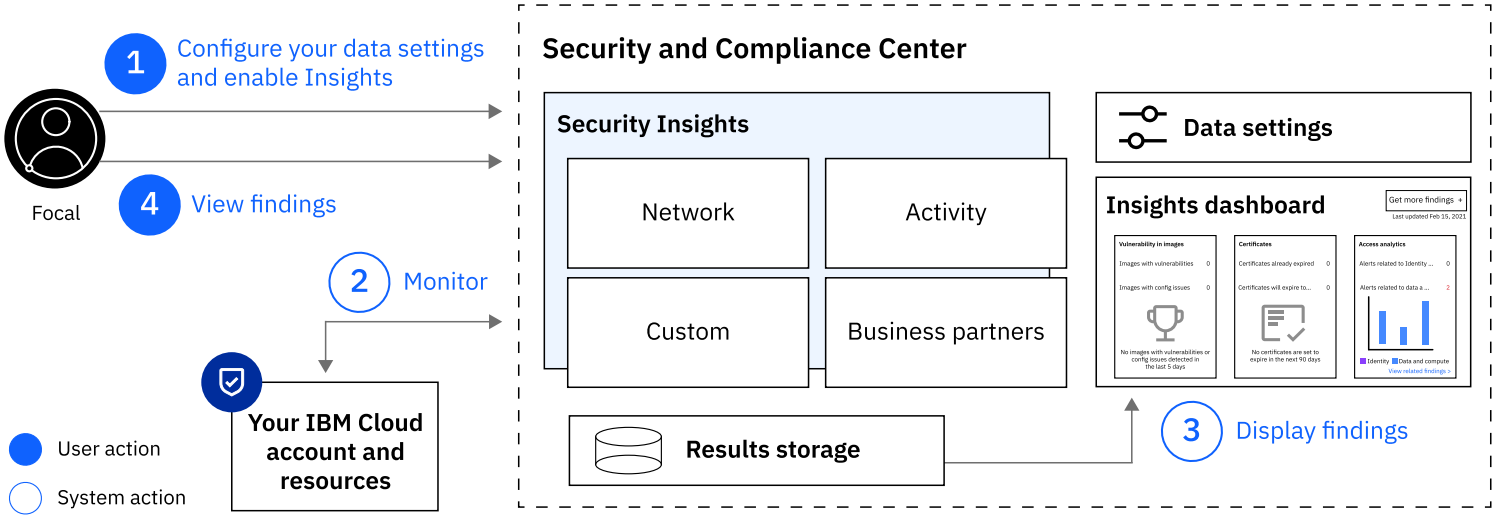
- By monitoring and analyzing your VPC flow logs, you can identify suspicious behavior through your the network communication between your VPC interfaces. For example, you can identify Virtual Server Instances that might be compromised or attempts to compromise your VSIs.

Custom insights

- To view all of your security alerts in one place, you can integrate your own security tools with the Security and Compliance Center by using the Findings API.

Business partners

- If you work with one of our business partners such as Caveonix, Twistlock, or NeuVector, you can easily integrate your findings with the Security and Compliance Center to further assess the risk and compliance posture of your workloads that are deployed on IBM Cloud.



Module 1: Manage Access Controls and Authorization in IBM Cloud
Enabling Network Insights

Enabling Network Insights

With Security Insights, formerly known as IBM Cloud® Security Advisor, you can continuously analyze your Virtual Private Cloud (VPC) network interface flow logs to detect any suspicious activity by using learned patterns and threat intelligence.

Connecting to Cloud Object Storage

Before you can analyze your network communication, Security Advisor must have access to your network flow logs that are stored in Cloud Object Storage. To create the connection between the services, you must store the logs in a Cloud Object Storage bucket and then grant the service access to the bucket.

What Classifies As Suspicious Network Traffic?

The behavioral patterns of peers that are used as scanners, for mining cryptocurrency, as part of a botnet, for anonymization services, or have been found to distribute malware are continuously monitored by IBM X-Force. When you enable Network Insights, your VPC interface flow logs are analyzed for behavioral patterns and compared to the intelligence that is gathered by IBM X-Force to detect potentially compromised VSIs that run in your VPC.

Module 1: Manage Access Controls and Authorization in IBM Cloud Summary

Module Summary

- All services that are organized in a resource group in your account are managed by using IBM Cloud Identity and Access Management (IAM). Account owners are automatically assigned the account administrator role.
- Service access roles enable users to be assigned different levels of permission for calling the service's API and accessing the UI for the service. The following table provides example actions that can be taken depending on the assigned roles based on using the Object Storage service.
- Identity providers (IdP's) add a level of security for your mobile and web apps, through authentication. With IBM Cloud® App ID, you can configure one or several identity providers to create a custom sign-in experience for your users.
- To ensure that you can securely manage your data when you use IBM Cloud® App ID, it is important to know exactly what data is stored and encrypted and how you can delete any stored personal data.
- When you invite a user to your account, you can select from three classic infrastructure permission sets that assign bulk access: View only, Basic user, Super user.
- If you want to determine which users, access groups, service IDs, and services can access a specific resource, you can download a report from the Resource list in your account.
- Activity Insights compares your user and application activity against predefined rule packages to identify suspicious behavior.
- Kubernetes Service helps you to deploy highly available containerized apps in a way that allows you to automate, isolate, secure, manage, and monitor your workloads across zones and regions.
- With Security Insights, formerly known as IBM Cloud® Security Advisor, you can continuously analyze your Virtual Private Cloud (VPC) network interface flow logs to detect any suspicious activity by using learned patterns and threat intelligence.
- With IBM Cloud® Security and Compliance Center, you can take advantage of built-in insights to analyze your user activity and network communication in order to identify unauthorized or suspicious behavior in your IBM Cloud resources or applications.

Module 1
Check Your Knowledge

Question 1.

An administrator is setting up access groups for the federated users of an organization in IBM Cloud. All managers must be granted Manager access to Cloud Object Storage and Cloudant. What is the best way to set up this requirement?

A. Create two access groups, one for each service, and assign the Manager role to each individual service and add all required users to the access groups.

B. Create one access group with an access policy that assigns Manager role to All Identity and Access enabled services and add all required users to the access group.

C. Create one access group with an access policy that assigns Manager role to each individual service and a dynamic rule that matches users whose federated identity contains the attribute isManager=true.

D. Create two access groups, one for each service, and assign the Manager role to each individual service, and a dynamic rule that matches users whose federated identity contains the attribute isManager=true.

Answer C. Create one access group with an access policy that assigns Manager role to each individual service and a dynamic rule that matches users whose federated identity contains the attribute isManager=true.

Module 1
Check Your Knowledge

Question 2.

To be able to analyze network communication, IBM Cloud Security Insights must have access to the network flow logs. Which type of storage is used for network flow logs?

A. Block Storage
B. File Storage
C. VMware vSAN
D. Cloud Object Storage

Answer D. Cloud Object Storage is used for network flow logs.

Module 1
Check Your Knowledge

Question 3.

Which Platform management role can perform all platform actions except for managing the account and assigning access policies?

A. Viewer
B. Editor
C. Operator
D. Administrator

Answer B. An editor can perform all platform actions except for managing the account and assigning access policies

Module 1
Check Your Knowledge

Question 4.

What is an example action that a service access reader role would do for Object Storage service?

A. List and download objects
B. Create and destroy buckets and objects
C. Manage all aspects of data storage
D. Edit buckets and objects

Answer A. A reader role would list and download objects.

Module 1
Check Your Knowledge

Question 5.

Which IBM Cloud App ID token type is described as the smaller the value, the more protection you have in cases of token theft?

A. Access
B. Refresh
C. Anonymous

Answer A. Access token type offers more protection in cases of token theft.

Module 1
Check Your Knowledge

Question 6.

What data is stored and encrypted in App ID?

A. App ID encrypts Kubernetes data
B. App ID encrypts service profiles
C. App ID encrypts Open Shift data
D. App ID stores and encrypts user profile attributes.

Answer D. App ID stores and encrypts user profile attributes.

Module 1
Check Your Knowledge

Question 7.

When you invite a user to your account, you can select from three classic infrastructure permission sets that assign bulk access. What are they? Select all that apply.

A. Super user
B. IBM-managed key
C. Basic user
D. View only

Answer A, C and D. When you invite a user to your account, you can select from three classic infrastructure permission sets that assign bulk access: View only, Basic user, Super user.

Module 1
Check Your Knowledge

Question 8.

Why would you download a report from a Resource list in your account?

A. To determine which users can access a specific resource
B. To retrieve service role data
C. To delete resources
D. To access administrative powers

Answer A. If you want to determine which users, access groups, service IDs, and services can access a specific resource, you can download a report from the Resource list in your account.

Module 1
Check Your Knowledge

Question 9.

What available activity insights rule package finding type reports when a key is deleted?

A. ata-kms-service
B. ata-kms-key-unwrap-ccw
C. ata-kms-key-deleted
D. Ata-kms-key-access

Answer C. ata-kms-key-deleted reports when a key is deleted.

Module 1
Check Your Knowledge

Question 10.

What does IBM Cloud Security and Compliance Center do? Select all that apply.

A. Encrypt data
B. Analyze Use activity
C. Identify unauthorized or suspicious behavior
D. Analyze Network Traffic

Answer B, C, and D. With IBM Cloud® Security and Compliance Center, you can take advantage of built-in insights to analyze your user activity and network traffic in order to identify unauthorized or suspicious behavior in your IBM Cloud resources or applications.