2019 IBM Cloud
用戶實作課程 秋季班

2019 IBM Cloud
用戶實作課程 秋季班

IBM Cloud
VPC, IKS, COS 架構設計說明

IBM Cloud Unit
雲端專家
馮建國 (Gordon)

Virtual Private Cloud (VPC)

What is a Virtual Private Cloud?

A Virtual Private Cloud (VPC) is **a private network in the public cloud** that combines

the logical **isolation** and **security** of a private cloud

+

the **availability**, **cost effectiveness** and **scalability** of the public cloud

Positioning Classic Infrastructure and VPC Infrastructure

Classic

Existing IaaS Platform
Ideal for "Lift & Shift" workloads

Bare Metal
Market leading service

VMware & SAP
Flexible deployment options

Network Appliances
Multiple vendors to choose from

Enterprise Storage Protocols
iSCSI and NFS-based offerings

Databases, SAP, VMware, GPU-based Workloads

Strong Connectivity
fast, simple to use together

VPC

All-new IaaS Platform
Ideal for Cloud Native + Cloud Enabled

Unified Experience
Fully integrated into IBM Cloud Platform

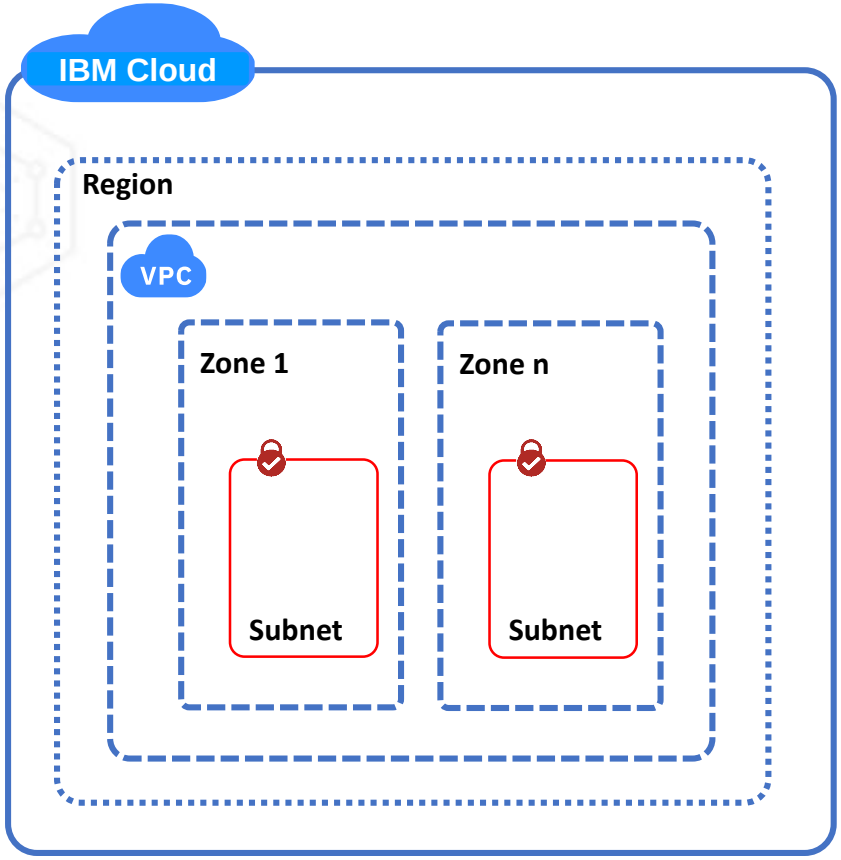
Developer Friendly API
New REST-based API aligned to industry

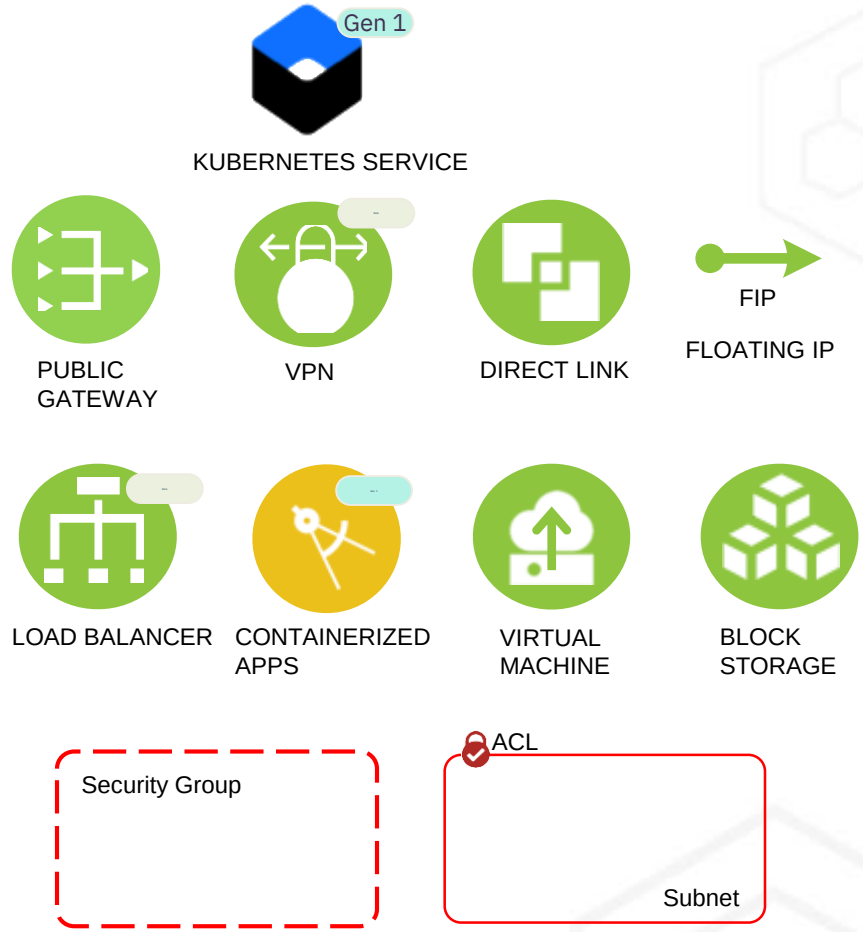
Faster, More Scalable Provisioning
Provision more resources, faster

Virtual Networking
Manage network topology via API, network performance up to 80Gbps

Web-facing applications, batch workloads, simulations, event streaming

Key Features of a VPC





VPC infrastructure - New and Improved Capabilities

Gen 2 Up to 80 Gbps Network performance for Virtual Server Profiles

Gen 2 Up to 5x faster provisioning

- New developer friendly API that easily integrates to existing tooling
- VPC users and permissions are fully integrated into IAM and the IBM Cloud platform
- “Bring your own IPs” (BYOIP) greatly improved in VPC, especially for overlapping IP space

Gen 1 “Bring your own Key” (BYOK) to encrypt block volumes using a customer managed key for improved security

- Simpler Block Storage access allowing volumes to mount and go, no need for clients to configure operating systems
- Import Custom Images from COS

VPC Features

Regions, Availability Zones, Subnets

- **Multi Zone Regions (MZR)**
- An IBM Cloud region with three availability zones that are logically and physically independent from one another but networked together

Availability Zones (AZ)

- Independent fault domains that do not share physical infrastructure
- An abstracted service end-point for fault tolerance
- Have latency requirement of <500 usec intra-zone & <2 ms inter-zone

Subnet

- Isolated networks, typically with open communication within the subnet, but controlled access to networks outside of the subnet, including the internet.
- Allows private address spaces with RFC1918
- Allows BYO Subnet range in addition to default range provided

Classic Infrastructure:

- Data Centers
- PODS

Available

VPC
- 5 per region

VPCs w/ Classic Access
- 1 per region, per account

Subnet
- 15 per VPC

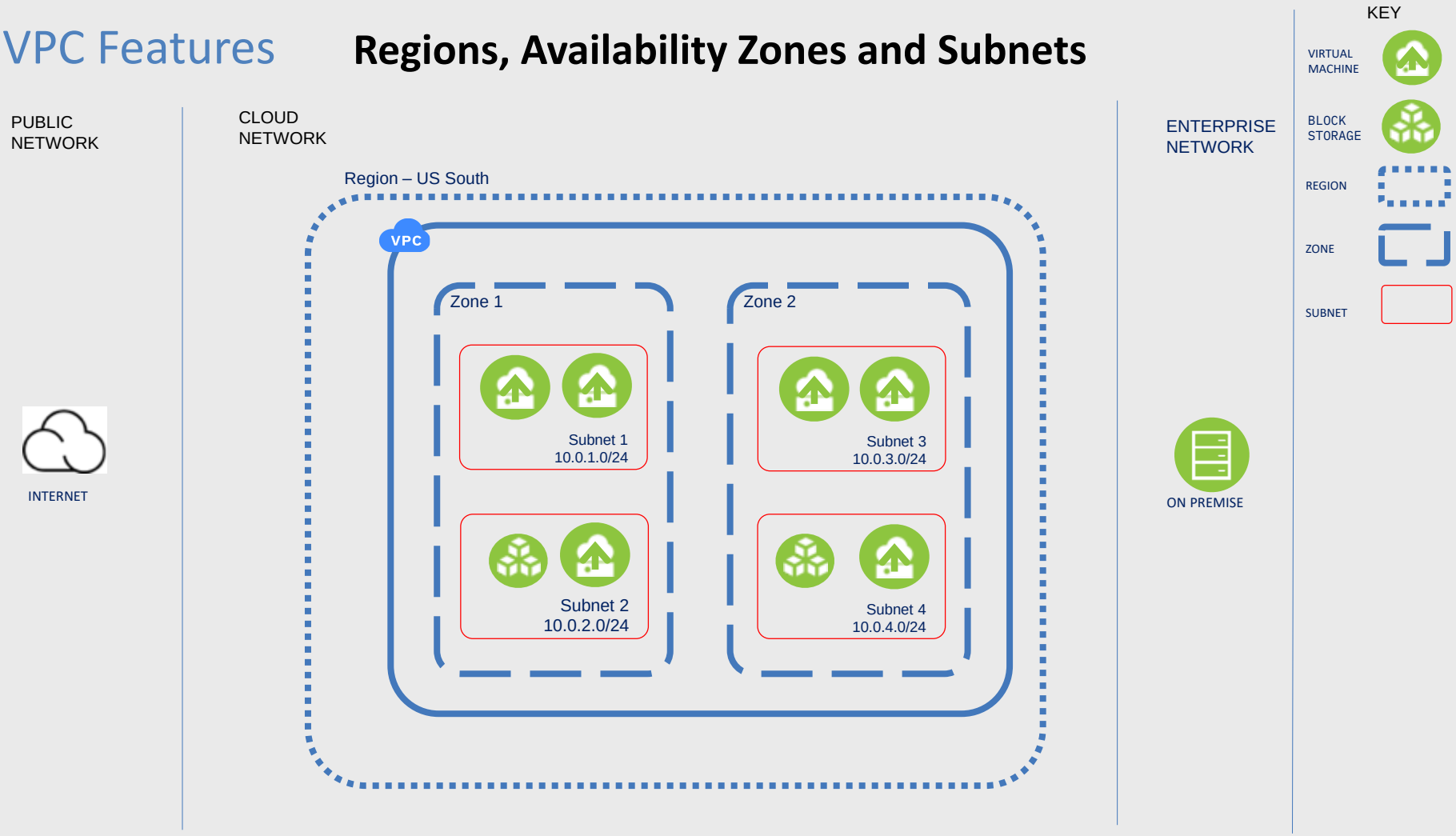
MZRs Gen 1
- us-south (DAL)
- jp-tok (TOK)
- eu-gb (LON)
- au-syd (SYD)
- eu-de (FRA)

MZRs Gen 2
- us-south (DAL)

For up-to-date quotas always refer to the Cloud Docs page

VPC Features

Regions, Availability Zones and Subnets



VPC Features Network Security

Access Control List (ACL)

- Enables customers to allow/deny ingress traffic to subnet and egress traffic from subnet
- ACL is stateless
- ACL consists of rules and each rule has source IP, source port, destination IP, destination port and protocol

Security Groups for VPC

- A virtual firewall that controls the traffic for one or more VSIs within a VPC
- A collection of rules that allow traffic to or from its associated VSI
- Allows for modification of those rules

Classic Infrastructure:

- Vyatta
- Fortigate
- Security Groups

Available

ACLs Gen 1
- 30 per region
- 20 ingress rules per ACL
- 20 egress rules per ACL

ACLs Gen 2
- 25 per VPC
- 25 ingress rules per ACL
- 25 egress rules per ACL

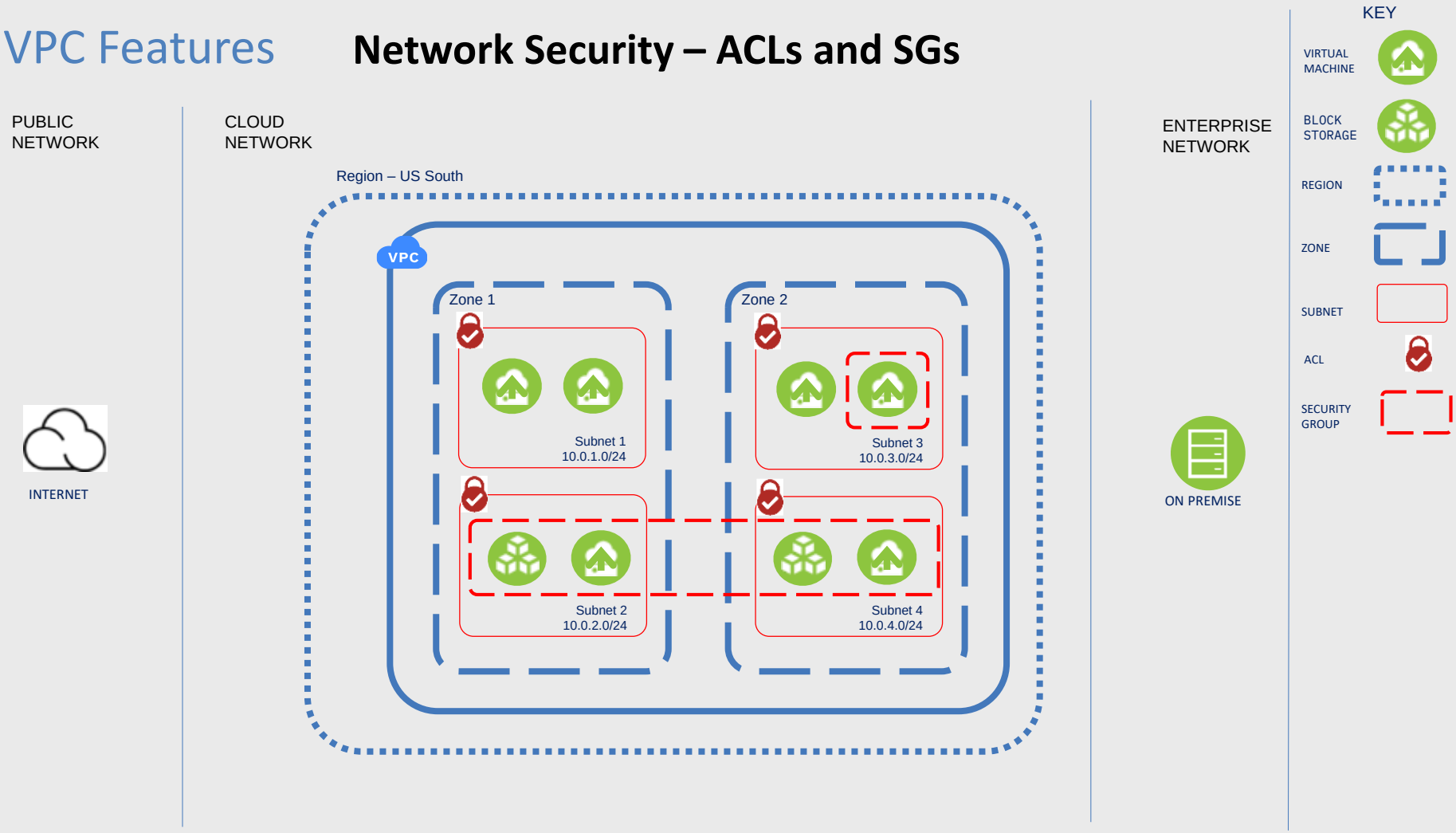
SGs Gen 1
- 500 per account
- 5 per network interface
- 50 rules per Security Group
- 5 remote rules per security group
- 100 NICS per SG

SGs Gen 2
- 25 per VPC
- 25 rules per Security Group
- 5 remote rules per security group

For up-to-date quotas always refer to the Cloud Docs page

VPC Features

Network Security – ACLs and SGs



VPC Features

Internet Connectivity

Public Gateway (PGW)

- enables a subnet (with all the VSIs attached to the subnet) to connect to the Internet
- optionally create a PGW and attach a subnet to the PGW

- A public IP address reachable by the Internet
- FIP addresses are associated to instances in a VPC
- Floating IP address are reserved from a pool of available Floating IP addresses
- FIPs can be associated / un-associated to any instance in the same VPC

Classic Infrastructure:

- Vyatta / VRA VPN
- Juniper vSRX
- Direct Link

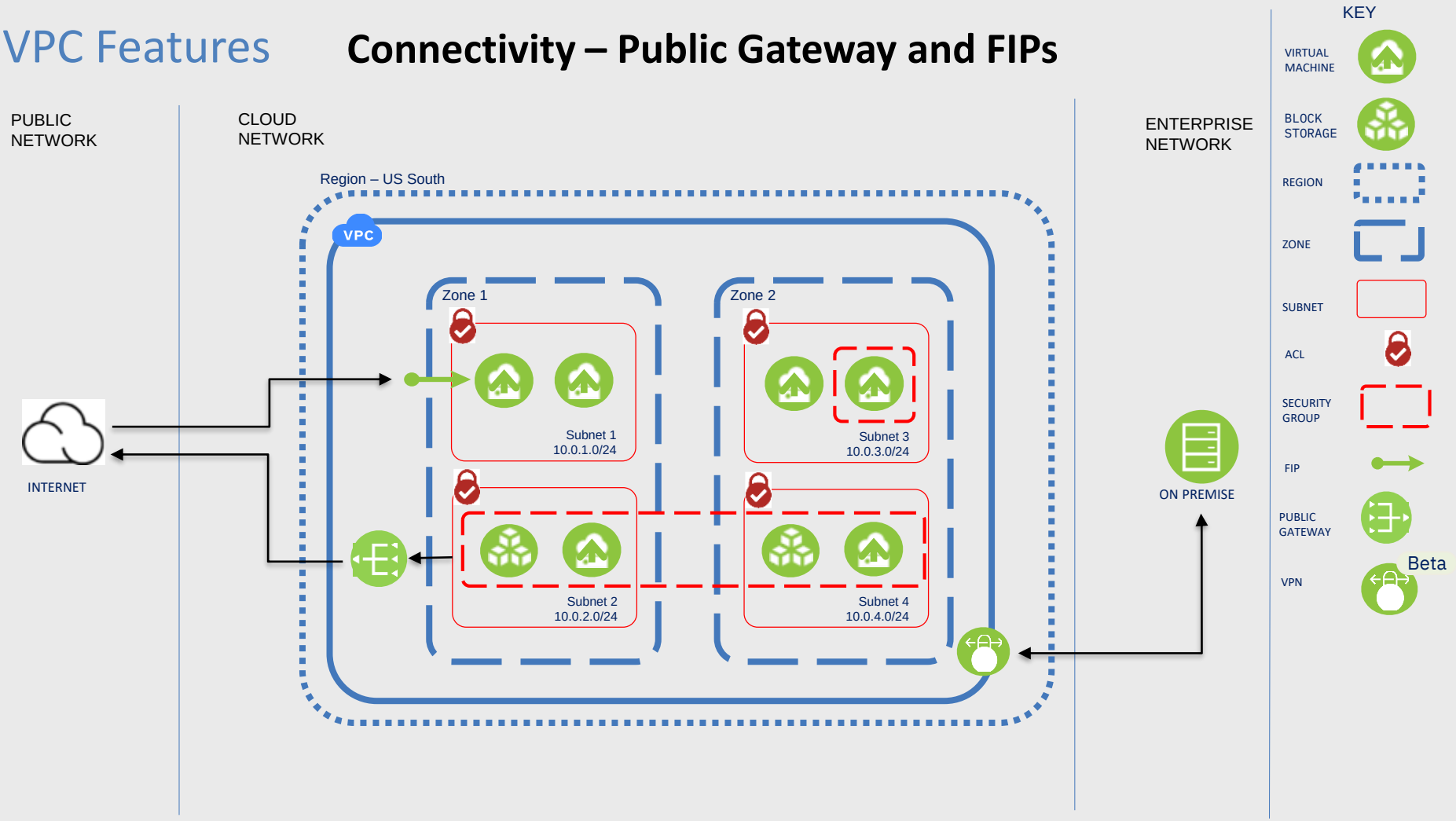
Available

Gen 1	Gen 2
Public Gateways - 1 per VPC per zone	**Public Gateways** - 1 per VPC per zone
Address Prefixes - 5 per VPC per zone	**Address Prefixes** - 5 per zone
FIP - 100 per zone per account	**FIP** - 5 per VPC per zone

For up-to-date quotas always refer to the Cloud Docs page

VPC Features

Connectivity – Public Gateway and FIPs



VPC Features

Elastic Load Balancing

Load Balancer for VPC

- Layer 4/7 load balancing w/ HTTP, HTTPS, TCP ports
- Integrated health checks
- Round Robin, Weighted Round Robin and Least Connections Algorithms
- FQDN for VIP on public subnet, backend servers on customer's private network
- SSL Offload
- Termination of incoming HTTPS traffic
- Seamless integration with Certificate Manager service

- Load Balancer is in Beta for Gen 2
- No charges for Load Balancing during the Beta period

- **Classic Infrastructure:**

- Cloud Load Balancer
- Netscaler VPX, MPX

Available

Cloud Load Balancer

- 20 per account
- 10 listeners per load balancer
- 10 pools per load balancer
- 50 members per pool

For up-to-date quotas always refer to the Cloud Docs page

VPC Features Global Load Balancing

Cloud Internet Services

- A Global Load Balancer (GLB) and more

Load balancing, edge performance and security services across over 150 global locations:

- Global Load Balancing: 6 origins with 60s health checks originating from one geo-region
- DDoS Protection: Un-metered protection with 14Tbps always-on capacity
- Web Application Firewall with on/off security policy
- TLS Certificate Support: Wildcard certificate or upload customer certificate
- Domain Name Server (DNS)
- Caching / Content Delivery Network with 50 page rules

- **Classic Infrastructure:**
- Cloud Internet Services

Available

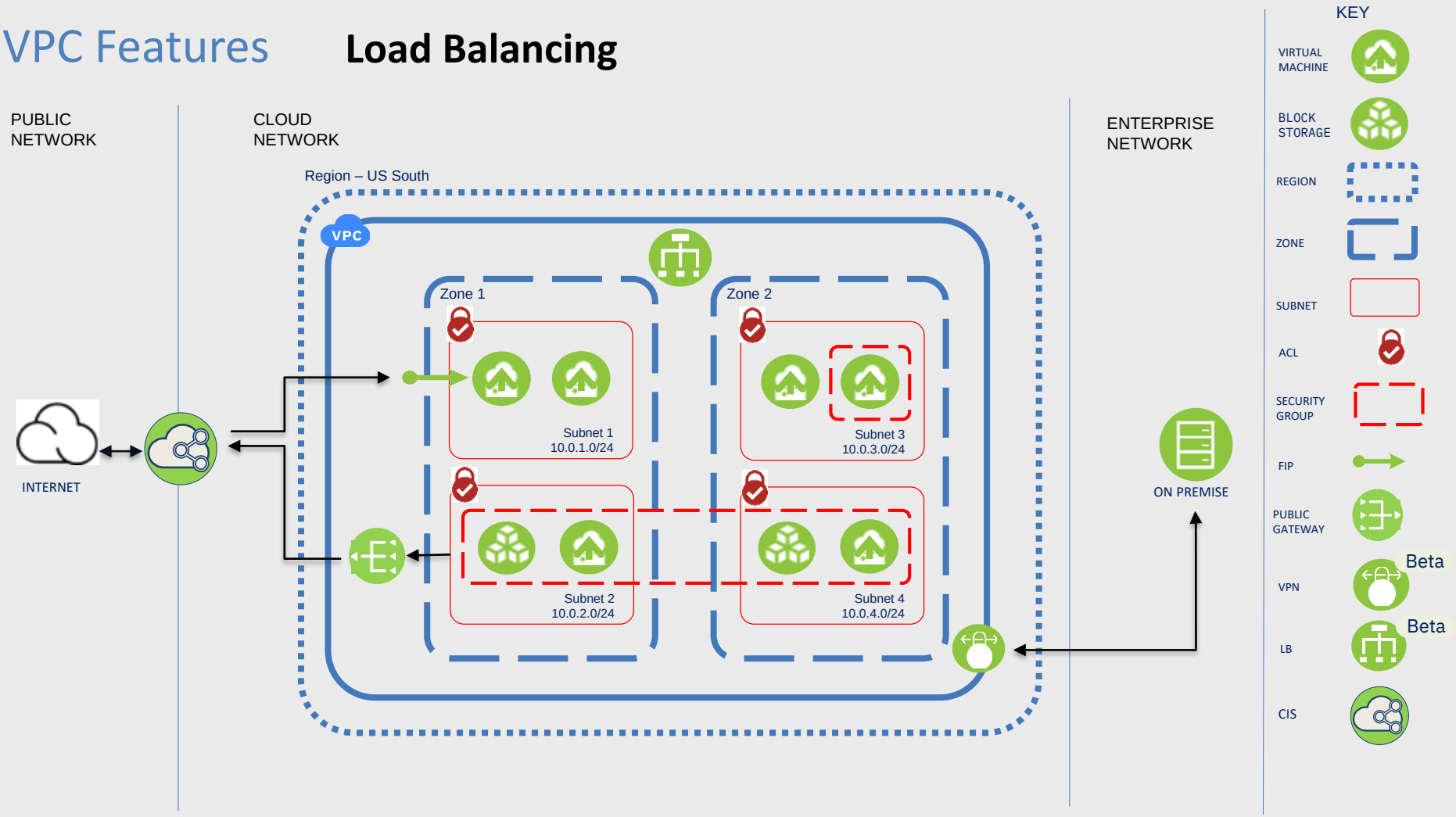
CIS

- 30 day free trial or $275/mo. Per domain

For up-to-date quotas always refer to the Cloud Docs page

VPC Features

Load Balancing



VPC Features **Compute**

Virtual Server Instances

- Multi- homed
- Multiple vNIC
- Profiles of pre defined vcpu/RAM configurations
  - Balanced (1 vcpu: 4 GB RAM)
  - Compute (1:2)
  - Memory (1:8)
- Includes new larger sizes up to 62x248 Gen 1, 48x192 Gen 2
- Basic Platform Integration: IAM, Resource Groups, Usage Dashboard
- Basic monitoring and logging

Stock OS options:

- CentOS 7.x
- Ubuntu 16.04 Gen 1, 18.04
- Debian 8.x , 9.x
- Windows 2016, 2012 R2, 2012
- RHEL 7.x

Custom image import

SSH only authentication for Linux images

SSH key encryption for Windows passwords

- **Classic Infrastructure:**
- VSIs

Available

Gen 1	Gen 2
VSIs	**VSIs**
- 100 VSIs per account	- 200 vCPUs per region
- 5 vNICs per VSI	- 800GB RAM per region
- 1 Floating IP Address per VSI	- 5 vNICs per VSI
- 100 SSH keys per account	- 1000 SSH keys per account
- Up to 16Gbps	- Up to 80 Gbps
- Provision in minutes	- Provision in seconds

For up-to-date quotas always refer to the Cloud Docs page

All VSIs will require a 100 GB primary volume

Primary volume is Block Storage with General Purpose Tier (3 IOPs per GB)

Users will be billed for storage

VPC Features **Storage**

Block Storage

- Boot volumes are required to boot VSI's within a VPC
- Customers who need additional storage beyond a boot disk for VSI can attach additional storage to support their workloads
- Encrypt volumes (Boot and Secondary Data) with keys stored in Key Protect or HPCS during VPC VSI creation
- Enterprise BYO Custom Images is supported
- Volumes are encrypted by default via the provider managed key

- **Classic Infrastructure:**
- Block Storage for Classic

Available

Gen 1

Block Storage

- 4 secondary volumes may be requested per new instance ,for existing instances with less than 4 cores 4 volumes is the limit
- 12 secondary volumes may be requested per instance for existing instance with 4 or more cores

Gen 2

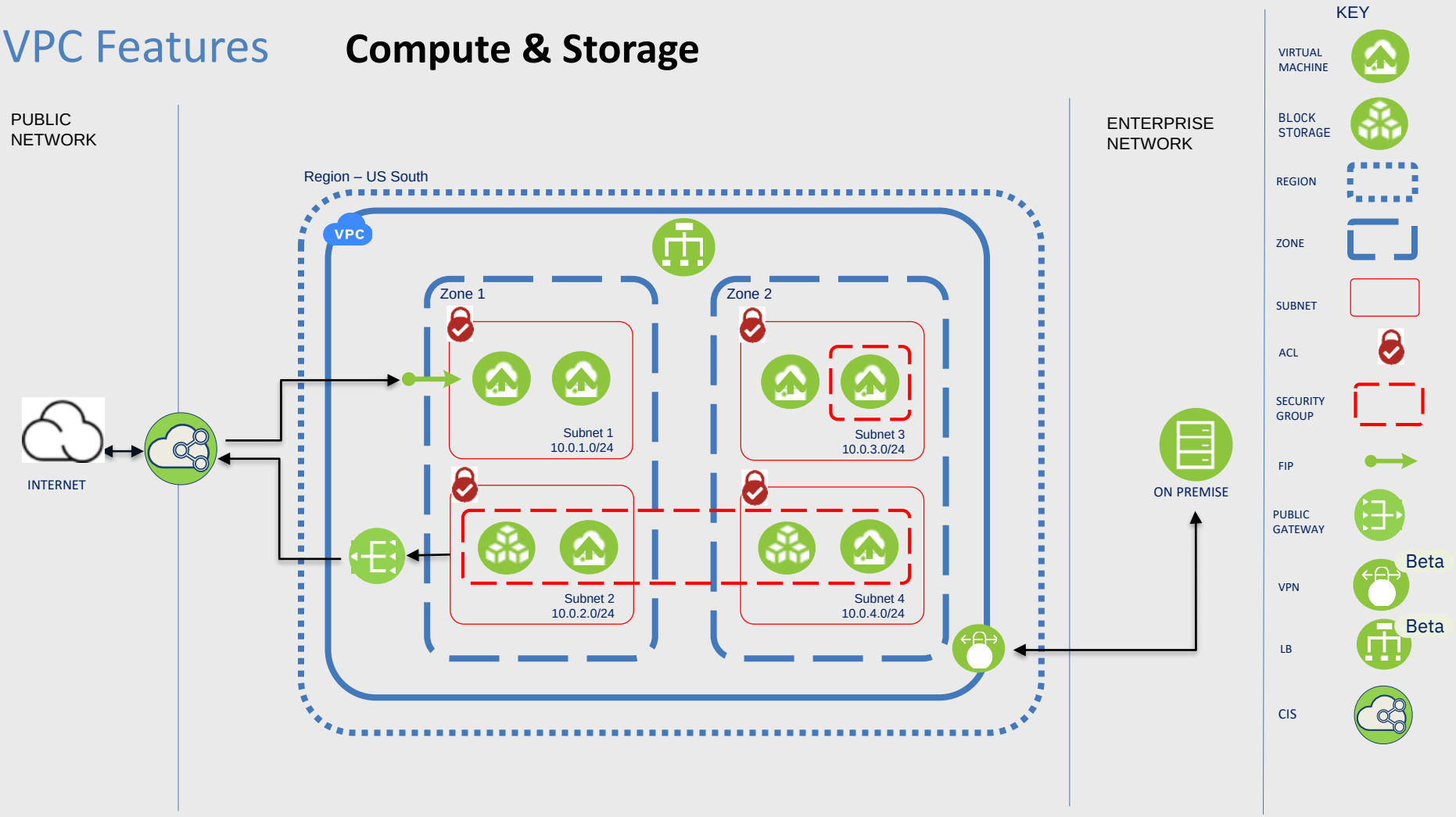
Block Storage

- 750 Block Storage Volumes per zone

For up-to-date quotas always refer to the Cloud Docs page

VPC Features

Compute & Storage



VPC Features

Hybrid Connectivity

VPN-as-a-Service

- Secure connection via an encrypted tunnel between customer and VPC or VPC to VPC
- Adheres to common protocol and encryption standards

Direct Link via Classic Access

- Private connectivity for maximum speed, security and resiliency
- Variety of connectivity options and port speeds from 50Mbps to 10Gbps in one of IBM Cloud's global data centers
- Over 30 partners to choose from worldwide

- **Classic Infrastructure:**

- IPSec VPN
- Direct Link

Available

VPN

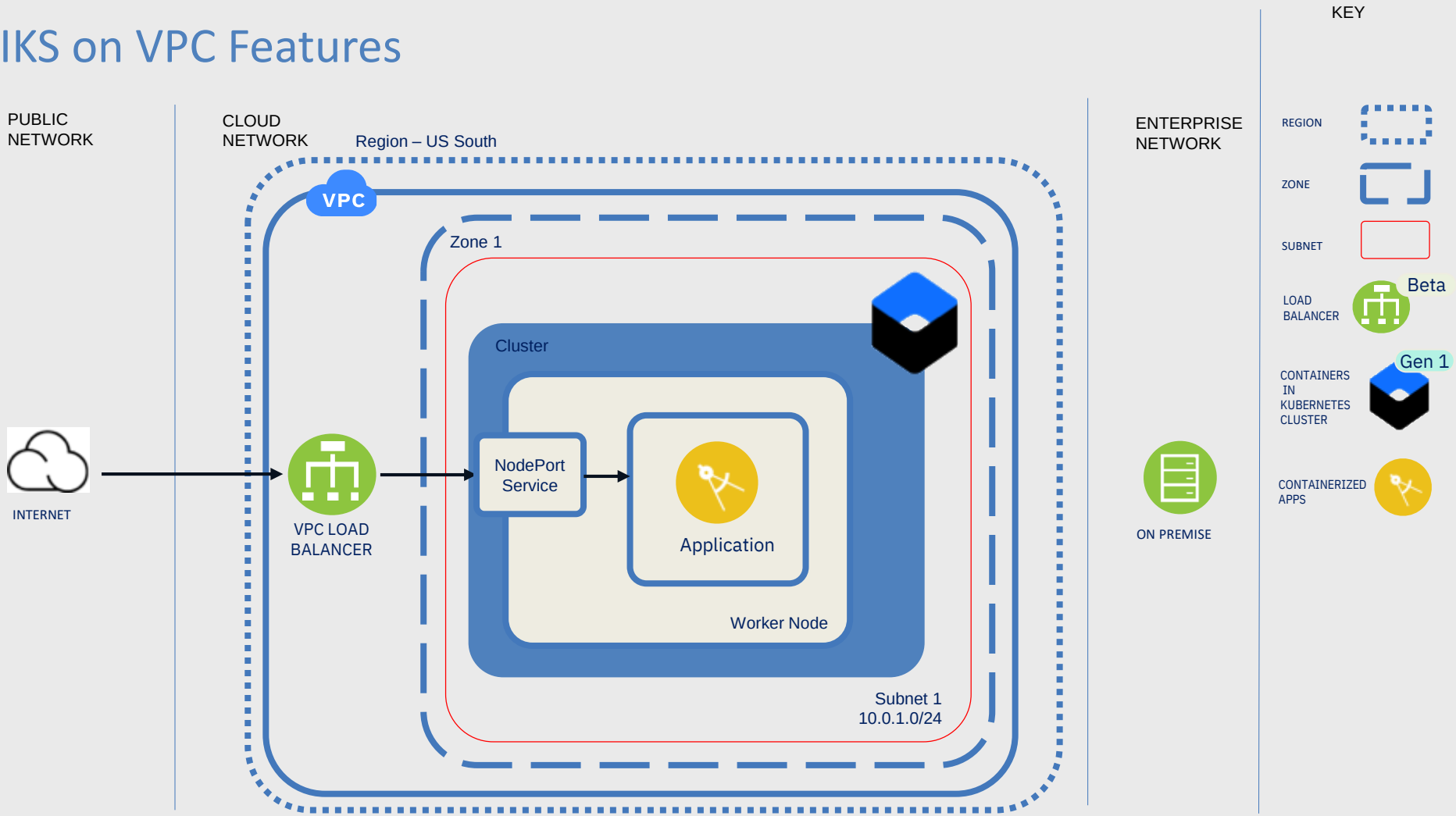
- 20 gateways per account
- 3 gateways per zone
- 10 VPN connections per gateway

Direct Link

- Requires VPC w/ Classic Access

For up-to-date quotas always refer to the Cloud Docs page

IKS on VPC Features



IKS on VPC Features

Gen 1

IKS Workers

- New machine types
- Primary disk is SAN
- Provisioned in customer Subnets
- *ibmcloud ks worker-reload* now via *ibmcloud ks worker-replace*
- *ibmcloud ks worker-update* now replaces worker with new one
- Flat pricing model (no tiering for extended use of worker)
- Compatible with IBM Cloud Service Endpoint (for connectivity with Kubernetes Master)

IKS Storage

- Support for Block Storage PVCs
- Support for Object Storage PVCs

Compatible with VPC VPNaaS

- Leverage common VPN solution across VMs and IKS Workers

IKS Load Balancer and ALB/Ingress

- Leverages VPC LBaaS
- DNS based HA
- Supports multizone Public and Private
- Does not support source IP preservation
- Load Balancer is TCP only (can carry HTTP and HTTPS traffic)

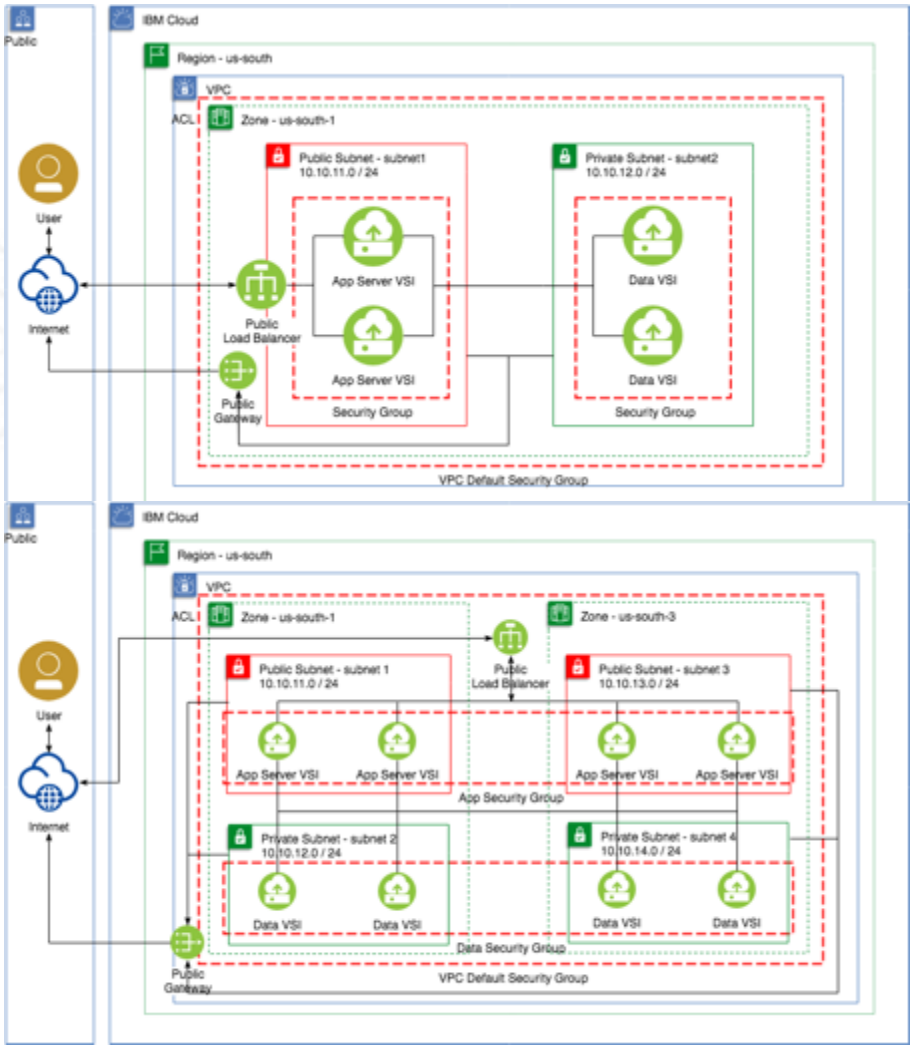
IKS Support for VPC Network ACLs and Kubernetes NetworkPolicy

- Create VPC subnets for IKS clusters and create network ACLs for easy host level traffic control.
- Use Kubernetes NetworkPolicy for container/Pod level network access control.

- **Classic Infrastructure:**

- IKS Workers
- IKS Storage
- IKS Load balancer
- IKS Support
- Kubernetes NetworkPolicy

For up-to-date quotas always refer to the Cloud Docs page



Example Architectures and Solutions

Creating a classic cluster in your Virtual Private Cloud (VPC):
https://cloud.ibm.com/docs/containers?topic=containers-vpc_ks_tutorial&origin_team=T02J3DPUE

Basic 3 tier app w LB:
https://github.ibm.com/customer-success/ibmcloud/tree/master/VPC_Phase1/VPC_Scenarios/vpc1

Multi zone 3 tier app w LB:
https://github.ibm.com/customer-success/ibmcloud/tree/master/VPC_Phase1/VPC_Scenarios/vpc2

Private and public subnets:
https://cloud.ibm.com/docs/tutorials?topic=solution-tutorials-vpc-public-app-private-backend

Isolated workloads multi zone:
https://cloud.ibm.com/docs/tutorials?topic=solution-tutorials-vpc-multi-region

VPC VPN Gateway:
https://cloud.ibm.com/docs/tutorials?topic=solution-tutorials-vpc-site2site-vpn

Use bastion host:
https://cloud.ibm.com/docs/tutorials?topic=solution-tutorials-vpc-secure-management-bastion-server

IBM Kubernetes Service (IKS)

IBM Cloud
Kubernetes Service

kubernetes

A **managed service** providing an intuitive user experience with simplified cluster lifecycle management on upstream **Kubernetes** clusters. Includes built-in **security and isolation** to enable rapid delivery of apps, while leveraging IBM Cloud Services including Weather data, IoT, Analytics, or **AI capabilities with Watson.** Available in six IBM regions worldwide, including **35+ datacenters**.

Learn more at: www.ibm.com/cloud/container-service

AICPA SOC · ISO 3402 · HIPAA · PCI DSS · certified kubernetes 1.12 · certified kubernetes 1.13 · certified kubernetes 1.14

Developer Productivity, Choice, Control, & Consistency

Speed

Portability

Performance & Control

Cloud Functions
"Serverless" / Event Driven Apps

Cloud Foundry
Open PaaS Environment

Containers & Kubernetes
Maximum Portability

Virtual Server or VMware
Leverage Existing Images & Tools

Bare Metal
Maximum Performance & Control

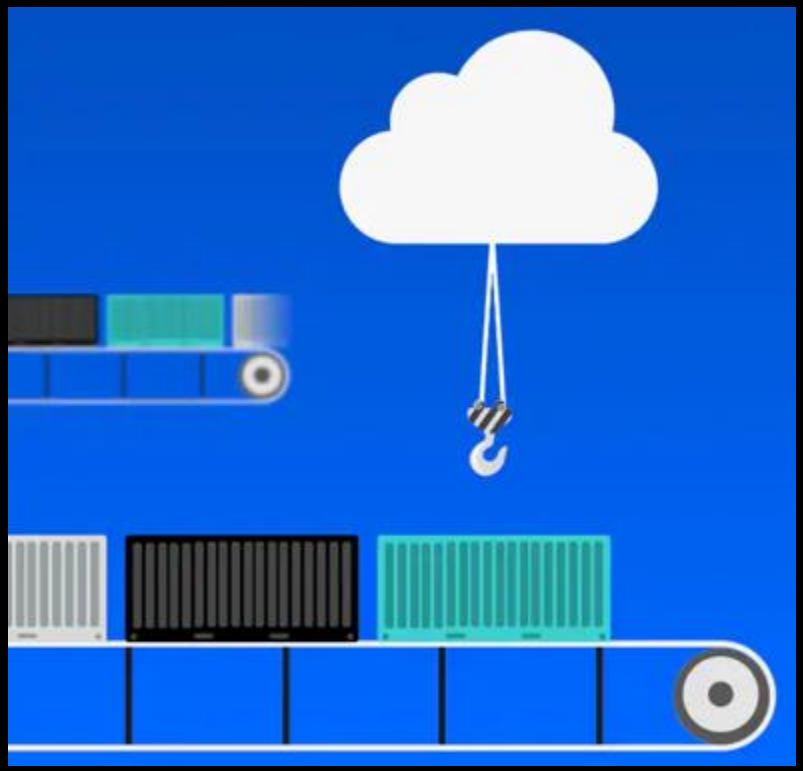
Language/ Framework

.js .java liberty .py .php .go .rb express spring

Containers change the economics of delivery

Organizations are adopting containers to improve developer productivity, efficiency in DevOps, and application portability

- Lightweight packaging that includes the software and all its dependencies
- Easily portable across on-premises and public cloud environments
- More efficient use of infrastructure than traditional VM deployments



Orchestration requirements with containers

Kubernetes provides an open-source solution for:

- Container deployment scheduling
- Cluster management
- Service discovery
- Provisioning
- Monitoring
- Configuration management

Business value of containerization and Kubernetes:

- Expedite innovation to market
- Accelerate application development
- Increase operational efficiency
- Enable DevOps
- Eliminate vendor lock-in

Intelligent Scheduling

Self-healing

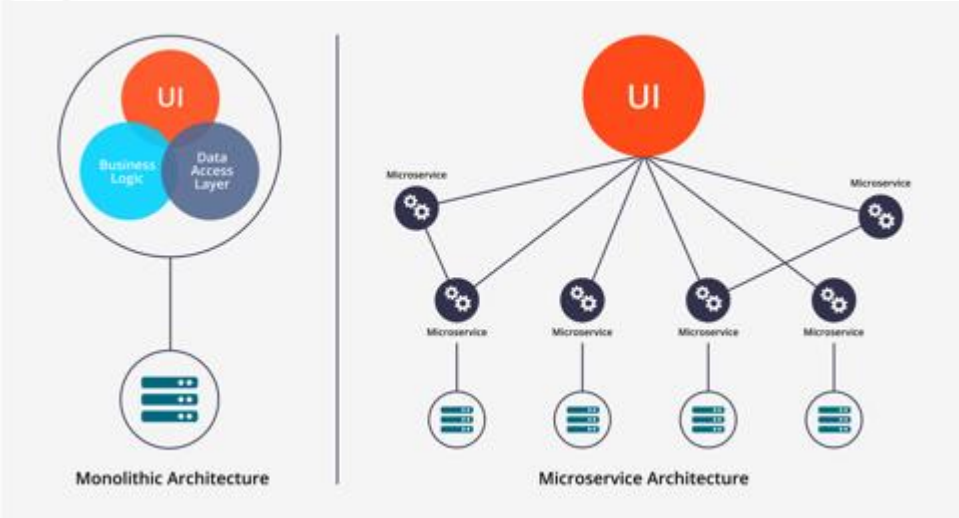
Horizontal scaling

Service discovery & load balancing

Automated rollouts and rollbacks

Secret and configuration management

Microservices



An engineering approach focused on decomposing an application into single-function modules with well defined interfaces which are independently deployed and operated by a small team who owns the entire lifecycle of the service.

Microservices accelerate delivery by minimizing communication and coordination between people while reducing the scope and risk of change.

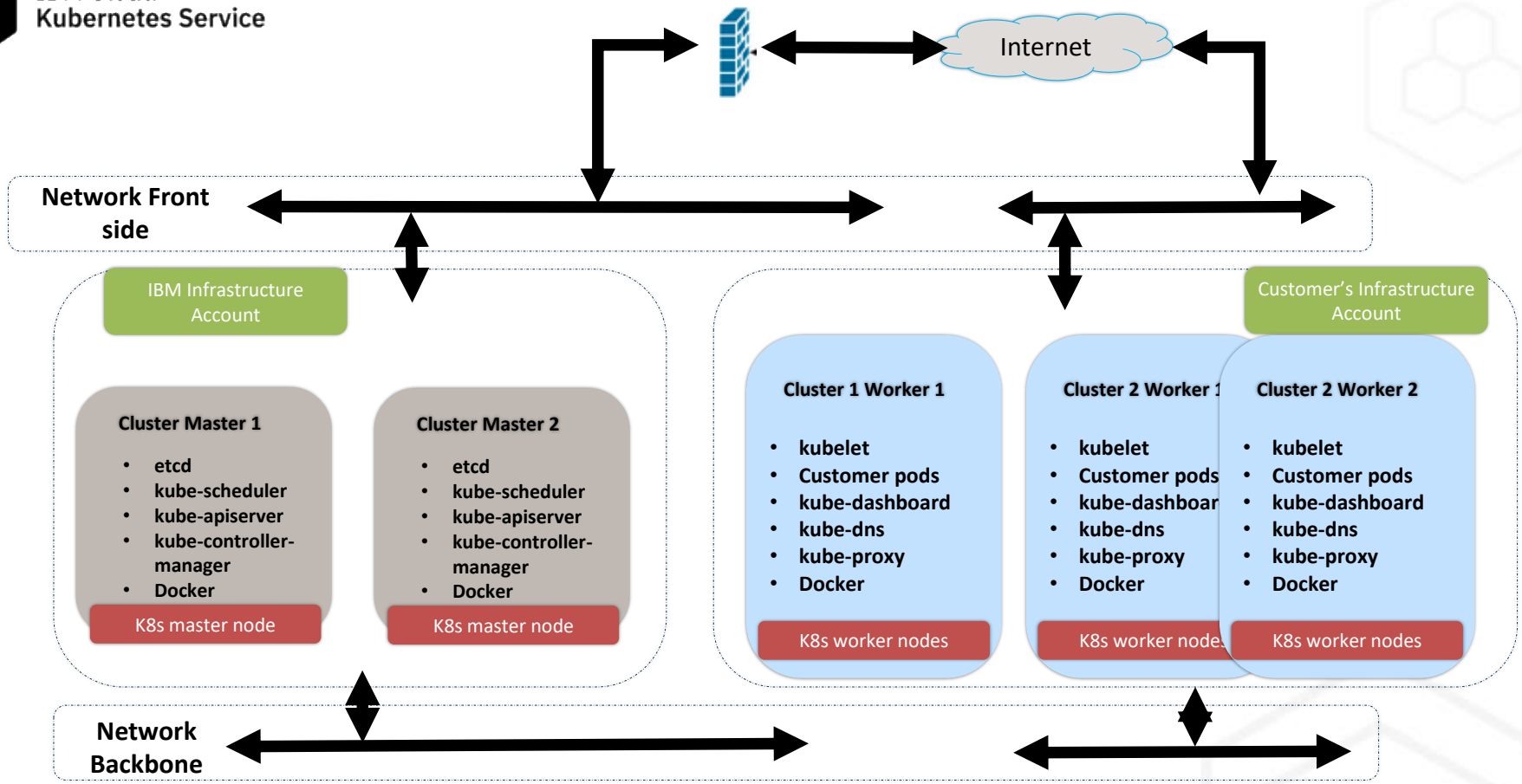
Workload flexibility

6 IBM Cloud Regions, 35+ Datacenters

https://console.bluemix.net/docs/containers/cs_regions.html#regions-and-locations

Region04	Data Center	City
AP North	• hkg02 • seo01 • sng01 • tok02 • tok04 • tok05	• Hong Kong • Seoul • Singapore • Tokyo
AP South	• mel01 • syd01 • syd04	• Melbourne • Sydney
EU Central	• ams03 • **oslo01** • **mil01** • par01 • fra02 • fra04 • fra05	• Amsterdam • Oslo • Milan • Paris • Frankfurt
United Kingdom	• lon02 • lon04 • lon05 • lon06	• London
US East	• mon01 • tor01 • wdc04 • wdc06 • wdc07	• Montreal • Toronto • Washington, DC
US South	• sao01 • hou01 • **sjc03** • **sjc04** • dal10 • dal12 • dal13	• Sao Paulo • Houston • San Jose • Dallas

IBM Cloud
Kubernetes Service



IKS Capabilities

Simplified cluster management

Design your own cluster

Security & isolation

Extend apps with IBM Cloud services

Native open-source experience

Integrated operational tools

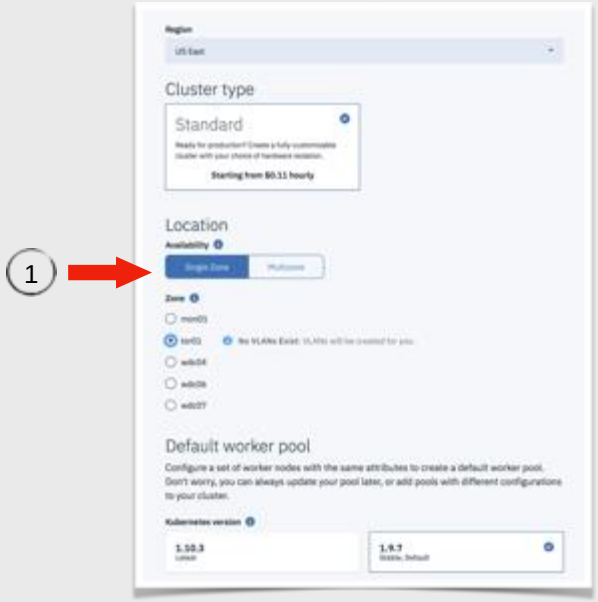
IBM Cloud
Kubernetes Service

Simplified Cluster Management

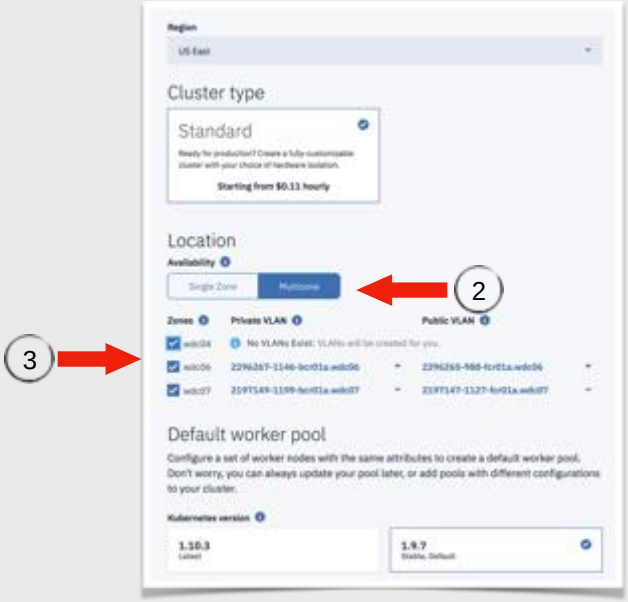
- Intuitive graphical user experience
- CLI and API alternatives
- Fully managed master nodes
- Highly available (HA) masters
- User controlled worker node management
- Worker node auto-recovery
- Worker node auto-scaling

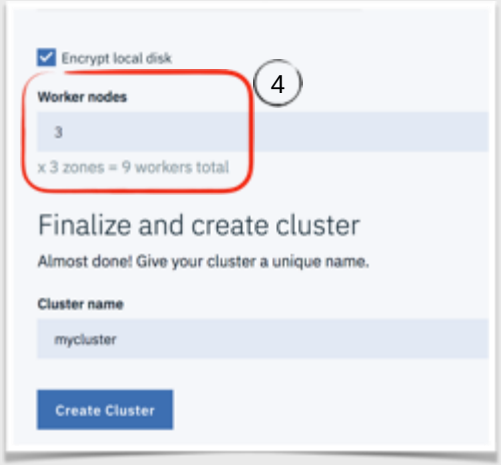
Simplified Cluster Management

Single Zone Cluster

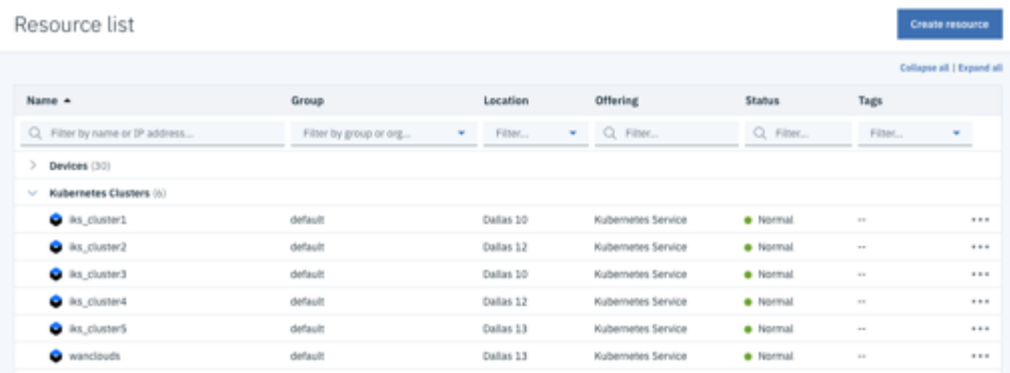


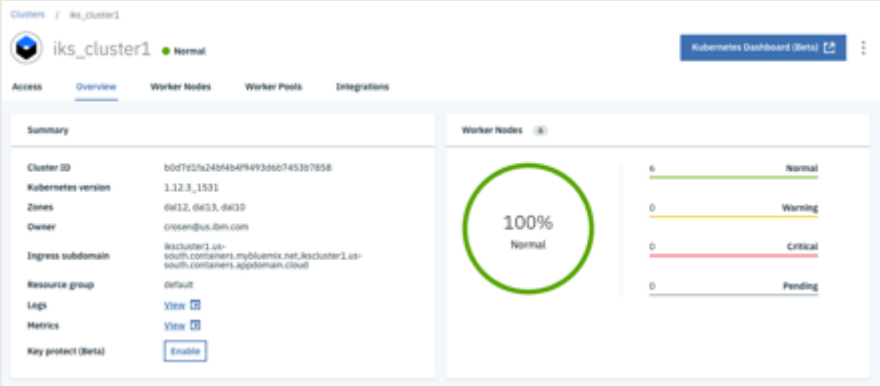
Multizone Cluster

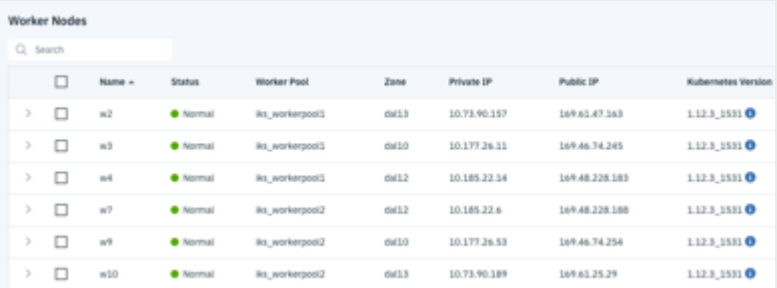




Simplified Cluster Management







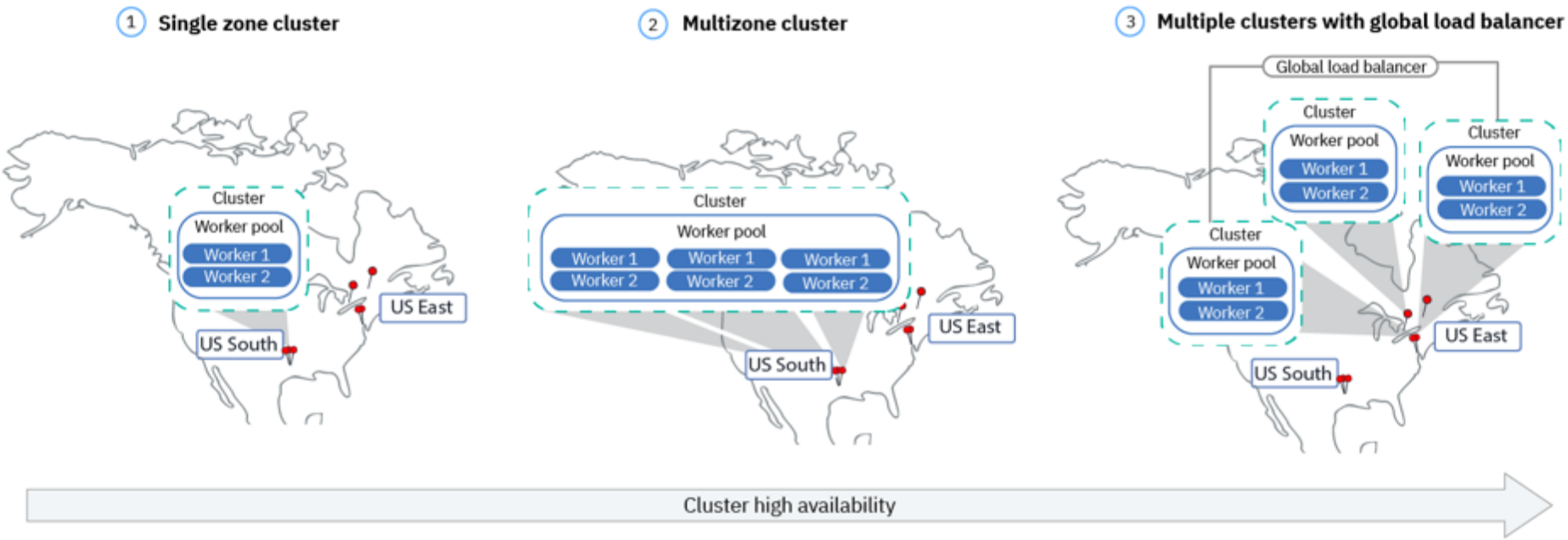
What are high availability masters?

HA masters will dramatically increase availability of the API server within your IKS clusters.

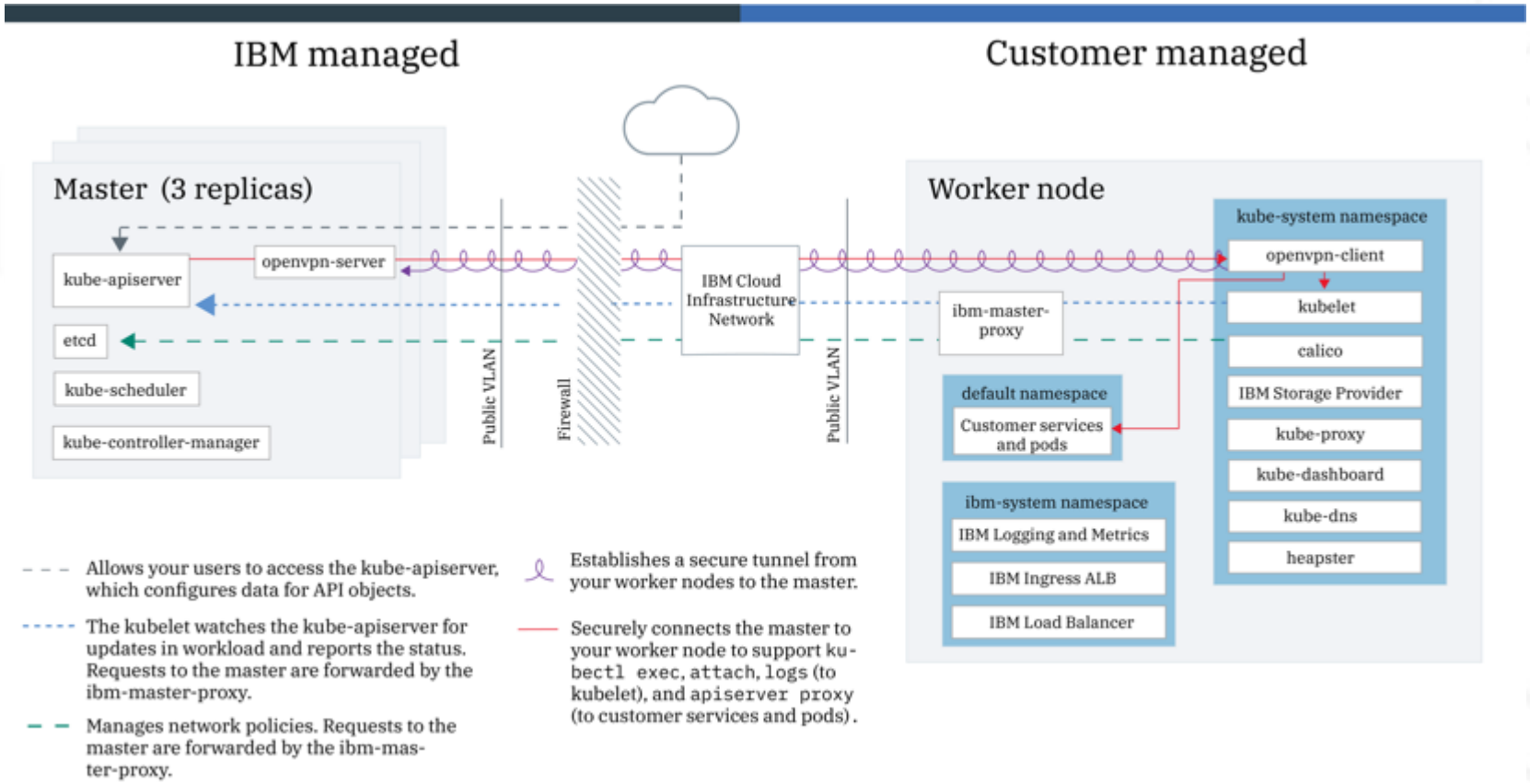
In an MZR, those masters are distributed across datacenters where that cluster is running, ensuring availability during upgrades or catastrophic outage to one DC.

In an SZR, those masters are distributed across different hosts, ensuring availability during upgrades of Kubernetes versions or physical host level access.

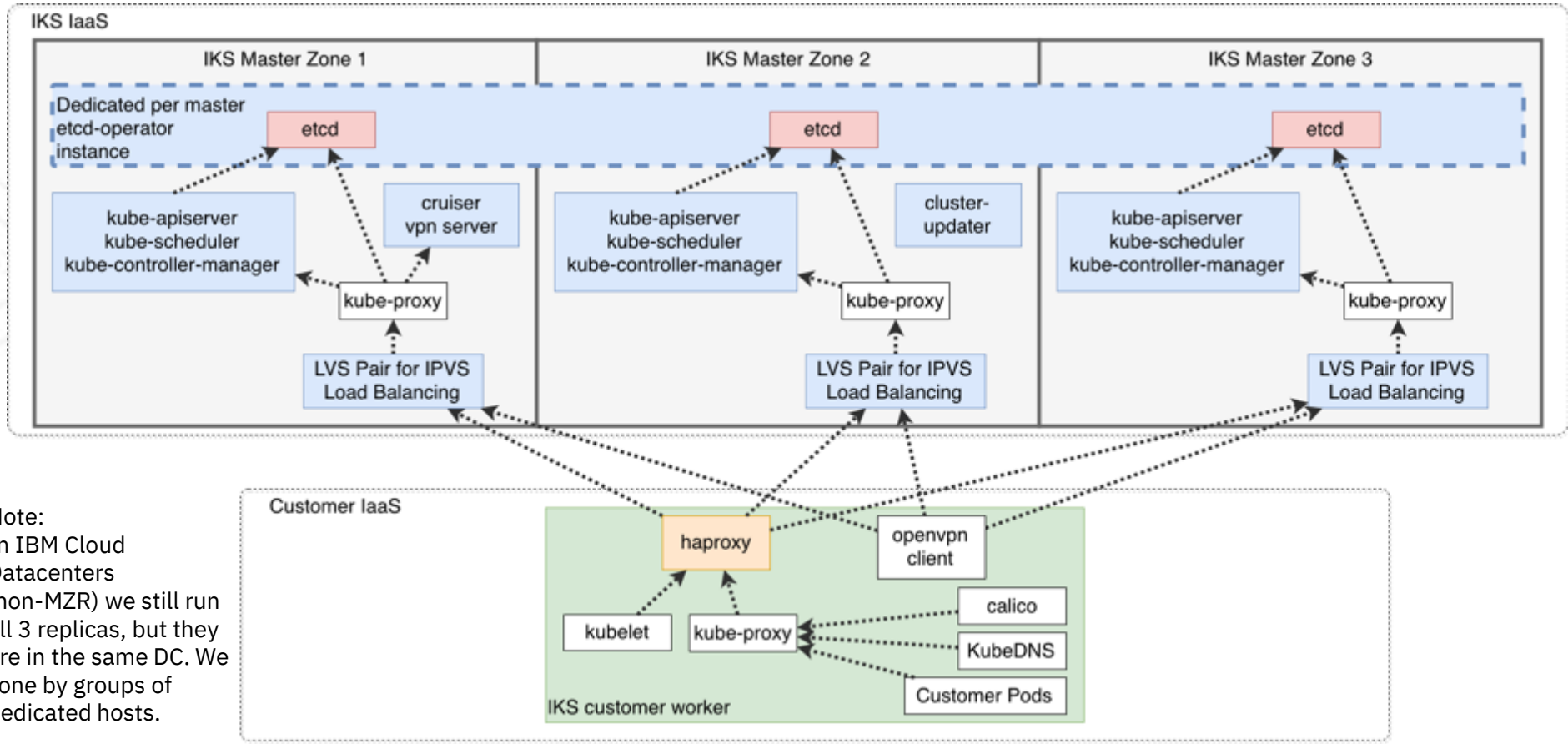
Clustering


1 Single zone cluster
Cluster
Worker pool
Worker 1
Worker 2
US East
US South
2 Multizone cluster
Cluster
Worker pool
Worker 1
Worker 2
Worker 1
Worker 2
Worker 1
Worker 2
US East
US South
3 Multiple clusters with global load balancer
Global load balancer
Cluster
Worker pool
Worker 1
Worker 2
Cluster
Worker pool
Worker 1
Worker 2
Cluster
Worker pool
Worker 1
Worker 2
US East
US South
Cluster high availability

IKS Management Architecture – with HA Masters

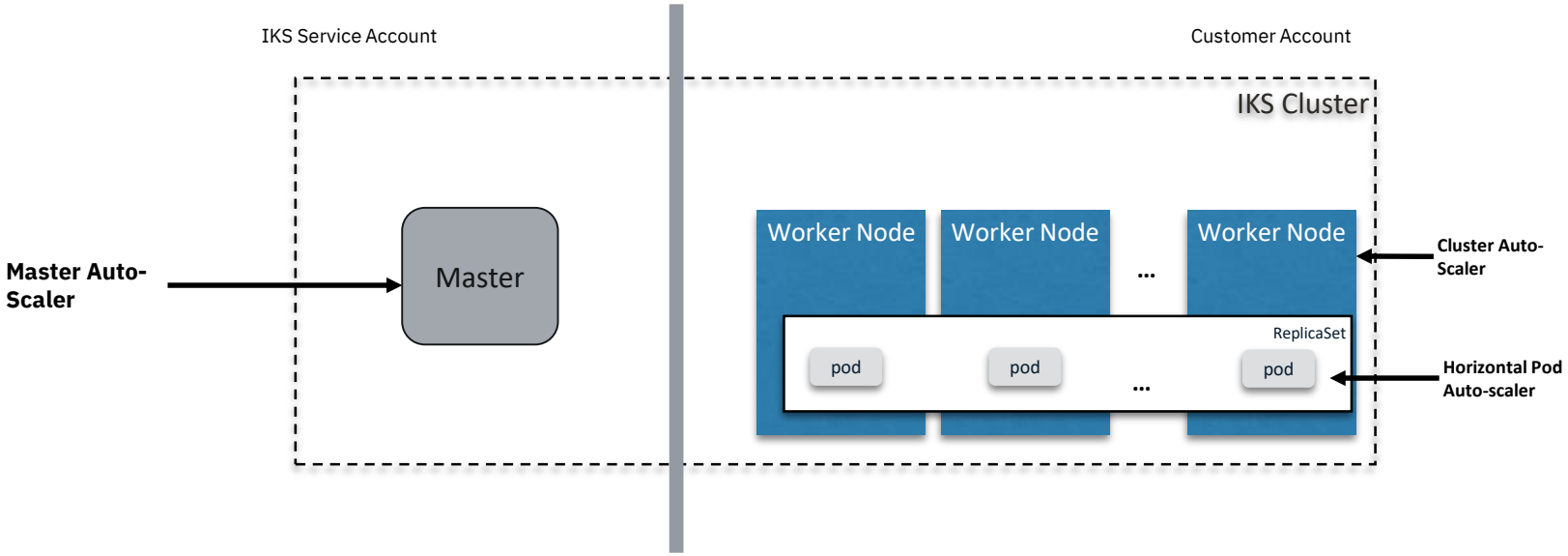


HA Masters Architecture



Note:
In IBM Cloud Datacenters (non-MZR) we still run all 3 replicas, but they are in the same DC. We zone by groups of dedicated hosts.

Auto-Scaling



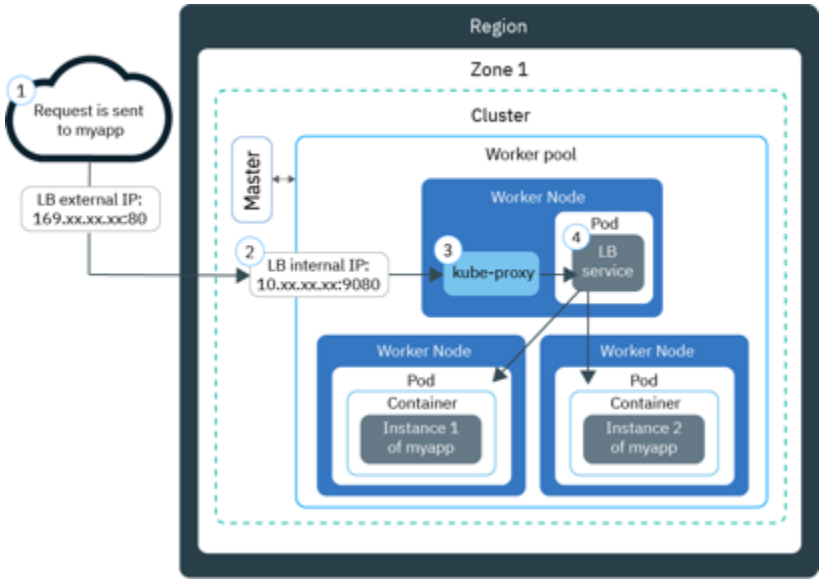
IBM Cloud
Kubernetes Service

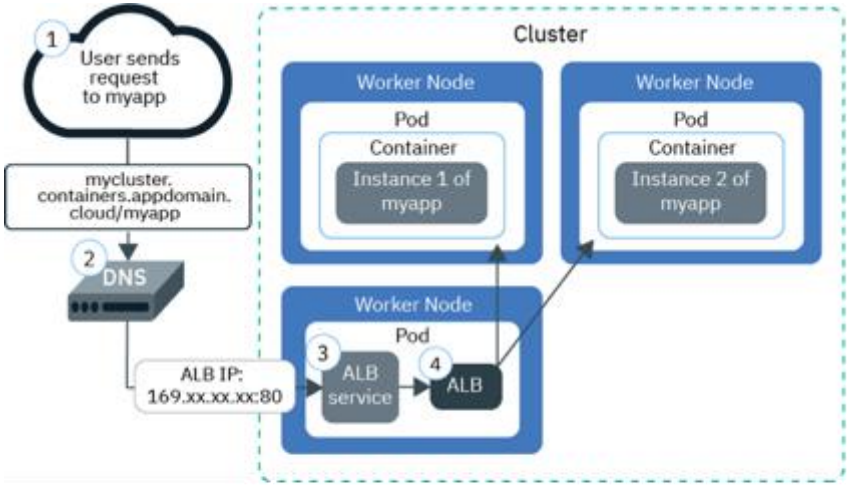
Design Your Own Cluster

- Tunable capacity
- Select between shared and dedicated compute using virtual server instances
- Bare metal worker nodes enabling Trusted Compute
- Multizone clusters in IBM Cloud multizone regions and single zone clusters in 25+ datacenters
- Edge nodes
- Configurable networking and storage
- Integrated VPN in-cluster providing IPSec tunnels

Load Balancer and Ingress

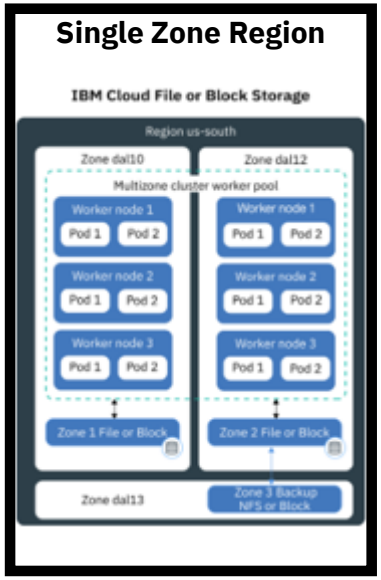
- Cloudflare DNS
- Multizone load balancer with health checks
- Wildcard certificate management by IBM Cloud Certificate Manager
- AppID oauth support
- Public and private options
- *Bring your own ingress controller*
  - Community ingress controller
  - Istio ingress gateway
- *Controlled ALB update*

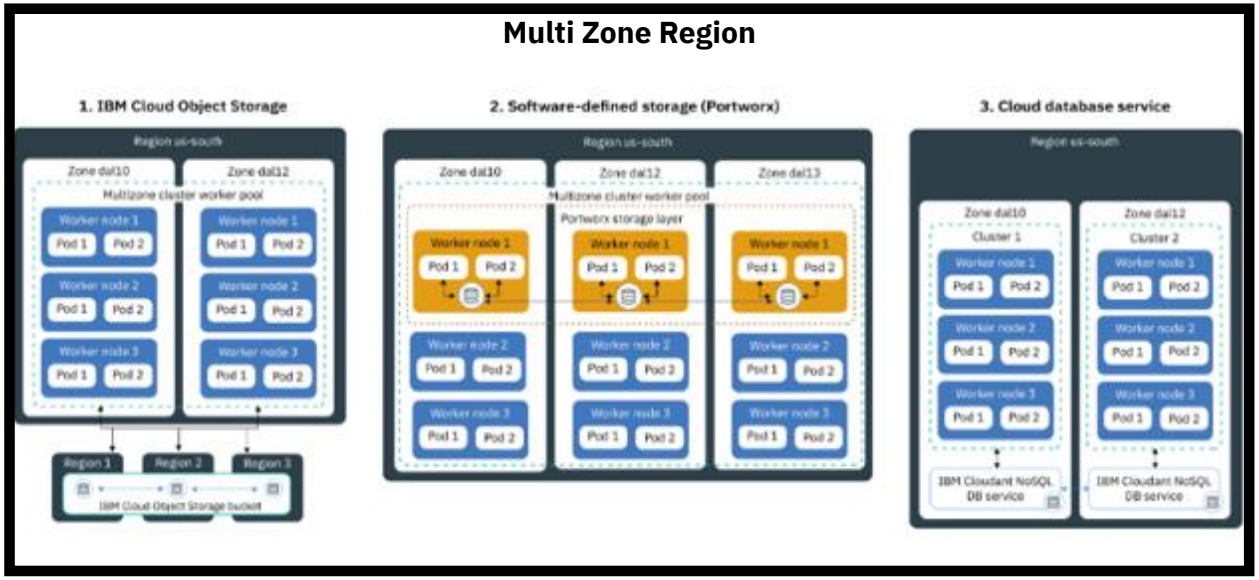





```
+ bx cs albs --cluster dan-istio2
OK
ALB ID                                                  Enabled  Status   Type    ALB IP
private-cr8b68ac88787345f9b35a622b6dfc556f-alb1         false    disabled private -
public-cr8b68ac88787345f9b35a622b6dfc556f-alb1          true     enabled  public  169.60.89.198
```

Persistent Storage

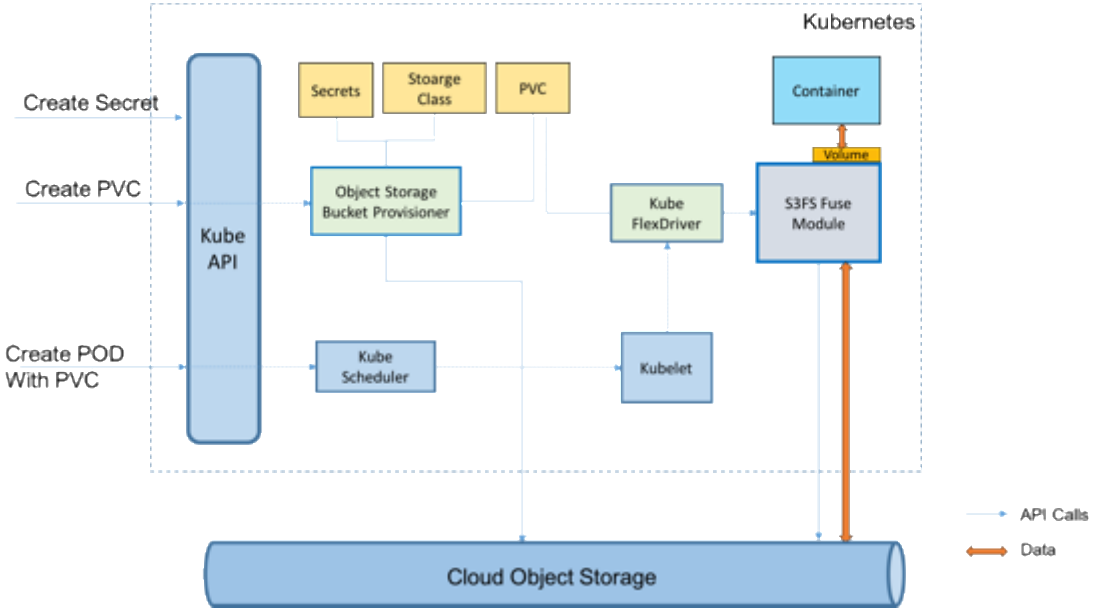




https://console.bluemix.net/docs/containers/cs_storage_planning.html#choose_storage_solution

S3FS Storage

IBM Cloud Object Storage plugin



https://github.com/IBM/ibmcloud-object-storage-plugin

IBM Cloud
Kubernetes Service

Container Security & Isolation

- Isolated compute, networking, and storage
- Automatic encryption of secrets and volumes
- Customer managed keys using HSM backed IBM Key Protect
- Default LUKS encryption of /var/lib/docker
  - Every worker node in each cluster has a unique encryption key
- Store your images securely in your hosted private registry
- Vulnerability Advisor provides Docker image and running container scanning to detect vulnerabilities and configuration weaknesses
- Image signing by integrating with Docker Notary
- Image security deployment enforcement controls

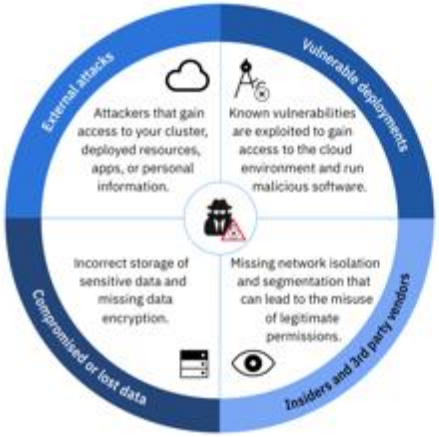
Secure from day one

- Secure master
- Secure worker nodes
- Secure network
- Secure storage
- Secure images
- Secure access

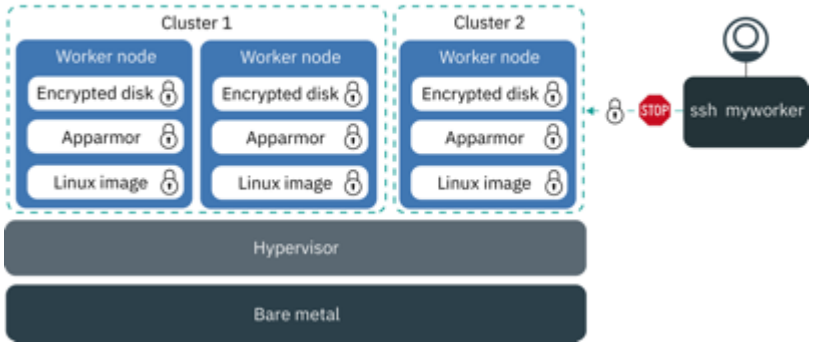
https://console.bluemix.net/docs/containers/cs_secure.html#security

Overview of security threats for your cluster

To protect your cluster from being compromised, you must understand potential security threats for your cluster and what you can do to reduce the exposure to vulnerabilities.



Worker node setup (VM on shared hardware)



Compliance

- SOC1
- SOC2
- ISAE 3402
- HIPAA

Image scanning and enforcement

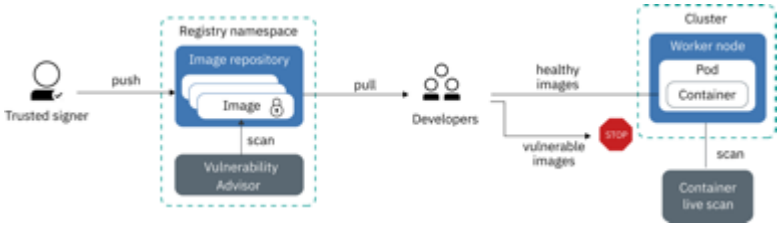
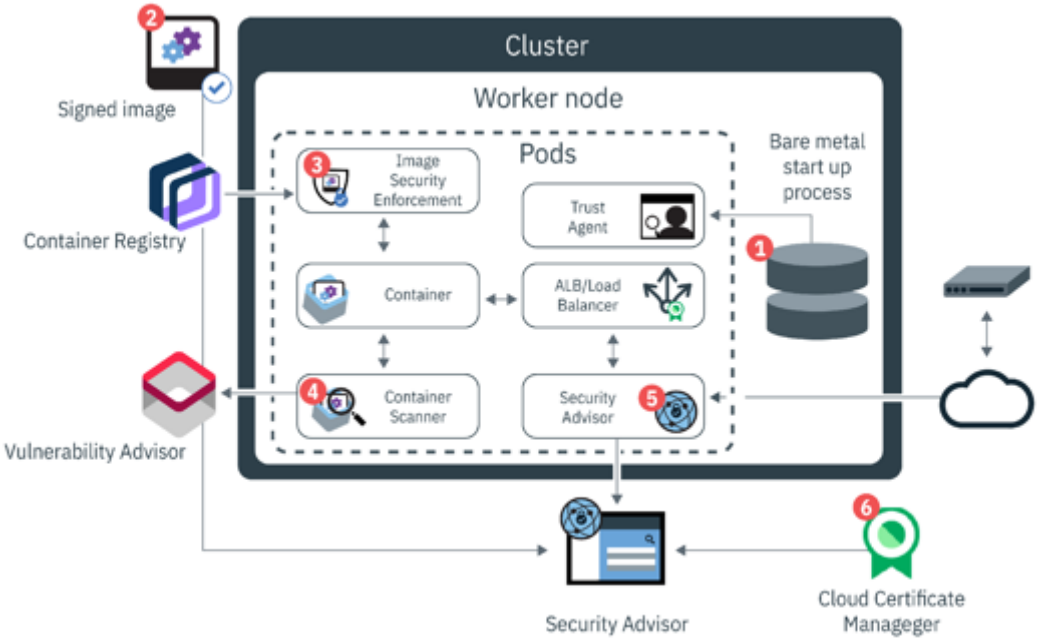


Image Security Enforcement in IBM Cloud Kubernetes Service

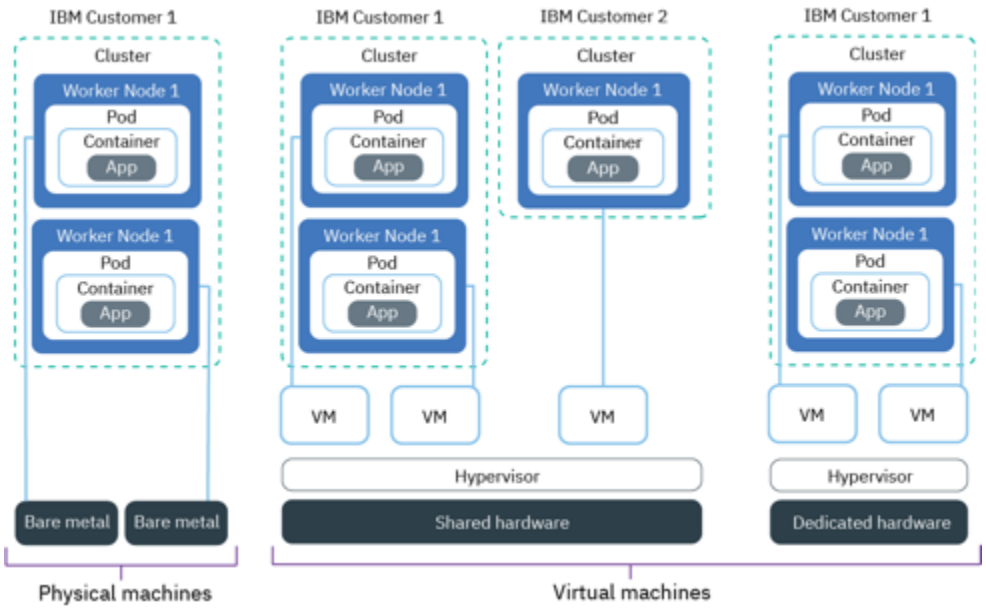
Control which images can be deployed in your Kubernetes clusters based on vulnerabilities and image signing

- Docker Notary for image signing
- Blocks vulnerable images from being deployed
- Blocks deployment of images with an unknown identity (missing signed keys)
- Ensures higher security of an IKS cluster by avoiding the running of potentially malicious code



Worker Node Isolation

- **Shared Compute**
  - Single-tenant virtual server instance, running on multi-tenant hypervisor and hardware
  - Lower cost
- **Dedicated Compute**
  - Single-tenant stack: virtual server instance, hypervisor, and hardware
  - Hardware isolated to account
- **Bare Metal**
  - Single-tenant physical server
  - No hypervisor
  - GPU option
  - Higher network throughput



- https://console.bluemix.net/docs/containers/cs_clusters.html#shared_dedicated_node

IBM Cloud
Kubernetes Service

Extend IBM Cloud Services

- Enhance your application with Watson, IoT, Analytics and Data Services
- Persistent volumes using IBM Cloud storage (file, block, object)
- IP and application Load Balancing
- Integrated with IBM Cloud identity and access management
- Control access and billing using Resource Groups

IBM Cloud
Kubernetes Service

Native Kubernetes Experience

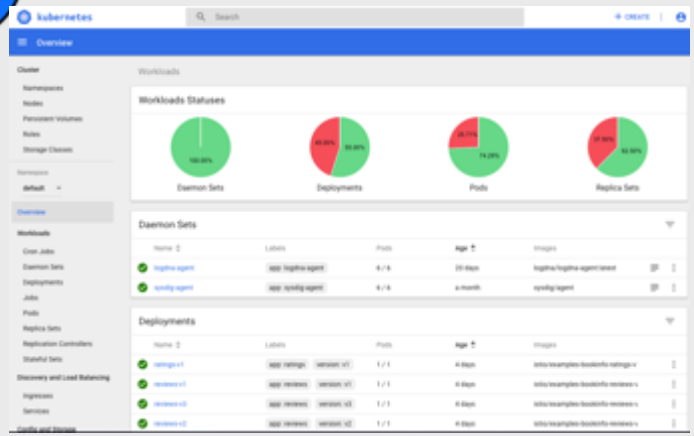
- Seamless experience moving from local development to IBM Cloud
- 100% Kubernetes API and tools
- Certified Kubernetes provider
- Conformance tested for Kubernetes 1.9, 1.10, 1.11
- Supports Kubernetes dashboard
- Leverage Docker images

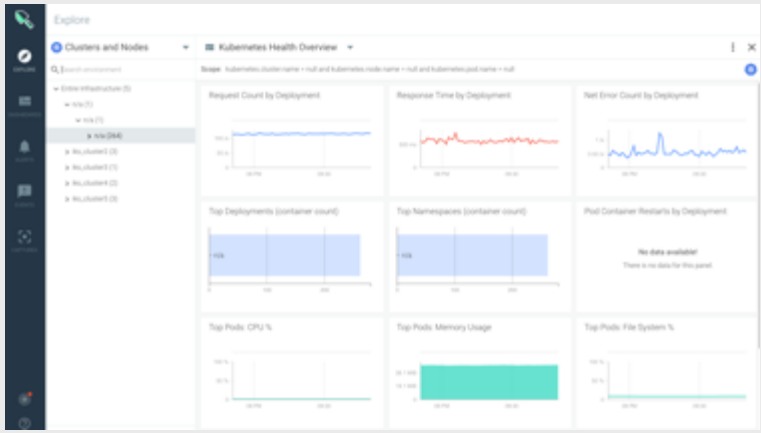
IBM Cloud
Kubernetes Service

Integrated Operational Tools

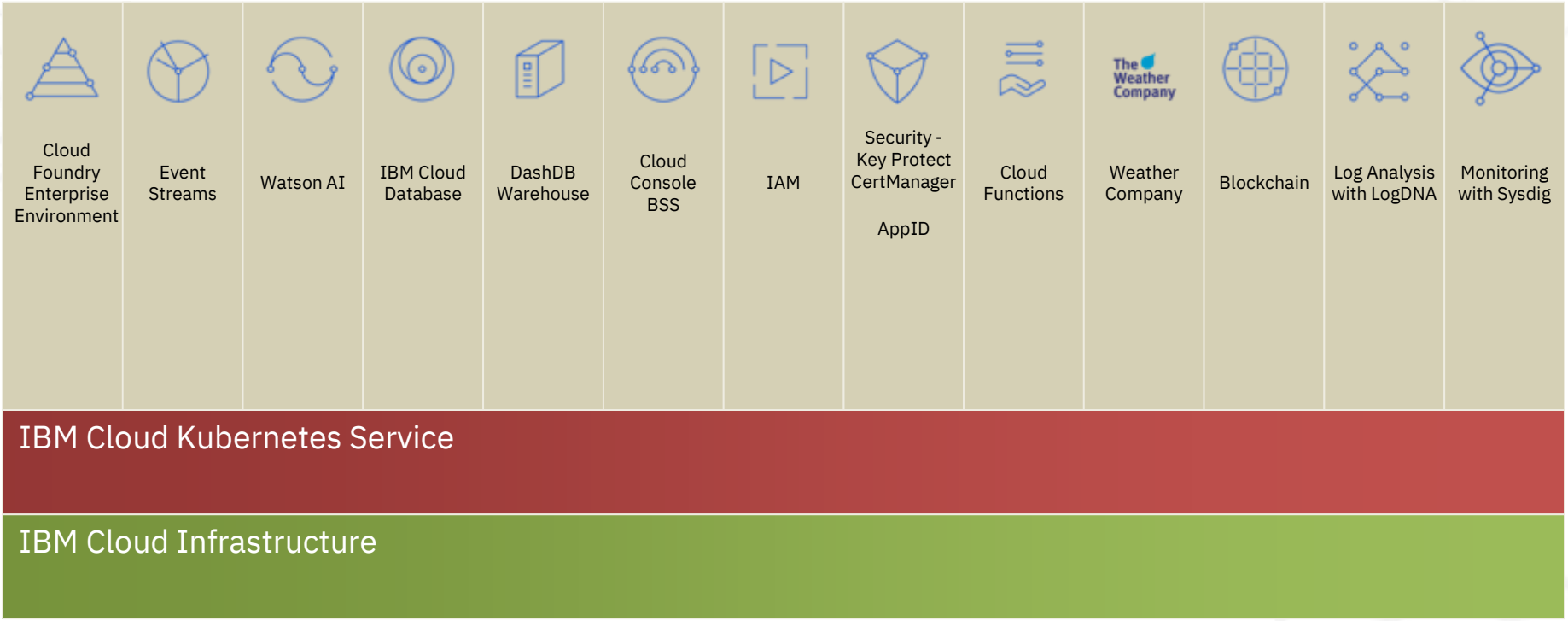
- Built-in log and metrics collection with IBM Cloud log and monitoring services
- Use with IBM DevOps tools such as Delivery Pipeline
- Supports popular add-ons including Prometheus, Weave, Sysdig, fluentd and others

Integrated Operational Tools





IBM Cloud Runs on Kubernetes for Massive Scale and Workload Diversity



Cloud Object Storage (COS)

Cloud Object Storage:
The foundation for data services

Scalability with virtually no limits for always-on availability

Easy to scale capacity or performance

Security built-in for trust and compliance

- Encrypted data with our keys or yours
- Identify Access Management
- Lockable WORM data

Simplicity of the cloud

- Industry standard API
- Access data concurrently from any location
- Always on-line

Savings up to 70%

- Low cost, flexible tier offerings
- Native high-speed file transfer (no charge for ingress)
- Cross Region all-inclusive pricing, no additional charges for multiple regions

Cost Effective

Flex tier offering for variable workloads with low pricing

Native built-in fast high-speed file transfer capabilities, with no charge ingress

Cross Region offering with all-inclusive pricing, no additional charges for multiple regions

Cloud Data Use Cases

Backup	Archive	NAS to Cloud	Migration
Content Management	Cloud Native	Modern Apps/ IoT/ SaaS	Analytics

Why Cloud Data Services

Secure resilient data storage destination for on prem to cloud and cloud native workloads

On-Premises

- Enterprise Data
- VMWare
- NAS/File Data

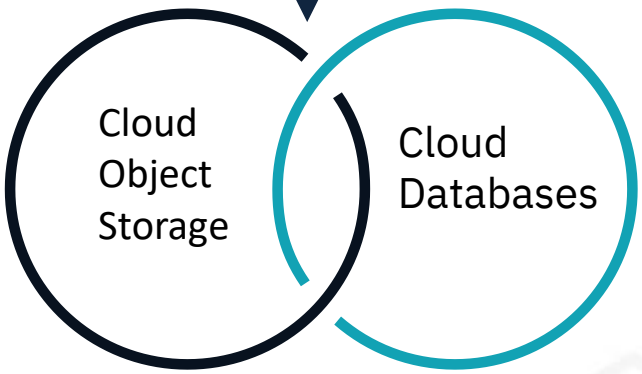
Store, access, backup, & archive your data

Apps & Runtimes

vmware SAP Kubernetes

Cloud Services

Analytics IoT Blockchain Watson



- Built on IBM Cloud Infrastructure
- Multi Zone Regions & Cross Region Options

Cloud Object Storage Data Flow

Query and Transform Your Data

w/SQL Query, Watson Skills

Migrate and access data in the cloud quickly

High-speed transfer

Archive your data for long-term data retention

Archive

Back up your data, runtimes, and workloads to resilient data storage

w/Backup Solution

IBM Cloud Object Storage

Lock your data for compliance

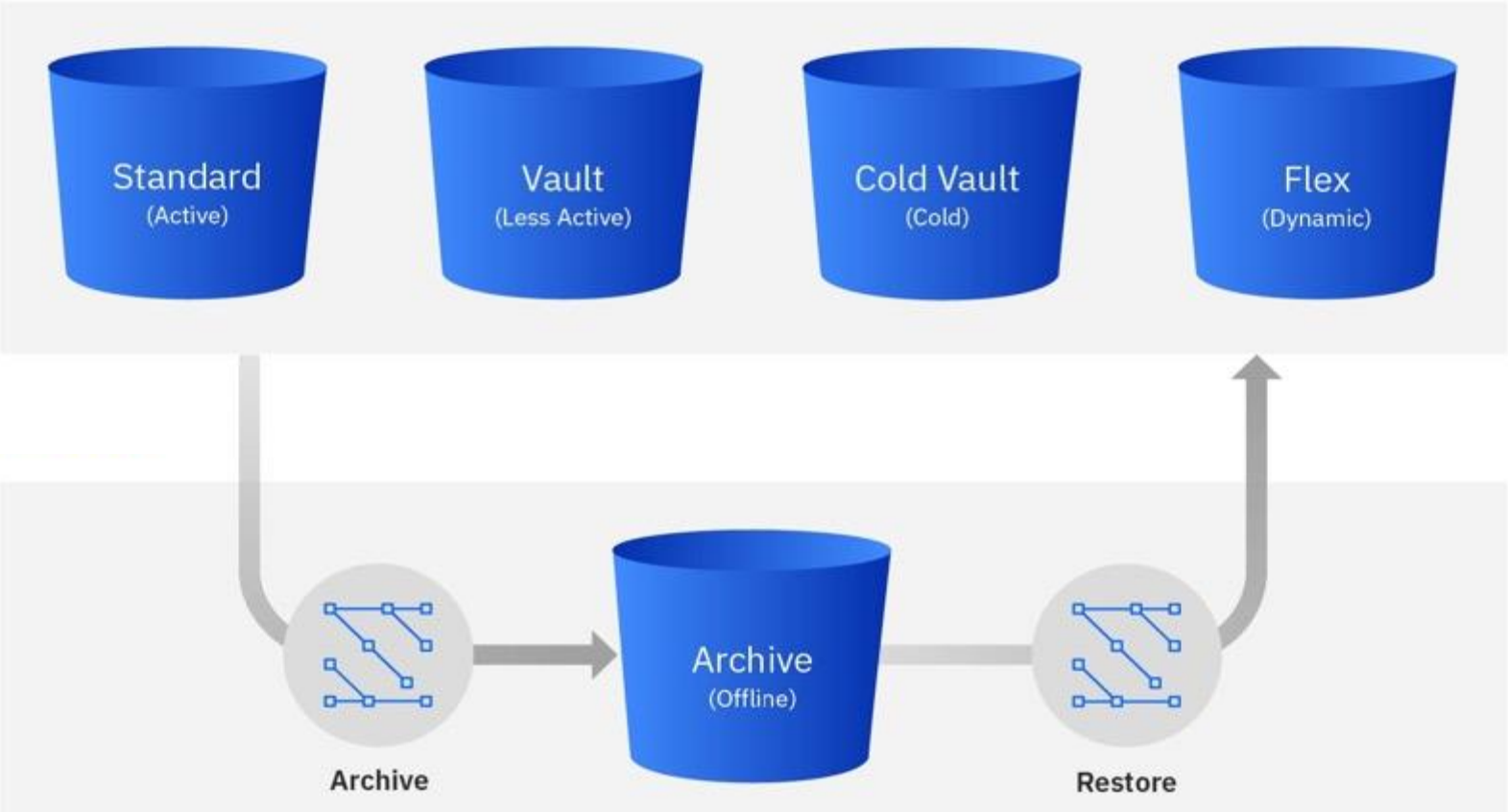
Immutable Storage

Flexible storage tiers

Predictable and consistent data access pattern

Unpredictable or variable data access pattern

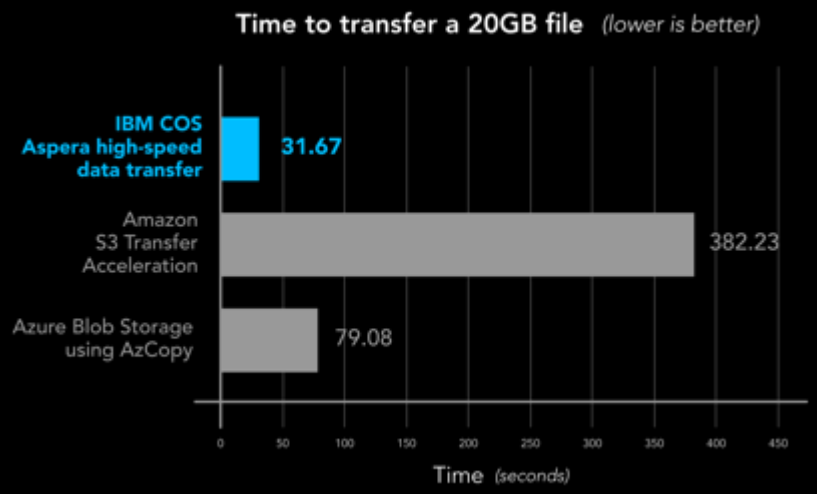
Low cost Archive for Long Term Data Retention



Cloud Object Storage: Aspera high-speed transfer

- No charge for data upload
- IBM SDKs for ease of use
- Ideal for large files and variable network connections
- Faster transfer speed than standard HTTP
- Security that starts at the point of transfer

Leading high speed data transfer performance -built in



- Performance testing conducted by third party - Principled Technologies
- Uploaded same 20GB file for all the offerings - distance US to India
- 12x faster than AWS S3 Transfer Acceleration
- 2.5x faster than Azure Blob storage using AzCopy

For detailed testing information, see the full PT report at http://facts.pt/docm5vh

Cloud Object Storage Data Management & Resiliency

Multi Zone Regions and Cross Regional worldwide locations

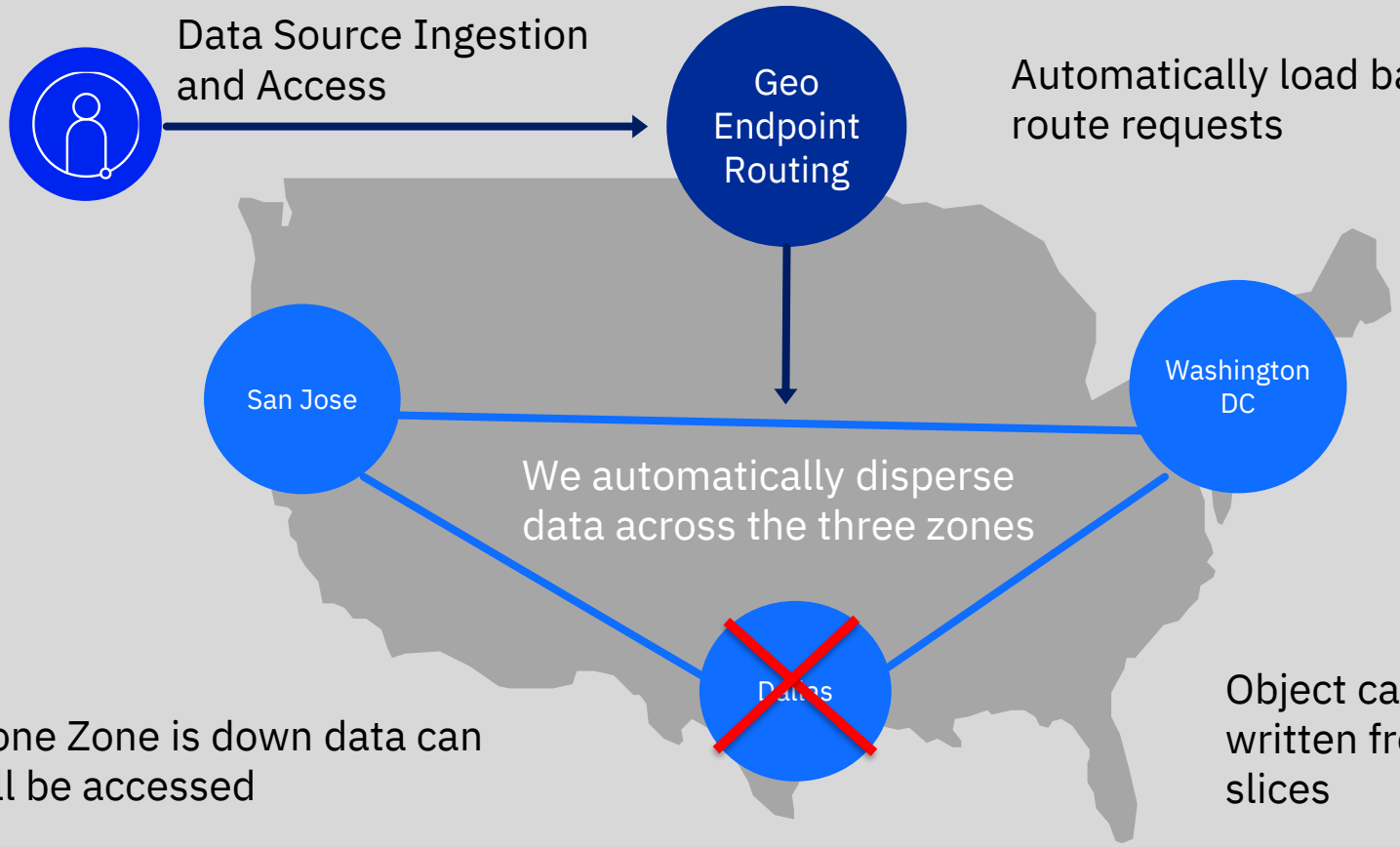
Storage flexibility with storage tiers and Archive

Designed to protect data and maintain availability

Redundant network paths and redundant system components

Security and control over your data with encryption options, policies and permissions

Cross Region Resiliency

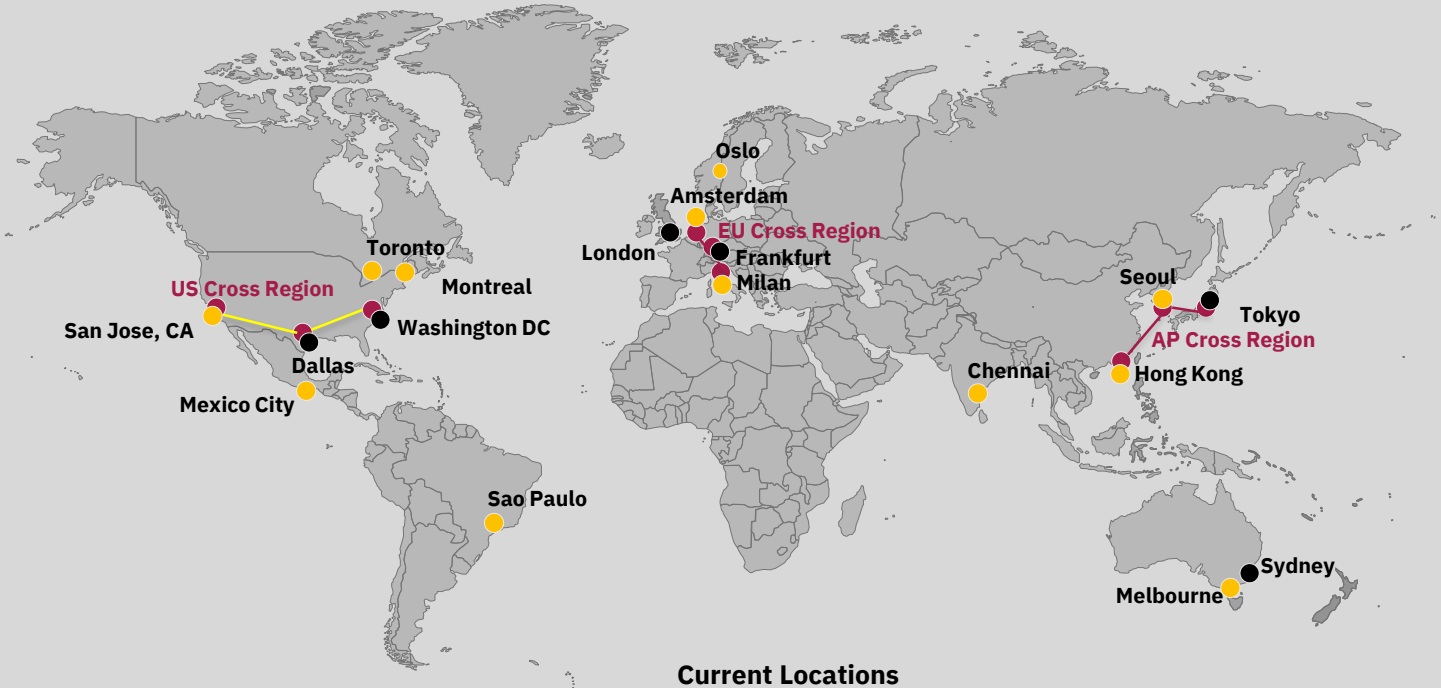


If one Zone is down data can still be accessed

Object can be read and written from a subset of slices

IBM Cloud Object Storage spanning the globe with coverage

- **Cross Region:** Your data is stored across three regions within a geography for highest availability and resiliency.
- **Regional:** Your data is stored in multiple data center facilities within a single geographic region for best availability and performance.
- **Single Data Center:** Your data is stored across multiple devices in a single data center for when data locality matters most.



Current Locations

- **Cross Region:** United States - (Dallas, Washington DC, San Jose). Europe - (Amsterdam, Frankfurt, Milan). Asia Pacific - (Hong Kong, Tokyo, Seoul).
- **Regional:** U.S. East (Washington D.C), U.S. South (Dallas) EU GB (London) , EU DE (Frankfurt), JP-Tokyo, **Sydney, Australia**
- **Single Data Center Offerings:** Toronto, Melbourne, Chennai, Amsterdam, Sao Paulo, Oslo, Seoul, Montreal, **Mexico City, San Jose, Milan, Hong Kong**
- **Federal**: Washington, D.C., Dallas

**** New 2019 locations highlighted ****

IBM Cloud Object Storage spanning the globe with coverage (Archive)

Archive: Archive is our lowest-cost option for data that is rarely accessed. Archive works with our existing storage-class tiers (Standard, Vault, Cold Vault, Flex), enabling you to reduce storage costs even further by storing data offline with our lowest-priced storage.

Archive Pricing:

Archive tier (for Cold data/long-term retention)
Storage/Restore: $0.002/$0.02
Latency: < 12 hours
Minimum storage duration: 180 days

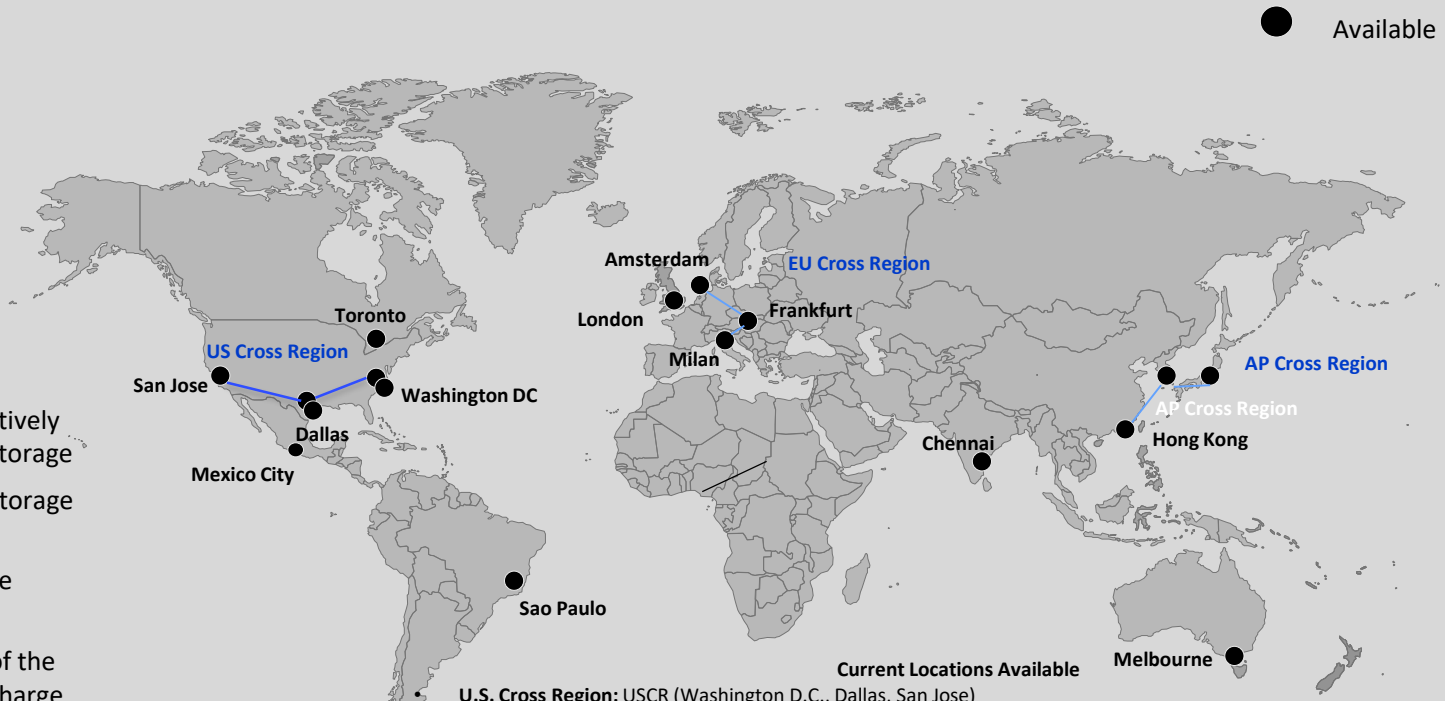
Archive Current Locations

- **Regional:** U.S. East (Washington DC), US South (Dallas) EU Great Britain (London), EU Germany (Frankfurt), Asia Pacific: (Tokyo, Japan), Sydney, Australia.

IBM Cloud Object Storage spanning the globe with coverage (Aspera)

Aspera: Fastest, easiest way to upload data into the cloud with Cloud Object Storage Aspera high-speed transfer. Aspera is natively integrated into COS. Data upload is included as part of the COS service at no additional charge.

- Aspera high-speed transfer natively integrated into Cloud Object Storage
- Integrated into Cloud Object Storage UI portal for ease of use
- Ideal for large files and variable network connections
- Data upload included as part of the COS service, at no additional charge
- Faster transfer speed than standard HTTP
- Active transfer continues even when the browser is closed
- Security that starts at the point of transfer
- SDK Available for Java and Python



Current Locations Available

- **U.S. Cross Region:** USCR (Washington D.C., Dallas, San Jose)
- **U.S. Regional:** U.S. South (Dallas) and U.S. East (Washington D.C)
- **AP Regional:** Japan
- **AP Cross Regional** (Tokyo, Seoul, Hong Kong)
- **EU Cross Regional:** EUCR (Amsterdam, Frankfurt, and Milan)
- **EU Regional:** EU Great Britain (London) and EU Germany (Frankfurt)
- **AU Regional**: Sydney
- **Single Data Center:** (Melbourne, Australia) (Toronto, Canada) (Chennai, India) (Amsterdam, Netherlands), (Sao Paulo, Brazil), (Oslo, Norway), (Seoul, South Korea), (Montreal, Québec), (Mexico City, Mexico), (Milan, Italy), (San Jose, USA), (Hong Kong, China)

IBM Cloud Object Storage spanning the globe with coverage (Key Protect)

Key Protect: Allows Customers to have their own managed encryption keys for higher level data security.

- SSE-C - Customer Keys via IBM Key Protect IBM's Key Management Service
- Data isolation using encryption keys controlled and managed by the customer
- COS Advanced Encryption Settings – Allow buckets to be encrypted using Key Protect with Key Management.
- Support for both customer bring your own key (BYOK) and Key Protect generated Customer Root Keys (CRKs).
- Easy to manage encryption keys and policies for applications to leverage Object-level encryption

Current Locations

- **U.S. Regional:** U.S. South (Dallas) and U.S. East (Washington D.C.)
- **EU Regional:** EU Great Britain (London) and EU Germany (Frankfurt)
- **AP Regional:** Tokyo, Japan
- **Australia:** Sydney

Immutable Object Storage (WORM) Availability: Regional MZR's

WORM: IBM Cloud **Immutable Object Storage** allows client(s) to preserve electronic records for long-term and maintain data integrity in a WORM (Write-Once-Read-Many), non-erasable and non-rewritable manner.

Feature Overview:

- Objects written to a COS bucket with retention policy can have an assigned retention period during ingest, or inherit the default retention period of the COS bucket if no retention period is specified.
- Individual object within a COS bucket with retention policy can have Legal Hold(s) - preventing object from being deleted or overwritten (even after retention period expires).
- Objects can only be deleted after expiration of retention period AND removal/deletion of all legal hold(s) on the object.
- Buckets with retention policy can only be deleted after all objects are deleted.

This feature will help client(s) in the data storage and preservation requirement(s) generally part of industry regulations including:

- Securities and Exchange Commission (**SEC**) rule 17a-4(f)
- Financial Industry Regulatory Authority (**FINRA**) Rule 4511, which references SEC Rule 17a-4(f)
- Commodity Futures Trading Commission (**CFTC**) Rule 1.31(b)-(c)

Immutable Storage Locations (WORM)

Regional: U.S. East (Washington D.C), U.S. South (Dallas), EU Great Britain (London), EU Germany (Frankfurt), AP Japan (Tokyo), Sydney, Australia

Note: Key Protect and Aspera not supported with WORM in Regional MZR's.

Encryption

Leverage IBM Cloud Object Storage encryption options to meet your security requirements

SSE- Provider Managed

- SSE- Provider Managed for Data at Rest
- Default automatic encryption for data stored in IBM COS
- Automatically encrypts objects stored in IBM COS for data at rest security
- IBM COS service encrypts each object using per-object segment uniquely generated encryption key
- Keys are secured and reliably stored using Information Dispersal Algorithm (IDA) that protects object data using an All-or-Nothing Transform (AONT) method

SSE-C

- SSE-C - Support for Customer Keys via API
- This feature adds API headers to the existing storage API that give customers the ability to provide their own keys to encrypt objects in IBM Cloud
- Enables customers to retain complete control of keys used for data encryption
- Supports non cloud key management, some security conscious customers require a product that can integrate with their on-premise key management solution

SSE-KMS

- SSE-C - Customer Keys via IBM Key Protect (IBM's Key Management Service)
- Data isolation using encryption keys controlled and managed by the customer
- IBM COS Advanced Encryption Settings – Allow buckets to be encrypted using Key Protect with Key Management
- Support for both customer bring your own key (BYOK) and Key Protect generated Customer Root Keys (CRKs).
- Easy to manage encryption keys and policies for applications to leverage Object-level encryption

Services Ecosystem for New AI and Cloud Native Workloads

Data Scientists & Analysts

- KUBERNETES SERVICE
- POWERAI
- MACHINE LEARNING
- KNOWLEDGE CATALOG
- AI OPENSCALE
- SQL QUERY
- APACHE SPARK
- ANALYTICS ENGINE
- FUNCTIONS
- EVENT STREAMS
- STREAMING ANALYTICS

Backup

- CLOUDANT
- DB2
- DB2 WAREHOUSE
- POSTGRES
- MYSQL
- MONGODB
- REDIS
- ELASTICSEARCH
- RABBITMQ
- ETCD
- RETHINKDB
- JANUSGRAPH
- SCYLLADB

IBM Cloud Object Storage

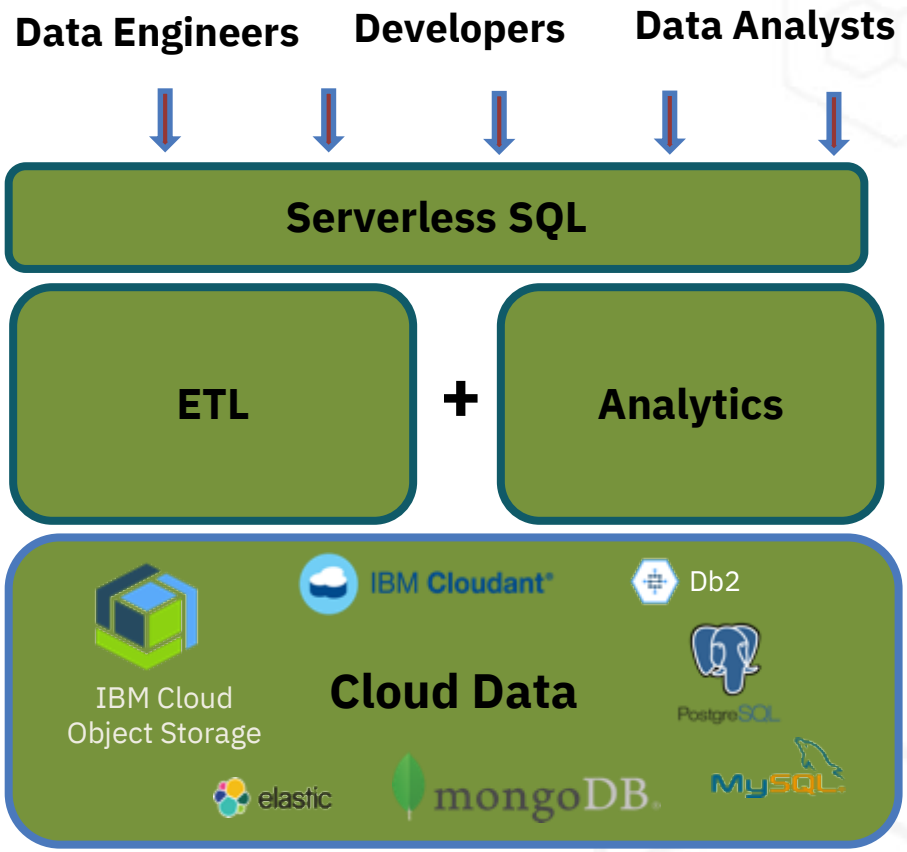
- ACTIVITY TRACKER
- KEY PROTECT
- Cloud IAM

Solutions

- SECURITY ADVISOR
- SPECTRUM PROTECT PLUS ON IBM CLOUD
- BOX
- BLOCKCHAIN
- CONTAINER REGISTRY
- INTERNET OF THINGS PLATFORM

Query data directly in Object Storage With IBM Cloud SQL Query

- Quickly submit and run SQL queries directly to Cloud Object Storage
- No setup required
- Query data where it resides
- Write results back to Cloud Object Storage
- Leverage Cloud Object Storage permissions and policies to securely access your data

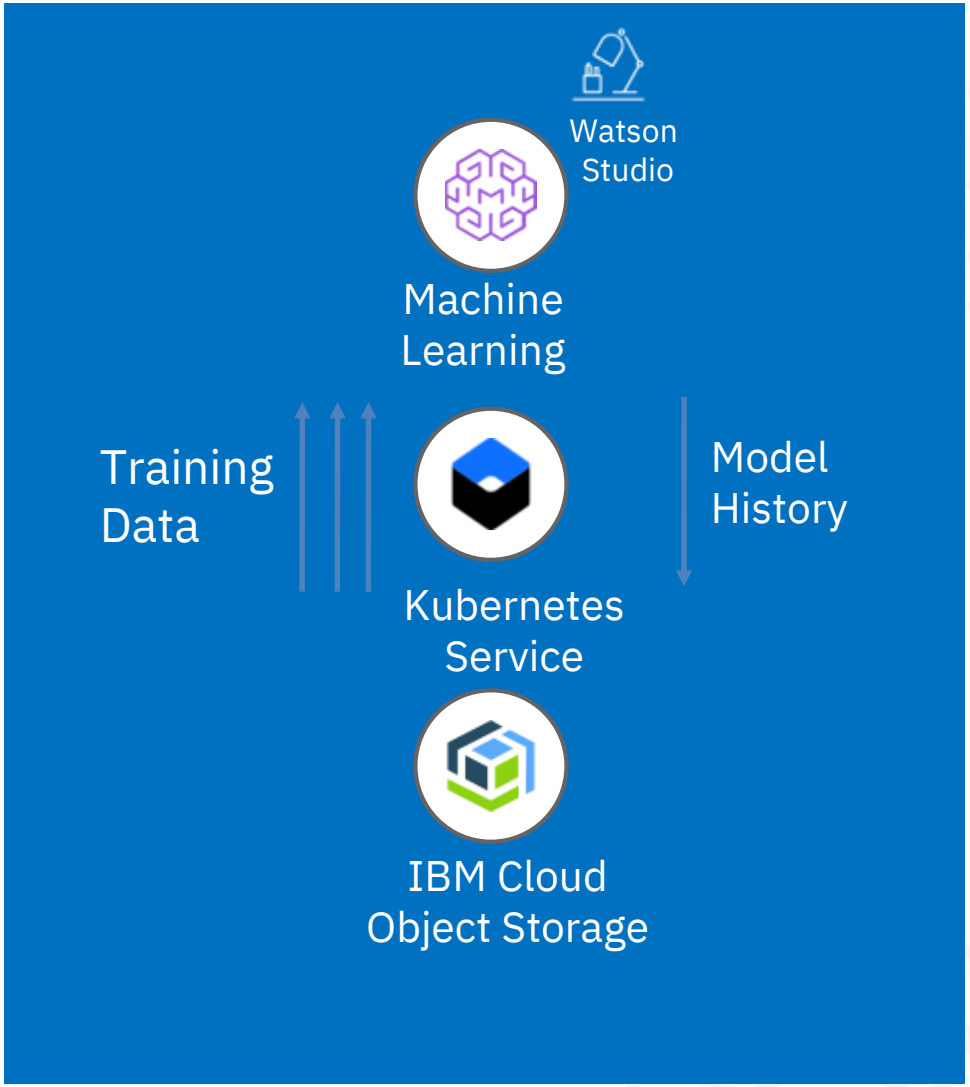


Apply advanced AI

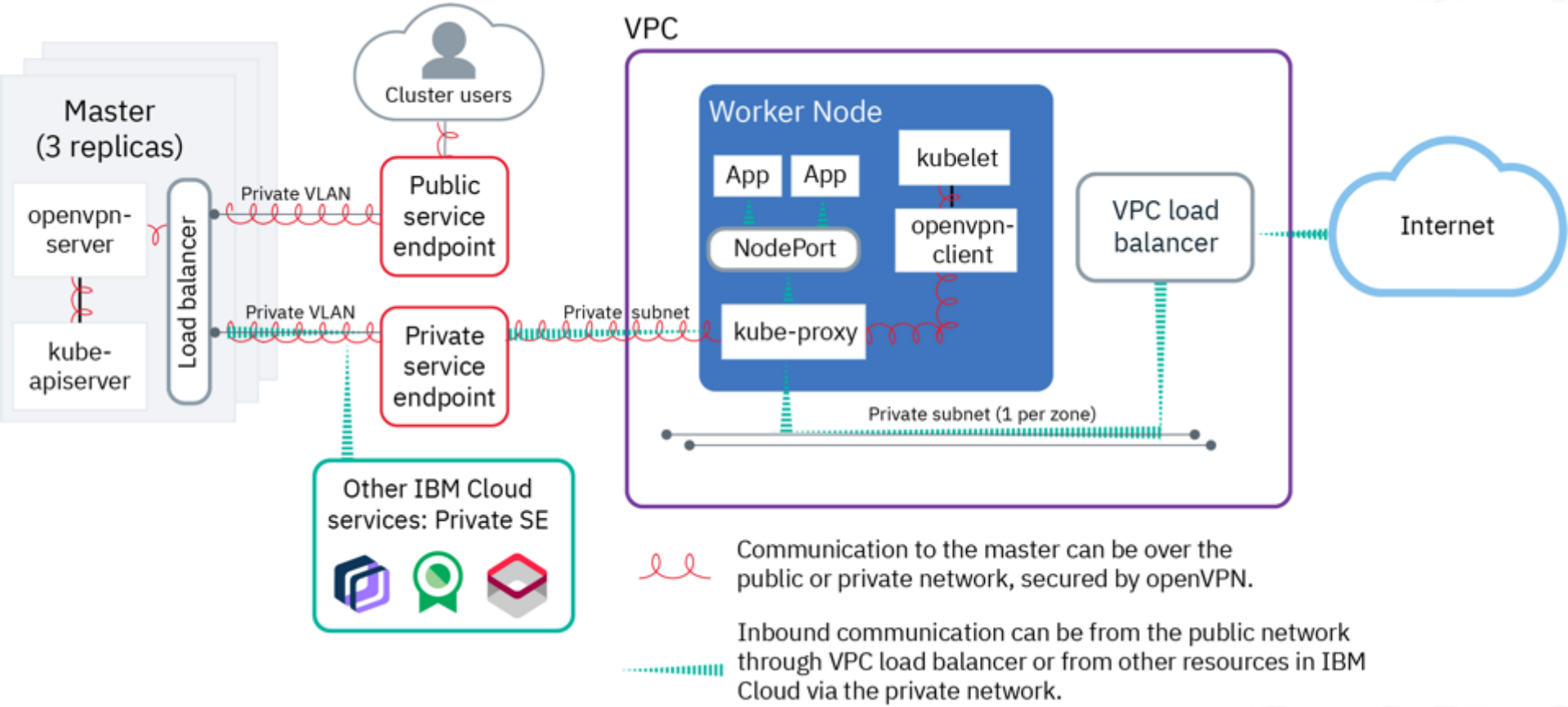
Cloud Object Storage

Directly learn from data in Cloud Object Storage

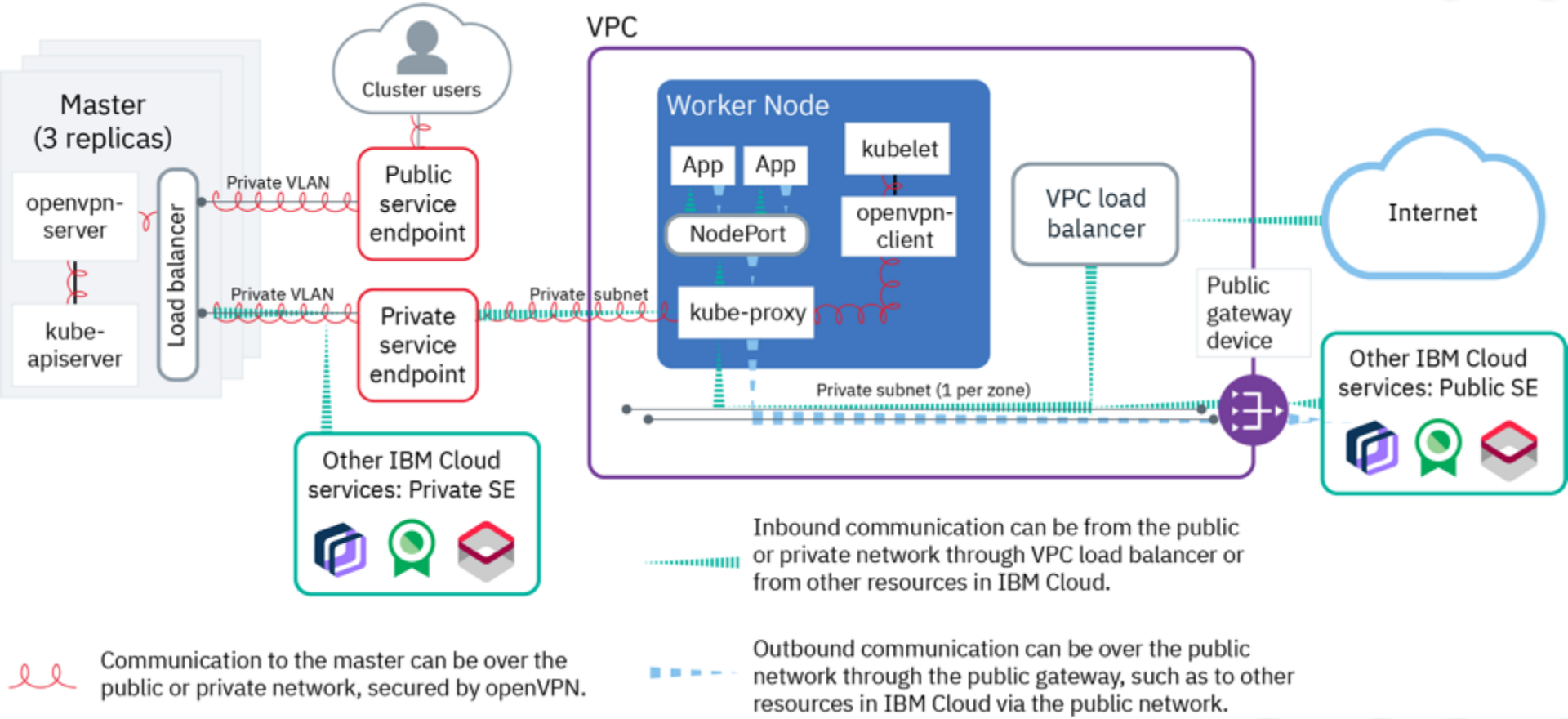
- No need to pre-copy the data!
- IBM optimized integration with Kubernetes support



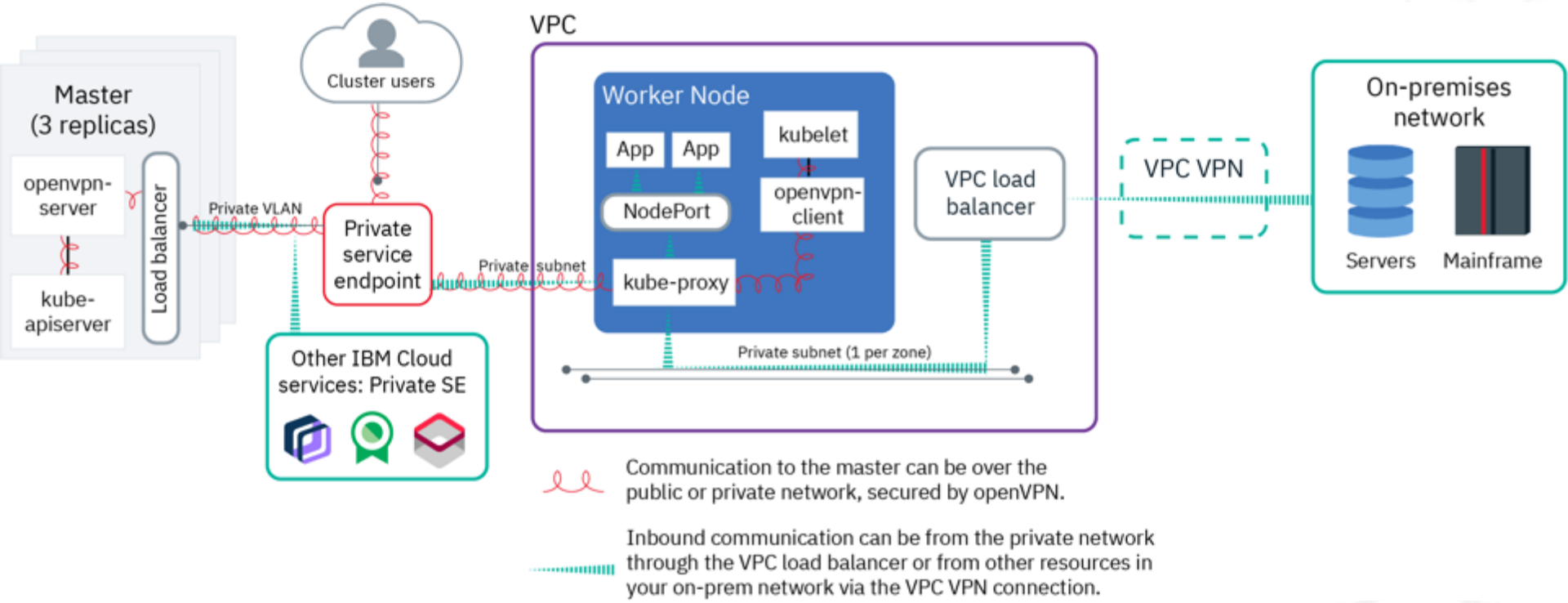
Scenarios: VPC cluster network setups with IKS



Scenario: Run internet-facing app workloads in a VPC cluster with limited public egress



Scenario: Extend your on-premises data center to a VPC cluster



2019 IBM Cloud
用戶實作課程 秋季班

THANK YOU