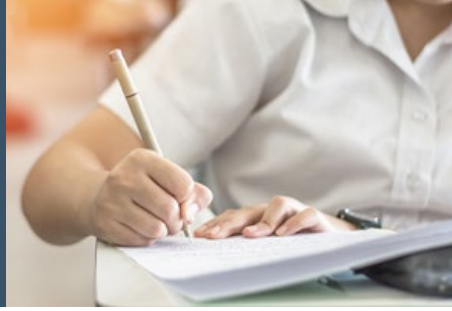
IBM Security Engineer
Study Guide



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

What's in the Study Guide

This study guide covers:

- Secure Cloud Compute 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. Secure Cloud Compute in IBM Cloud
2. Securing Internal and External Connections
3. Identifying Solutions in Code Engine
4. Security Controls in Classic Infrastructure

Objectives

1. Secure infrastructure and hybrid cloud connections in IBM Cloud
2. Secure Cloud compute in IBM Cloud
3. Secure Kubernetes services in IBM Cloud
4. Secure VMware solutions in IBM Cloud
5. Manage access controls and authorization in IBM Cloud
6. Manage configuration of security and compliance solutions

Module 1: Secure Cloud Compute in IBM Cloud
Introduction and Objectives

In Module 1 of the Study Guide the subject matter:

- Covers secure interconnected services with VSIs in VPC, Power VSIs, Code Engine, and security controls in Classic infrastructure.

Lessons

- Securing interconnected services in IBM Cloud with VSIs in VPCs
- Distinguishing secure connections to databases (Getting Endpoints)
- Differentiating secure connections to storage
- Choose characteristics of secure connections to integration APIs
- Recognize connections to Watson APIs
- Module Summary
- Knowledge Check Questions

Objectives

- Secure interconnected services with VSIs in VPC

Module 1: Secure Cloud Compute in IBM Cloud
Service Endpoints Integration

Service Endpoints Integration

All Cloud Databases deployments offer integration with IBM Cloud Service Endpoints. It gives you the ability to enable connections to your deployments from the public internet and over the IBM Cloud Private network.
Service Endpoints are available in all IBM Cloud Multi-Zone Regions and some Single-Zone Regions. Deployments in all other regions are able to use Service Endpoints.

Public Endpoints

Public endpoints provide a connection to your deployment on the public network. At provision time, a public endpoint is the default option for all deployments. Your environment needs to have internet access to connect to a deployment.

Private Endpoints

A deployment with a service endpoint on the private network gets an endpoint that is not accessible from the public internet. All traffic is routed to hardware dedicated to Cloud Databases deployments and remains on the IBM Cloud Private network. All traffic to and from this endpoint is free and unmetered on the condition that the traffic remains in IBM Cloud. After your environment has access to the IBM Cloud Private network, an internet connection is not required to connect to your deployment.

Module 1: Secure Cloud Compute in IBM Cloud
Virtual Private Endpoints

Virtual Private Endpoints

IBM Cloud® Virtual Private Endpoint (VPE) for IBM Cloud® Virtual Private Cloud provides connection points to IBM services on the IBM private network from your VPC network.

Setting up your VPE

1. Create an IBM Cloud® Virtual Private Cloud.
2. Make sure that your VPC has at least one VSI (virtual server instance), and can connect to the VSI.
3. Make sure your Cloud Databases deployment's private endpoint is enabled.
4. In the IBM Cloud console, click the Menu icon and select -> VPC Infrastructure -> Network -> Virtual private endpoint gateways.
5. After you create your VPE, it might take a few minutes for the new VPE and private DNS to complete the process and begin working for your VPC. Completion is confirmed when you see an IP address set in the details view of the VPE.
6. To make sure private DNS is functioning for your VPE, **ssh** into your VSI and run **nslookup <instance_hostname>**
7. You can now use your instance in the VSI.

Module 1: Secure Cloud Compute in IBM Cloud
Data Encryption for VPC

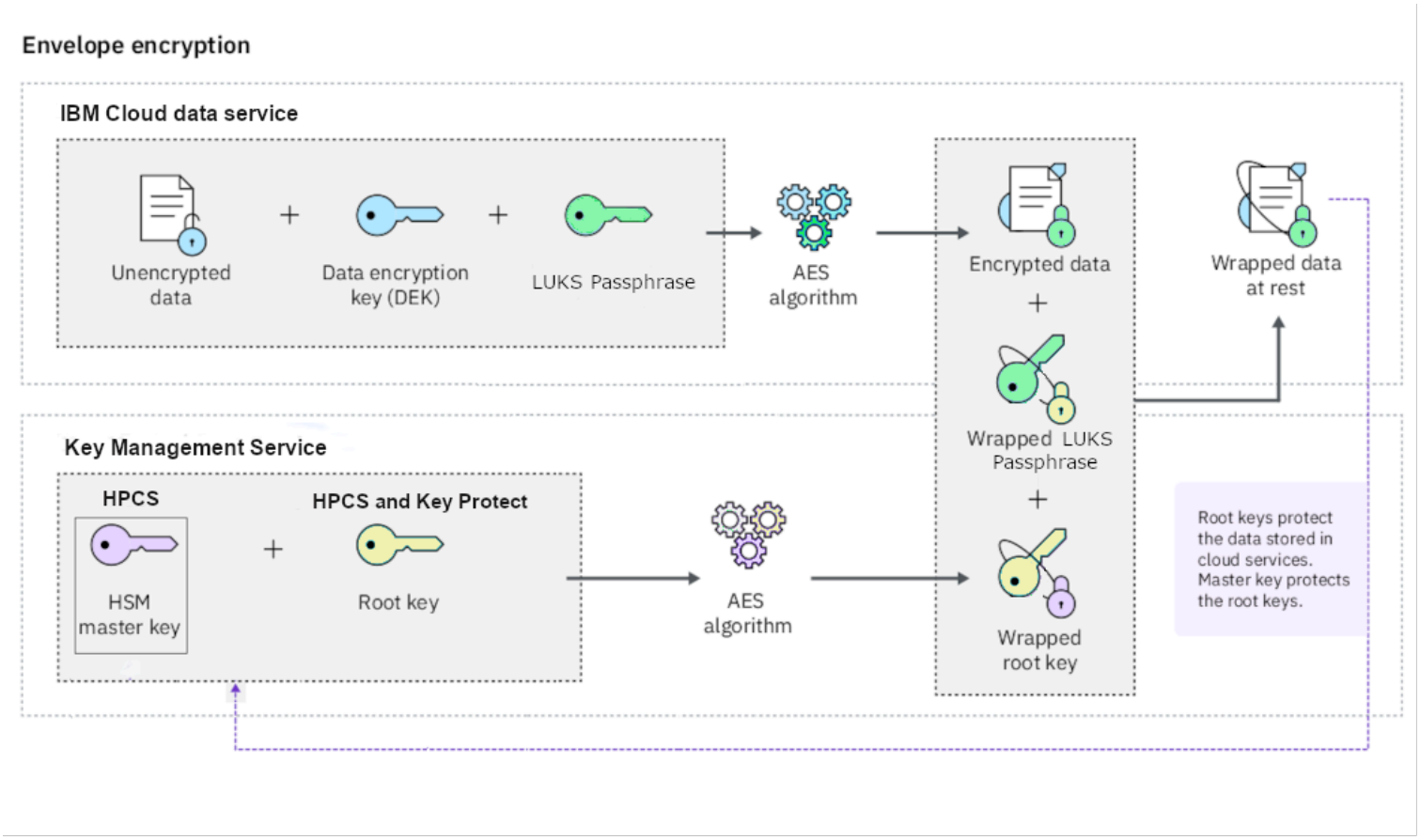
Data Encryption for VPC

IBM Cloud takes security seriously and understands the importance of encrypting data to keep it safe. Primary boot volumes and secondary data volumes are automatically encrypted using IBM-managed encryption. You can also choose to manage your own encryption for volumes and custom images by using customer-managed encryption.

Envelope encryption

Root keys serve as key-wrapping keys and are an important part of envelope encryption. With envelope encryption, root keys encrypt LUKS passphrases (also called *key encryption keys*) which, in turn, secure *data encryption keys* (DEKs) that encrypt your data on the virtual disk. Figure 1 illustrates this process.

Custom images are encrypted by your own LUKS passphrase you create by using QEMU. After the image is encrypted, you wrap the passphrase with your root key stored in the KMS.



Module 1: Secure Cloud Compute in IBM Cloud
Data Encryption for VPC

Data Encryption for VPC Cont'd

Encryption is handled by IBM Cloud VPC's host/hypervisor technology for your instances. This feature provides greater level of security over solutions that provide only storage node encryption-at-rest. Data is always encrypted with envelope encryption within the cloud. Your data is protected while in transit between the host system and Block Storage for VPC, and while at rest in the storage system.

Stock and custom images use QEMU Copy On Write Version 2 (QCOW2) file format. LUKS encryption format secures the QCOW2 format files. IBM uses the AES-256 cipher suite and XTS cipher mode options with LUKS. This combination provides you a much greater level of security than AES-CBC, along with better management of passphrases for key rotation, and provides key replacement options in case your keys are compromised.

In total, four keys protect your data:

- An **IBM-managed key** encrypts your data in the backend storage system - IBM-managed encryption on the storage system is always applied, even when you use customer-managed encryption. This key protects your data while in transit and while at rest.
- A **data encryption key (DEK)** encrypts data within the QCOW2 file and secures the block data clusters in the virtual disk - The DEK is managed by open source QEMU technology and auto-generated when a QCOW2 file is created.
- A **LUKS passphrase (also called a "key encryption key")** encrypts and decrypts the DEK - This key is managed by the VPC generation 2 infrastructure and is encrypted by your root key. It's stored as metadata associated with the block storage volumes containing the QCOW2 file.
- A **customer root key** that encrypts volume and custom image passphrases with envelope encryption, which creates the WDEK - Root keys are customer-managed from KMS instances (Key Protect or HPCS) and stored and managed securely within the KMS instance. The root key also unwraps (decrypts) the WDEK, providing access to your encrypted data.

Module 1: Secure Infrastructure and Hybrid Cloud Connections in IBM Cloud Summary

Module Summary

- All Cloud Databases deployments offer integration with IBM Cloud Service Endpoints.
- It gives you the ability to enable connections to your deployments from the public internet and over the IBM Cloud Private network.
- IBM Cloud® Virtual Private Endpoint (VPE) for IBM Cloud® Virtual Private Cloud provides connection points to IBM services on the IBM private network from your VPC network.
- Primary boot volumes and secondary data volumes are automatically encrypted using IBM-managed encryption.
    - You can also choose to manage your own encryption for volumes and custom images by using customer-managed encryption.
- There are four keys to protect your data: IBM-managed key, data encryption key (DEK) ,LUKS passphrase (also called a "key encryption key"), customer root key

Module 1
Check Your Knowledge

Question 1.

True or False: Service Endpoints are available in all IBM Cloud Multi-Zone Regions

A. True
B. False

Answer A. Service Endpoints are available in all IBM Cloud Multi-Zone Regions

Module 1
Check Your Knowledge

Question 2.

What does IBM Cloud Virtual Private Endpoint provide?

A. Connection points to IBM services on the IBM private network from your VPC network
B. Connection points to IBM services on the IBM public network from your VPC network
C. Connection points to IBM services on the IBM shared network from your VPN network

Answer A. IBM Cloud® Virtual Private Endpoint (VPE) for IBM Cloud® Virtual Private Cloud provides connection points to IBM services on the IBM private network from your VPC network.

Module 1
Check Your Knowledge

Question 3.

Fill in the blank: With _____ encryption, root keys encrypt LUKS passphrases.

A. IBM Cloud
B. Envelope
C. Control
D. Open

Answer B. With envelope encryption, root keys encrypt LUKS passphrases.

Module 1
Check Your Knowledge

Question 4.

Which key encrypts your data in the backend storage system?

A. Data encryption key (DEK)
B. IBM-managed key
C. Customer root key
D. LUKS passphrase (also called a "key encryption key")

Answer B. An IBM-managed key encrypts your data in the backend storage system

Module 2: Securing Internal and External Connections Introduction and Objectives

In Module 2 of the Study Guide the subject matter:

- Covers secure interconnected services with VSIs in VPC, Power VSIs, Code Engine, and security controls in Classic infrastructure.

Lessons

- Securing Internal and External Connections with Power VSIs
- Module Summary
- Knowledge Check Questions

Objectives

- Articulate how to create secure internal and external connections with Power VSIs

Module 2: Securing Internal and External Connections
IBM Power Systems Virtual Server

Configuring connectivity to Power Systems Virtual Server

You can use one of the following options to connect to the IBM Cloud classic environment:

- Using an SSL VPN with a jump server
- Using an IPSec VPN and a VRA (customer implementation)
- Using a Direct Link Connect connection and a VRA (customer implementation)

Connecting to the Power Systems Virtual Server environment

After you establish a connection to the IBM Cloud Classic environment, you must use a separate Direct Link Connect connection to connect to the Power Systems Virtual Server environment. You must use Direct Link Connect to connect to the Power Systems Virtual Server environment. This option provides high performance between the on-premises network and the Power Systems Virtual Server environment.

Connecting directly to the Power Systems Virtual Server environment by using Megaport connectivity services

You can connect directly to the Power Systems Virtual Server environment by using IBM Power Systems Virtual Server NNI Private Ports @ Megaport connectivity services.

Module 2: Securing Internal and External Connections Summary

Module Summary

- The IBM Cloud Direct Link service allows access to IBM Cloud resources over a private network from the Power Systems Virtual Server instance.
- You can use one of the following options to connect to the IBM Cloud classic environment:
  - Using an SSL VPN with a jump server
  - Using an IPSec VPN and a VRA (customer implementation)
  - Using a Direct Link Connect connection and a VRA (customer implementation)

Module 2
Check Your Knowledge

Question 1.

Which options can you use to connect to the IBM Cloud classic environment? Select all that apply.

A. Use an SSL VPN with a jump server
B. Use an IPSec VPN and a VRA
C. Use a Direct Link Connect connection and a VRA
D. Use a Kubernetes connection

Answer A, B, and C. You can use one of the following options to connect to the IBM Cloud classic environment:

- Using an SSL VPN with a jump server
- Using an IPSec VPN and a VRA (customer implementation)
- Using a Direct Link Connect connection and a VRA (customer implementation)

Module 3: Identifying Solutions in Code Engine Introduction and Objectives

In Module 3 of the Study Guide the subject matter:

- Covers secure interconnected services with VSIs in VPC, Power VSIs, Code Engine, and security controls in Classic infrastructure.

Lessons

- IBM Cloud Code Engine Solutions
- Module Summary
- Knowledge Check Questions

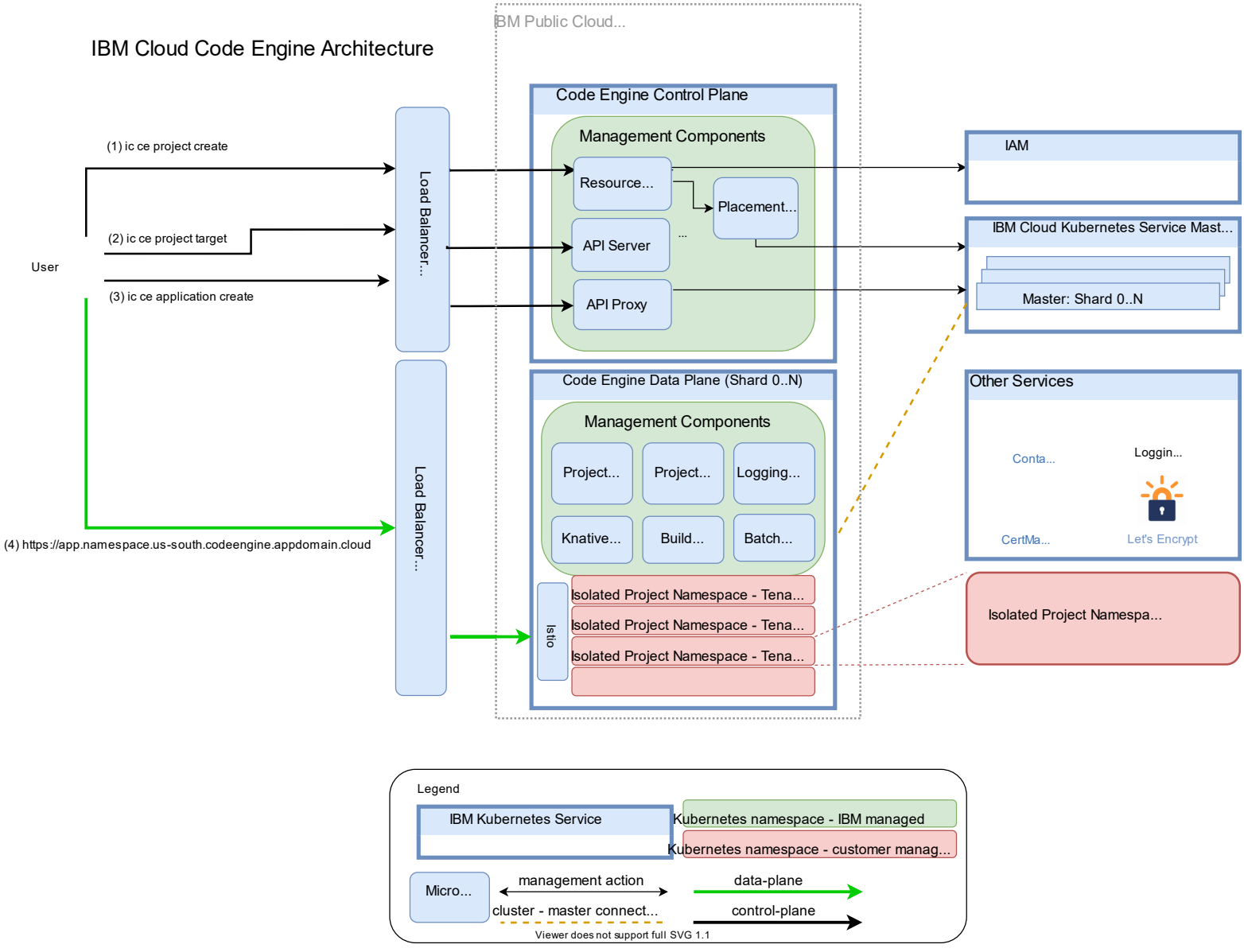
Objectives

- Identify solutions in Code Engine

Module 3: Identifying Solutions in Code Engine
Code Engine Architecture and Workload Isolation

Code Engine Architecture and Workload Isolation

IBM Cloud Code Engine is the IBM Cloud platform that unifies container images, 12-factor-apps, functions, and batch jobs as a one-stop-shop. It's a multi-tenant system that consists of three major building blocks: A control plane, a (set of) shard (or shards), and a routing layer. The control plane and the shards are realized as separate multi-zone Kubernetes clusters. The following diagram gives a graphical overview of the architecture.



Module 3: Identifying Solutions in Code Engine
Code Engine Architecture and Workload Isolation

Code Engine Architecture and Workload Isolation Cont'd

Code Engine is based on IBM Cloud Kubernetes Service clusters and depends on the components and workload isolation of the IBM Cloud Kubernetes Service.

All components are managed and owned by IBM and run in the IBM Cloud account. Each cluster is running in its own VPC and separated from other clusters.

The Code Engine control plane runs the components that are shared among all Code Engine users and make the Kubernetes cluster a true multi-tenant system. The control-plane consists of four microservices that are deployed on it.

Code Engine control-plane microservices	
Component	**Purpose**
Resource broker	Creates and deletes Code Engine project resources in the IBM Cloud resource controller and requests the placement of the project on a shard.
Project placement controller	Selects a shard and requests the creation, deletion, and isolation of the project on the shard.
API server	Provides the target information (**KUBECONFIG** file) for the selected project. It also performs IAM access policy checks and writes audit records.
Kube API proxy	Proxies each API request to the proper shard cluster, perform IAM policy checks, and writes audit records.

Module 3: Identifying Solutions in Code Engine
Code Engine Architecture and Workload Isolation

Code Engine Architecture and Workload Isolation Cont'd

The shards are running the customer workload, such as builds, batch jobs, or apps. Therefore, the shard cluster runs the following microservices to control the customer workloads.

Shard cluster microservices	
Component	**Purpose**
Project isolation controller	Manages and isolates the Kubernetes namespace corresponding to the Code Engine project resource. It monitors and ensures the isolation aspects like role-based-access-control (RBAC), pod security policies, resource quota, and network policies are enforced.
Project domain and cert controller	Manages the domain and certificates for the route endpoint of the project. The endpoint consists of a DNS entry and a wildcard certificate.
Knative and Istio	Manage the lifecycle of applications. Knative is responsible for scaling the application. Istio is responsible for routing the traffic to the proper revision and container of the application.
Batch controller	Manages the lifecycle and containers for jobs and job runs.
Build controller	Manages the lifecycle and containers for builds and build runs.
Service binding and IBM Cloud operator	Manage the lifecycle of secrets that are associated to bindings of IBM Cloud services to applications and jobs.
IBM Cloud Object Storage event source controller	Manage the lifecycle of event subscriptions from the IBM Cloud Object Storage service.

Module 3: Identifying Solutions in Code Engine Summary

Module Summary

- IBM Cloud Code Engine is the IBM Cloud platform that unifies container images, 12-factor-apps, functions, and batch jobs as a one-stop-shop.
- The Code Engine control plane runs the components that are shared among all Code Engine users and make the Kubernetes cluster a true multi-tenant system. The control-plane consists of four microservices that are deployed on it.
- Project isolation controller manages and isolates the Kubernetes namespace corresponding to the Code Engine project resource. It monitors and ensures the isolation aspects like role-based-access-control (RBAC), pod security policies, resource quota, and network policies are enforced.

Module 3
Check Your Knowledge

Question 1.

IBM Cloud Code Engine is the IBM Cloud platform that unifies...

A. Container images
B. 20-factor-apps
C. Functions
D. Batch jobs

Answer A, C, and D. IBM Cloud Code Engine is the IBM Cloud platform that unifies container images, 12-factor-apps, functions, and batch jobs as a one-stop-shop.

Module 4: Security Controls in Classic Infrastructure Introduction and Objectives

In Module 4 of the Study Guide the subject matter:

- Covers secure interconnected services with VSIs in VPC, Power VSIs, Code Engine, and security controls in Classic infrastructure.

Lessons

- Security Controls on Bare Metal in Classic Infrastructure
- Network Security with VSIs in Classic Infrastructure
- Module Summary
- Knowledge Check Questions

Objectives

- Implement security controls on Bare Metal in Classic infrastructure

Module 4: Security Controls in Classic Infrastructure
Hardware Monitoring and Security Controls

Hardware Monitoring and Security Controls

The escalation and sophistication of malicious threats has you employing more stringent security requirements and scrutinizing every aspect of your execution environment. You're looking to your cloud providers to offer hardware monitoring and security controls that can determine whether a workload is running on trusted hardware in a known location.
IBM Cloud® is leading the way to help you deploy hybrid and cloud environments with enhanced security verification of your launch environment by using Intel® Trusted Execution Technology (Intel® TXT).

How it works

Intel® TXT provides hardware monitoring and security controls that help assure businesses that a workload that is deployed on or migrated to the IBM Cloud infrastructure is running on trusted hardware in a known location.

What it does for you

Intel® TXT is especially advantageous for large enterprises subject to compliance and audit regulations, such as healthcare, financial services, and government organizations. It helps assure that tracking of all trusted resources can be integrated, managed, and reported on with the relevant compliance organizations (HIPAA, PCI, FedRAMP, ISO, FISMA, and SSAE 16).

Special Technical Notice IBM Cloud cannot assist with configuration of Intel® TXT settings due to the sensitivity of customer environments and data.

Module 4: Security Controls in Classic Infrastructure
Network Options

Network Options

IBM Cloud® Bare Metal Servers have a number of network choices available to suit your unique needs.

Port redundancy

Select this option to determine how you'd like to handle network connection redundancy. Choose from these options:

- **Automatic** is the default and recommended setting. It provides two physical network ports that are configured with LACP bonding on both the network and the operating system at time of provisioning. Automatic is the most hands-free option for continuous network availability.
- **User Managed** is available for advanced configurations. It provides two physical network ports, but the ports are configured independently on both the network and the operating system.
- **None** provides a single physical port to each network.

Always included options and services

The following network options and services are always included with your Bare Metal Servers:

- **Private network interface** - All Bare Metal Servers include access to the private network, which allows access to other IBM Services.
- **Primary IP addresses** - A private IPv4 address is included with a private network interface. If a public network interface is selected, a public IPv4 address is also included. These addresses provide basic connectivity to the server.
- **VPN Management** - Manage access to the subnet the server resides on for users when you connect through VPN.

Module 4: Security Controls in Classic Infrastructure
About Hardware Firewall

Hardware Firewall

A Hardware Firewall is a network device that is connected upstream from a server. The firewall blocks unwanted traffic from a server before the traffic ever reaches the server. The main advantage to having a Hardware Firewall is that a server only has to handle 'good' traffic and no resources are wasted dealing with the 'bad' traffic.
The Hardware Firewall leverages a multi-tenant enterprise platform to protect an individual server.

Overview and features

Intended Use: Single Server Primary Public IP Protection
User Interface: Integrated into IBM Cloud console and APIs
Features: Stateful Packet Inspection, Ingress Firewall Rules, IPv4, IPv6, Basic Logging
Server Network Interface Speeds: 100Mbps, 200Mbps, 1000Mbps, and 2000Mbps
It is required that the throughput of Hardware Firewall instance match the uplink speed of the server the firewall is being added to.

Server hardware firewall

Applicable when a public network interface is requested, this option places a firewall in front of your server. The rules of the firewall apply only to the IP addresses associated with the server.

Module 4: Security Controls in Classic Infrastructure Summary

Module Summary

- Intel® TXT provides hardware monitoring and security controls that help assure businesses that a workload that is deployed on or migrated to the IBM Cloud infrastructure is running on trusted hardware in a known location.
- Automatic is the default and recommended setting for network port redundancy. It provides two physical network ports that are configured with LACP bonding on both the network and the operating system at time of provisioning. Automatic is the most hands-free option for continuous network availability.
- A Hardware Firewall is a network device that is connected upstream from a server. The firewall blocks unwanted traffic from a server before the traffic ever reaches the server.

Module 4
Check Your Knowledge

Question 1.

What does Intel TXT provide? Selet all that apply.

A. Coud features
B. Hardware monitoring
C. Security controls
D. Kubernetes software

Answer B and C. Intel TXT provides hardware monitoring and security controls

Module 4
Check Your Knowledge

Question 2.

Which firewall is applicable when a public network interface is requested?

A. Red Hat OpenShift
B. Server hardware firewall
C. Kubernetes
D. Digital contracts

Answer B. Server hardware firewall is applicable when a public network interface is requested