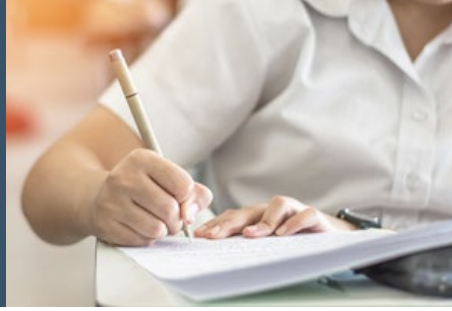
IBM Security Engineer
Study Guide



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 Kubernetes services 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 Kubernetes Services in IBM Cloud Part 1
2. Secure Kubernetes Services in IBM Cloud Part 2

Objectives

1. Implement security controls at the Kubernetes layer in IKS
2. Implement security controls at the infrastructure layer in IKS (VPC)
3. Implement security controls at the infrastructure layer in IKS (Classic)
4. Implement security controls at the OpenShift platform layer in Red Hat OpenShift
5. Implement security controls at the infrastructure layer in Red Hat OpenShift (VPC)
6. Implement security controls at the infrastructure layer in Red Hat OpenShift (Classic)
7. Implement security in Red Hat OpenShift on IBM Cloud Satellite

Module 1: Secure Kubernetes Services in IBM Cloud Part 1 Introduction and Objectives

In Module 1 of the Study Guide the subject matter:

- Introduces how to implement security controls at the Kubernetes layer in IKS, the infrastructure layer in IKS (VPC), and the infrastructure layer in IKS (Classic).

Lessons

- Security Controls at the Kubernetes Layer in Kubernetes Service
- Security Controls at the Infrastructure Layer in Kubernetes Service (VPC)
- Security Controls at the Infrastructure Layer in Kubernetes Service (Classic)
- Module Summary
- Knowledge Check Questions

Objectives

- Implement security controls at the Kubernetes layer in IKS
- Implement security controls at the infrastructure layer in IKS (VPC)
- Implement security controls at the infrastructure layer in IKS (Classic)

Module 1: Secure Kubernetes Services in IBM Cloud Part 1
Controlling User Access with IBM Cloud IAM and Kubernetes RBAC

Understanding RBAC permissions

RBAC roles and cluster roles define a set of permissions for how users can interact with Kubernetes resources in your cluster.

What do these roles look like in my cluster?

If you want users to be able to interact with Kubernetes resources from within a cluster, you must assign user access to one or more namespaces through IBM Cloud IAM service access roles. Every user who is assigned a service access role is automatically assigned a corresponding RBAC cluster role. These RBAC cluster roles are predefined and permit users to interact with Kubernetes resources in your cluster. Additionally, a role binding is created to apply the cluster role to a specific namespace, or a cluster role binding is created to apply the cluster role to all namespaces.

Example cluster use cases and IAM roles

Use Case	Example Roles and Scope
App auditor	Viewer platform access role for a cluster, region, or resource group, Reader service access role for a cluster, region, or resource group.
App developers	Editor platform access role for a cluster, Writer service access role scoped to a namespace, Cloud Foundry developer space role.
DevOps operator	Operator platform access role for a cluster, Writer service access role not scoped to a namespace (for the whole cluster), Cloud Foundry developer space role.
Operator or site reliability engineer	Administrator platform access role for a cluster, region, or resource group, Reader service access role for a cluster or region

Module 1: Secure Kubernetes Services in IBM Cloud Part 1
Overview of network security options

Overview of network security options

Control traffic to and from your cluster and traffic between pods in your cluster by creating network rules and policies.
Control traffic to and from your cluster with VPC access control lists (ACLs) and VPC security groups, and control traffic between pods in your cluster with Kubernetes network policies.

Access control lists (ACLs) or security groups?

Although you can use either VPC ACLs or VPC security groups to control inbound traffic to and outbound traffic from your cluster, security groups are easier to implement. You can simplify your security setup by adding rules to only the default security group for your cluster, and leaving the default ACL for your VPC as-is.

Module 1: Secure Kubernetes Services in IBM Cloud Part 1
Overview of network security options

Overview of network security options cont'd

Comparison of network security options

The following table describes the basic characteristics of each network security option that you can use for your VPC cluster in IBM Cloud Kubernetes Service.

Policy type	Application level	Default behavior	Use case	Limitations
VPC security groups (Recommended)	Worker node	Version 1.19 and later: The default security groups for your cluster allow incoming traffic requests to the 30000 - 32767 port range on your worker nodes. Version 1.18 and earlier: The default security group for your VPC denies all incoming traffic requests to your worker nodes.	Control inbound and outbound traffic to and from your worker nodes. Rules allow or deny traffic to or from an IP range with specified protocols and ports.	You can add rules to the default security group that is applied to your worker nodes. However, because your worker nodes exist in a service account and are not listed in the VPC infrastructure dashboard, you can't add more security groups and apply them to your worker nodes.
Kubernetes network policies	Worker node host endpoint	None	Control traffic within the cluster at the pod level by using pod and namespace labels. Protect pods from internal network traffic, such as isolating app microservices from each other within a namespace or across namespaces.	None

Module 1: Secure Kubernetes Services in IBM Cloud Part 1
Controlling traffic with network policies on classic clusters

Calico network policies

Calico network policies are a set of the Kubernetes network policies. You can apply Calico policies by using the **calicoctl** command line.
Calico enforces these policies, including any Kubernetes network policies that are automatically converted to Calico policies, by setting up Linux Iptables rules on the Kubernetes worker nodes.

Isolating clusters on the public network

You can isolate your cluster on the public network by applying Calico public network policies.
This set of Calico policies work in conjunction with the default Calico policies to block most public network traffic of a cluster while allowing communication that is necessary for the cluster to function to specific subnets.

Isolating clusters on the private network

You can isolate your cluster from other systems on the private network by applying Calico private network policies.
This set of Calico policies and host endpoints can isolate the private network traffic of a cluster from other resources in the account's private network, while allowing communication on the private network that is necessary for the cluster to function.
To allow your workers and pods to access IBM Cloud Container Registry over the private network, apply the **allow-private-services.yaml** and **allow-private-services-pods.yaml** policies. To access other IBM Cloud services that support private cloud service endpoints, you must manually add the subnets for those services to this policy.

Logging denied traffic

To log denied traffic requests to certain pods in your cluster, you can create a Calico log network policy.
When you set up network policies to limit traffic to app pods, traffic requests that are not permitted by these policies are denied and dropped. In some scenarios, you might want more information about denied traffic requests. For example, you might notice some unusual traffic that is continuously being denied by one of your network policies. To monitor the potential security threat, you can set up logging to record every time that the policy denies an attempted action on specified app pods.

Module 1: Secure Kubernetes Services in IBM Cloud Part 1
Classic: Opening required ports and IP addresses in your firewall

Running kubectl commands from behind a firewall

If corporate network policies prevent access from your local system to public endpoints via proxies or firewalls, to run kubectl commands, you must allow TCP access for the cluster. When a cluster is created, the port in the service endpoint URLs is randomly assigned from within 30000-32767. You can either choose to open port range 30000-32767 for any cluster that might get created or you can choose to allow access for a specific existing cluster.

Before you begin, allow access to run ibmcloud ks commands.

To allow access for a specific cluster:

1. ibmcloud login [--sso]
2. ibmcloud target -g <resource_group_name>
3. ibmcloud ks cluster get --cluster <cluster_name_or_ID>
4. curl --insecure <private_service_endpoint_URL>/version
5. Allow access to the IBM Cloud Container Registry regions that you plan to use on port 443 in your firewall.
6. Verify your connection.

Module 1: Secure Kubernetes Services in IBM Cloud Part 1
Restricting network traffic to edge worker nodes on classic infrastructure

Isolating networking workloads to edge nodes

Add the **dedicated=edge** label to worker nodes on each public or private VLAN in your cluster. The labels ensure that network load balancers (NLBs) and Ingress application load balancers (ALBs) are deployed to those worker nodes only. For NLBs, ensure that two or more worker nodes per zone are edge nodes. For ALBs, ensure that three or more worker nodes per zone are edge nodes. Both public and private NLBs and ALBs can deploy to edge worker nodes.

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

Module Summary

- If you want users to be able to interact with Kubernetes resources from within a cluster, you must assign user access to one or more namespaces through IBM Cloud IAM service access roles. Every user who is assigned a service access role is automatically assigned a corresponding RBAC cluster role.
- Control traffic to and from your cluster and traffic between pods in your cluster by creating network rules and policies.
- You can isolate your cluster on the public network by applying Calico public network policies.
- Calico network policies are a set of the Kubernetes network policies. You can apply Calico policies by using the calicoctl command line.
- If corporate network policies prevent access from your local system to public endpoints via proxies or firewalls, to run kubectl commands, you must allow TCP access for the cluster.
- For NLBs, ensure that two or more worker nodes per zone are edge nodes. For ALBs, ensure that three or more worker nodes per zone are edge nodes. Both public and private NLBs and ALBs can deploy to edge worker nodes.

Module 1
Check Your Knowledge

Question 1.

A banking application which deals with payments and money transfers must be deployed to Payment namespace in an IKS cluster running in an IBM Cloud VPC. The application must be isolated and should be accessible only to ACC service in the same namespace. Which option would secure the banking application?

A. Create Kubernetes network policy to allow traffic only from services in Payment namespace
B. Modify the default security group for the VPC to allow traffic only from selected endpoints
C. Modify the ACL for the VPC to allow traffic only from selected subnets
D. Create Kubernetes network policy to allow traffic only from ACC service to the banking service

➞ Answer D. Create Kubernetes network policy to allow traffic only from ACC service to the banking service

Module 1
Check Your Knowledge

Question 2.

What is the least privileged access role to give a user who requires billing access?

A. Admin
B. Writer
C. Viewer platform

Answer C. Viewer platform access role is the least privileged.

Module 1
Check Your Knowledge

Question 3.

How do you control traffic to and from your cluster and traffic between pods in your cluster?

A. Using Kubernetes
B. By creating envelope nodes
C. By creating network rules and policies
D. By using Red Hat OpenShift

Answer C. Control traffic to and from your cluster and traffic between pods in your cluster by creating network rules and policies.

Module 1
Check Your Knowledge

Question 4.

What should you do if corporate network policies prevent access from your local system to public endpoints via proxies or firewalls, to run **kubectl** commands?

A. You must allow ACL access for the cluster
B. You must give access to IBM Cloud admin
C. You must disallow TCP access for the cluster
D. You must allow TCP access for the cluster

Answer D. If corporate network policies prevent access from your local system to public endpoints via proxies or firewalls, to run kubectl commands, you must allow TCP access for the cluster.

Module 1
Check Your Knowledge

Question 5.

When isolating networking workloads to edge nodes, why would you add labels to worker nodes on each public or private VLAN in your cluster?

A. To ensure that NLBs and Ingress ALBs are deployed to those worker nodes and other nodes
B. To ensure that only NLBs are deployed to those worker nodes
C. To ensure that NLBs and Ingress ALBs are deployed to those worker nodes only
D. To ensure that NLBs and Ingress ALBs are not deployed to those worker nodes only

Answer C. To ensure that NLBs and Ingress ALBs are deployed to those worker nodes only

Module 1
Check Your Knowledge

Question 6.

Fill in the blank: Kubernetes policies protect pods from _____ network traffic.

A. External
B. Internal
C. Outward
D. Inside

Answer B. Internal network traffic.

Module 2: Secure Kubernetes Services in IBM Cloud Part 2 Introduction and Objectives

In Module 2 of the Study Guide the subject matter:

- Introduces how to implement security controls at the OpenShift platform layer in Red Hat OpenShift, the infrastructure layer in Red Hat OpenShift (VPC), the infrastructure layer in Red Hat OpenShift (Classic), and in Red Hat OpenShift on IBM Cloud Satellite.

Lessons

- Security Controls at the Platform Layer in Red Hat OpenShift
- Security Controls at the Infrastructure Layer in Red Hat OpenShift cluster on VPC
- Implement Security Controls in Red Hat OpenShift on Classic Infrastructure
- Implement Security in Red Hat OpenShift on IBM Cloud Satellite
- Module Summary
- Knowledge Check Questions

Objectives

- Implement security controls at the OpenShift platform layer in Red Hat Openshift
- Implement security controls at the infrastructure layer in Red Hat Openshift (VPC)
- Implement security controls at the infrastructure layer in Red Hat Openshift (Classic)
- Implement security controls in Red Hat Openshift on IBM Cloud Satellite

Module 2: Secure Kubernetes Services in IBM Cloud Part 2
Accessing Red Hat OpenShift clusters

Accessing VPC clusters through the private cloud service endpoint

The Red Hat OpenShift master is accessible through the private cloud service endpoint if authorized cluster users are in your IBM Cloud private network or are connected to the private network, such as through a VPC VPN connection. However, communication with the Kubernetes master over the private cloud service endpoint must go through the 166.X.X.X IP address range, which you must configure in your VPN gateway and connection setup. If you have a multizone cluster, repeat this step to configure a VPC gateway on a subnet in each zone where you have worker nodes

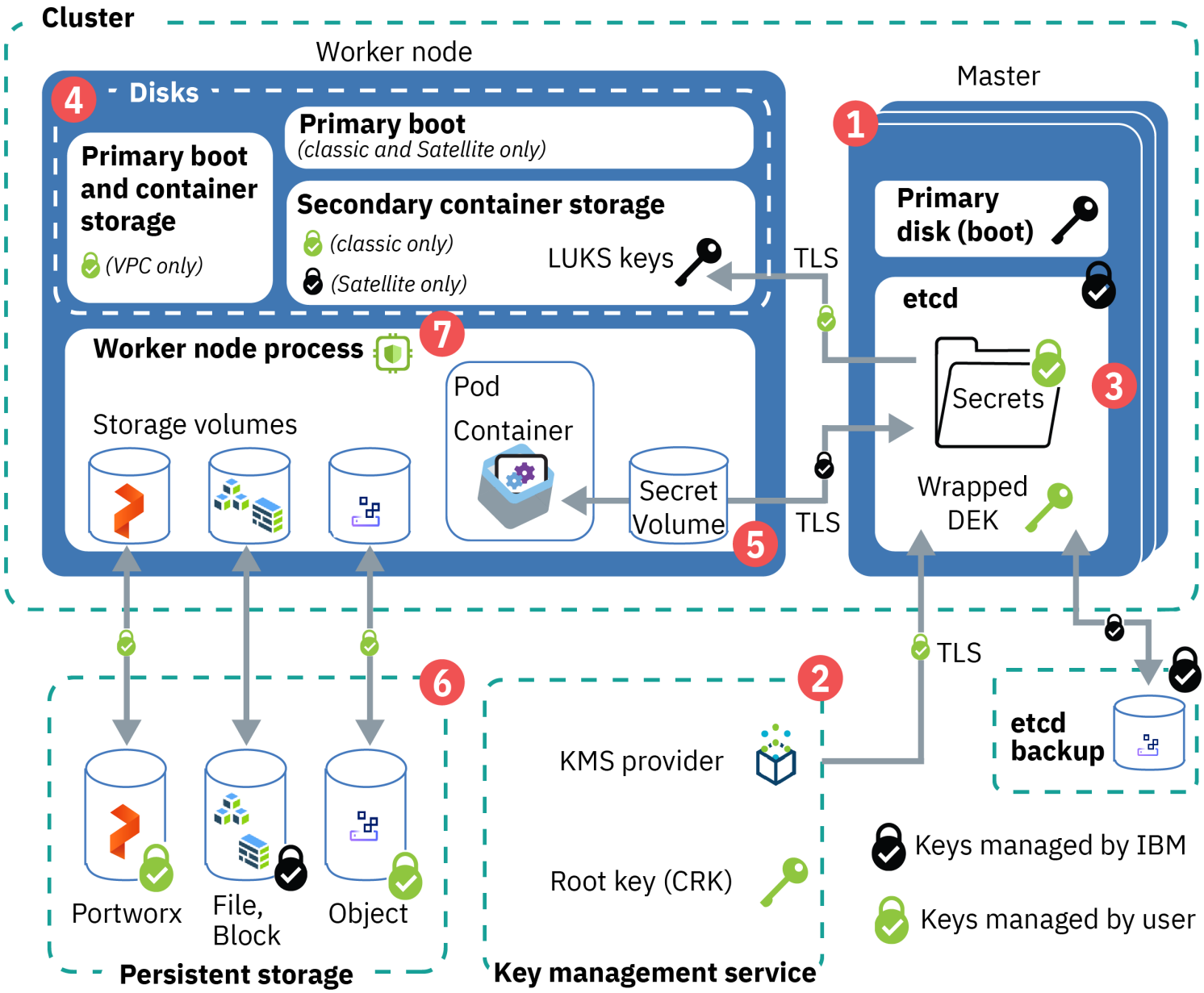
Creating an allowlist for the private cloud service endpoint

Control access to your private cloud service endpoint by creating a subnet allowlist. After you grant users access to your cluster through IBM Cloud IAM, you can add a secondary layer of security by creating an allowlist for the private cloud service endpoint. Only authorized requests to your cluster master that originate from subnets in the allowlist are permitted through the cluster's private cloud service endpoint.

Module 2: Secure Kubernetes Services in IBM Cloud Part 2
Protecting sensitive information in your cluster

Overview of cluster encryption

The following image and description(on next page) outline default and optional data encryption for Red Hat OpenShift on IBM Cloud clusters.



Module 2: Secure Kubernetes Services in IBM Cloud Part 2
Protecting sensitive information in your cluster

Overview of cluster encryption cont'd

1. **Red Hat OpenShift master control plane**: Components in the Red Hat OpenShift master boot up on a LUKS-encrypted drive using an IBM-managed key.
2. **Bring your own key (BYOK), for VPC and classic only**: When you enable a key management service (KMS) provider* for your cluster, you bring your own root key. The root key is used to encrypt the data encryption keys (DEKs) which are then used to encrypt the secrets in your cluster.
3. **Worker node disks**: Attached disks are used to boot your worker node, host the container file system, and store locally pulled images.
4. **Cluster secrets**: When you deploy your app, use Kubernetes secrets, which are base64 encoded by default.
5. **Persistent storage encryption**: You can choose to store data by setting up file, block, object, or software-defined Portworx persistent storage.
6. **Data-in-use encryption**: For select, SGX-enabled classic worker node flavors, you can use IBM Cloud Data Shield to encrypt data-in-use within the worker node.

Note: You can't disable KMS provider encryption. Do not delete root keys in your KMS instance, even if you rotate to use a new key. If you delete a root key that a cluster uses, the cluster becomes unusable, loses all its data, and can't be recovered. Similarly, if you disable a root key, operations that rely on reading secrets fail. Unlike deleting a root key, however, you can reenable a disabled key to make your cluster usable again.

Module 2: Secure Kubernetes Services in IBM Cloud Part 2
User access permissions

IBM Cloud IAM platform access roles

Red Hat OpenShift on IBM Cloud is configured to use IBM Cloud IAM Identity Service roles. IBM Cloud IAM platform access roles determine the actions that users can perform on IBM Cloud resources such as clusters, worker nodes, and Ingress application load balancers (ALBs). IBM Cloud IAM platform access roles also automatically set basic infrastructure permissions for users.

- **Actions requiring no permissions**: Any user in your account who runs the CLI command or makes the API call for the action sees the result, even if the user has no assigned permissions.
- **Viewer actions**: The Viewer platform access role includes the actions that require no permissions, plus the permissions that are shown in the Viewer tab of following table. With the Viewer role, users such as auditors or billing can see cluster details but not modify the infrastructure.
- **Editor actions**: The Editor platform access role includes the permissions that are granted by Viewer, plus the following. With the Editor role, users such as developers can bind services, work with Ingress resources, and set up log forwarding for their apps but can't modify the infrastructure.
- **Operator actions**: The Operator platform access role includes the permissions that are granted by Viewer, plus the permissions that are shown in the Operator tab of the following table. With the Operator role, users such as site reliability engineers, DevOps engineers, or cluster administrators can add worker nodes and troubleshoot infrastructure such as by reloading a worker node, but can't create or delete the cluster, change the credentials, or set up cluster-wide features like service endpoints or managed add-ons.

IBM Cloud IAM service access roles

Every user who is assigned an IBM Cloud IAM service access role is also automatically assigned a corresponding Kubernetes role-based access control (RBAC) role in a specific namespace. Do not assign IBM Cloud IAM platform access roles at the same time as a service access role. You must assign platform and service access roles separately.

Module 2: Secure Kubernetes Services in IBM Cloud Part 2
VPC: Opening required ports and IP addresses in other network firewalls

Opening ports in a corporate firewall

If corporate network policies prevent access from your local system to public endpoints via proxies or firewalls, you must allow access to run ibmcloud, ibmcloud oc, and ibmcloud cr commands, oc commands, and calicoctl commands from your local system.

Running ibmcloud, ibmcloud oc, and ibmcloud cr commands from behind a firewall

If corporate network policies prevent access from your local system to public endpoints via proxies or firewalls, to run ibmcloud, ibmcloud oc and ibmcloud cr commands, you must allow TCP access for IBM Cloud, Red Hat OpenShift on IBM Cloud, and IBM Cloud Container Registry.

Allowing traffic from your cluster in other services' firewalls or in on-premises firewalls

Allow your worker nodes to communicate with services that are protected by firewalls. For example, you might have services that run inside or outside IBM Cloud, or services that run on-premises, that are protected by a firewall. You want to permit incoming network traffic to those services from your cluster. In your service's firewall, you must add the external IP addresses of the public gateways on your cluster's VPC subnets.
If you want to permit egress from your firewall-protected services to your cluster, you must add your worker nodes' private IP addresses or your cluster's VPC subnet CIDRs in your service's firewall. Note that because worker nodes in VPC clusters have only private IP addresses, connections into the VPC cluster worker nodes can only originate from systems that are connected to your IBM Cloud private network.

Module 2: Secure Kubernetes Services in IBM Cloud Part 2
Overview of network security options

Overview Of Network Security Options

Control traffic to and from your cluster and traffic between pods in your cluster by creating network rules and policies.

Control traffic to and from your cluster with VPC access control lists (ACLs) and VPC security groups, and control traffic between pods in your cluster with Kubernetes network policies.

Note: An ACL must be created for each subnet that your cluster is attached to, but only one security group must be modified for all worker nodes in your cluster.

Module 2: Secure Kubernetes Services in IBM Cloud Part 2
Overview of network security options

Overview Of Network Security Options Cont'd

Comparison Of Network Security Options

The following table describes the basic characteristics of each network security option that you can use for your VPC cluster in Red Hat OpenShift on IBM Cloud.

Policy type	Application level	Use case	Limitations
VPC security groups (Recommended)	Worker node	Control inbound and outbound traffic to and from your worker nodes.	can't add more security groups and apply them to your worker nodes.
VPC security groups	Load balancer	Allow inbound traffic from all sources to the listener port on a public load balancer.	None
VPC access control lists (ACLs) (Not recommended)	VPC subnet	Control inbound and outbound traffic to and from the cluster subnet that you attach the ACL to.	can't be used to control traffic between the clusters that share the same VPC subnets. Instead, you can create Calico policies to isolate your clusters on the private network.
Kubernetes network policies	Worker node host endpoint	Control traffic within the cluster at the pod level by using pod and namespace labels.	None

Module 2: Secure Kubernetes Services in IBM Cloud Part 2
Classic: Opening Required Ports and IP Addresses in Your Firewall

Classic: Opening Required Ports and IP Addresses in Your Firewall

Review these situations in which you might need to open specific ports and IP addresses in your firewalls for your Red Hat® OpenShift® on IBM Cloud® clusters.

- **Corporate firewalls**: If corporate network policies prevent access from your local system to public endpoints via proxies or firewalls, you must allow access to run ibmcloud, ibmcloud oc, ibmcloud cr, oc, and calicoctl commands from your local system.
- **Gateway appliance firewalls:** If you have firewalls set up on the public or private network in your IBM Cloud infrastructure account, such as a VRA, you must open IP ranges, ports, and protocols to allow worker nodes to communicate with the master, with infrastructure resources, and with other IBM Cloud services.
- **Calico network policies:** If you use Calico network policies to act as a firewall to restrict all worker node egress, you must allow your worker nodes to access the resources that are required for the cluster to function.

Enable worker-to-worker communication

Enable worker-to-worker communication by allowing all TCP, UDP, VRRP, and IPEncap traffic between worker nodes on the public and private interfaces. Red Hat OpenShift on IBM Cloud uses the VRRP protocol to manage IP addresses for private load balancers and the IPEncap protocol to permit pod to pod traffic across subnets.

Module 2: Secure Kubernetes Services in IBM Cloud Part 2
Restricting Network Traffic to Edge Worker Nodes on Classic Infrastructure

Restricting Network Traffic to Edge Worker Nodes on Classic Infrastructure

Edge worker nodes can improve the security of your Red Hat® OpenShift® on IBM Cloud® cluster by allowing fewer worker nodes by isolating the networking workload.
When you mark these worker nodes for networking only, other workloads can't consume the CPU or memory of the worker node and interfere with networking.

Isolating networking workloads to edge nodes

Add the dedicated=edge label to worker nodes on each public or private VLAN in your cluster.

- In version 4 clusters, the labels ensure that network load balancer (NLB) pods are deployed to those worker nodes only. For NLBs, ensure that two or more worker nodes per zone are edge nodes. Note that router pods for Ingress controllers and routes are not deployed to edge nodes and remain on non-edge worker nodes.
- In version 3.11 clusters, the labels ensure that network load balancers (NLBs) and Ingress application load balancers (ALBs) are deployed to those worker nodes only. For NLBs, ensure that two or more worker nodes per zone are edge nodes. For ALBs, ensure that three or more worker nodes per zone are edge nodes. Both public and private NLBs and ALBs can deploy to edge worker nodes. Note that router pods are not deployed to edge nodes and remain on non-edge worker nodes.

Preventing app workloads from running on edge worker nodes

A benefit of edge worker nodes is that they can be specified to run networking services only.
Using the dedicated=edge toleration means that all network load balancer (NLB) and, in version 3.11 clusters, Ingress application load balancer (ALB) services are deployed to the labeled worker nodes only. However, to prevent other workloads from running on edge worker nodes and consuming worker node resources, you must use Kubernetes taints.

Module 2: Secure Kubernetes Services in IBM Cloud Part 2
Understanding Link Endpoints and Satellite

Satellite

With IBM Cloud Satellite, you can create a hybrid environment that brings the scalability and on-demand flexibility of public cloud services to the applications and data that run in your secure private cloud.

Understanding Link Endpoints and Satellite

Open up Satellite endpoints in the Satellite control plane to control and audit network traffic between your IBM Cloud Satellite® location and services, servers, or apps that run outside of the location.

With Satellite Link endpoints, you can allow any client that runs in your Satellite location to connect to a service, server, or app that runs outside of the location, or allow a client that is connected to the IBM Cloud private network to connect to a service, server, or app that runs in your location.

To establish the connection, you must specify the destination resource's fully qualified domain name (FQDN) or IP address, port, the connection protocol, and any authentication methods in the endpoint. The endpoint is registered with the Satellite Link component of your location's Satellite control plane. To help you maintain enterprise security and audit compliance, Satellite Link additionally provides built-in controls to restrict client access to endpoints and to log and audit traffic that flows over endpoints.

How do I make my data secure in transit?

Link endpoints between your location and IBM Cloud are secured through two levels of encryption: high-security encryption from the location’s connector to IBM Cloud that is provided by IBM , and an optional additional encryption layer between the source and destination resources.

All data that is transported over Satellite Link is encrypted using TLS 1.3 standards. This level of encryption is managed by IBM.

Module 2: Secure Infrastructure and Hybrid Cloud Connections in IBM Cloud Summary

Module Summary

- The Red Hat OpenShift master is accessible through the private cloud service endpoint if authorized cluster users are in your IBM Cloud private network or are connected to the private network, such as through a VPC VPN connection.
- You can't disable KMS provider encryption. Do not delete root keys in your KMS instance, even if you rotate to use a new key. If you delete a root key that a cluster uses, the cluster becomes unusable, loses all its data, and can't be recovered. Similarly, if you disable a root key, operations that rely on reading secrets fail. Unlike deleting a root key, however, you can reenable a disabled key to make your cluster usable again.
- Red Hat OpenShift on IBM Cloud is configured to use IBM Cloud IAM Identity Service roles. IBM Cloud IAM platform access roles determine the actions that users can perform on IBM Cloud resources such as clusters, worker nodes, and Ingress application load balancers (ALBs).
- If corporate network policies prevent access from your local system to public endpoints via proxies or firewalls, you must allow access to run ibmcloud, ibmcloud oc, and ibmcloud cr commands, oc commands, and calicoctl commands from your local system.
- Control traffic to and from your cluster and traffic between pods in your cluster by creating network rules and policies.
- Enable worker-to-worker communication by allowing all TCP, UDP, VRRP, and IPEncap traffic between worker nodes on the public and private interfaces. Red Hat OpenShift on IBM Cloud uses the VRRP protocol to manage IP addresses for private load balancers and the IPEncap protocol to permit pod to pod traffic across subnets.
- Edge worker nodes can improve the security of your Red Hat® OpenShift® on IBM Cloud® cluster by allowing fewer worker nodes by isolating the networking workload.
- When you mark these worker nodes for networking only, other workloads can't consume the CPU or memory of the worker node and interfere with networking.
- Link endpoints between your location and IBM Cloud are secured through two levels of encryption: high-security encryption from the location’s connector to IBM Cloud that is provided by IBM , and an optional additional encryption layer between the source and destination resources.

Module 2
Check Your Knowledge

Question 1.

In a Red Hat OpenShift cluster on IBM Cloud, the data in etcd is stored in the local disks of the Kubernetes master nodes. How are the secrets in the cluster encrypted?

A. Using third-party Vault services
B. Using AES-256 bit encryption manually
C. Using Hardware Security Module (HSM) automatically
D. Using wrapped Data Encryption Key (DEK) stored in etcd by enabling KMS service providers

Answer D. Using wrapped
Data Encryption Key (DEK) stored in etcd by enabling KMS service providers

Module 2
Check Your Knowledge

Question 2.

Which of the following are data encryption options for Red Hat OpenShift on IBM Cloud clusters? Select all that apply.

A. Bring your own key
B. Worker node disks
C. Cluster secrets
D. Digital certificates

Answer A, B, and C. Data encryption options are BYOK for VPC and classic only, worker node disks, and cluster secrets.

Module 2
Check Your Knowledge

Question 3.

What role must you NOT assign at the same time as a service access role?

A. IBM Cloud IAM service access roles
B. IBM Cloud IAM platform access roles
C. IBM Cloud IAM Kubernetes access roles
D. IBM Cloud IAM plane access roles

Answer B. Do not assign IBM Cloud IAM platform access roles at the same time as a service access role. You must assign platform and service access roles separately.

Module 2
Check Your Knowledge

Question 4.

What do you want to do if you have services that run inside or outside IBM Cloud, or services that run on-premises, that are protected by a firewall?

A. Encrypt your data
B. Allow your worker nodes to communicate with services
C. Don't allow your worker nodes to communicate with services
D. Allow platform nodes to communicate with services

Answer B. Allow your worker nodes to communicate with services that are protected by firewalls.

Module 2
Check Your Knowledge

Question 5.

Which policy type can't add more security groups and apply them to your worker nodes?

A. VPC security groups
B. VPC access control lists
C. Kubernetes network policies

Answer C. VPC Security groups can't add more security groups and apply them to your worker nodes.

Module 2
Check Your Knowledge

Question 6.

If you want to allow traffic to/from a cluster in the IBM Cloud, the firewall has to allow the connection, which consists of what?

A. Protocols
B. IBM-managed key
C. Ports
D. IP ranges

Answer A, C and D. If you want to allow traffic to/from a cluster in the IBM Cloud, the firewall has to allow the connection, which consists of a protocol (tcp, udp, etc), IP (source/destination) and port (80 for http, 443 for https, etc).

Module 2
Check Your Knowledge

Question 7.

What can improve the security of your Red Hat® OpenShift® on IBM Cloud® cluster by allowing fewer worker nodes by isolating the networking workload?

A. Edge worker nodes
B. Platform worker nodes
C. Service worker nodes
D. None of the above

Answer A. Edge worker nodes can improve the security of your Red Hat® OpenShift® on IBM Cloud® cluster by allowing fewer worker nodes by isolating the networking workload.

Module 2
Check Your Knowledge

Question 8.

What do you need to do to Satellite endpoints in the Satellite control plane to control and audit network traffic between your IBM Cloud Satellite® location and services, servers, or apps that run outside of the location?

A. Encrypt
B. Close off
C. Open up
D. Restructure

Answer C. Open up Satellite endpoints in the Satellite control plane to control and audit network traffic between your IBM Cloud Satellite® location and services, servers, or apps that run outside of the location.