



2019 IBM Cloud

用戶實作課程 冬季班





2019 IBM Cloud
用戶實作課程 冬季班

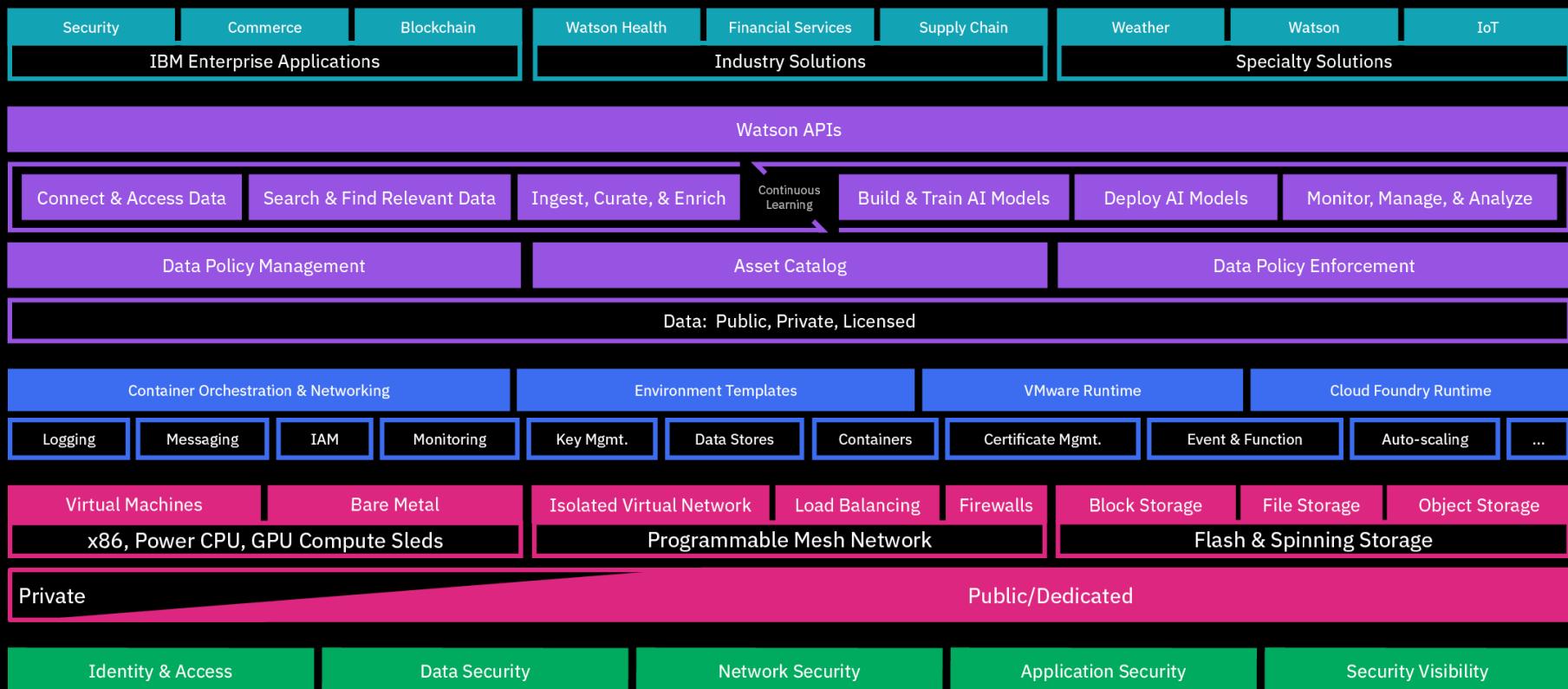
IBM Cloud 服務介紹

IBM Cloud Unit

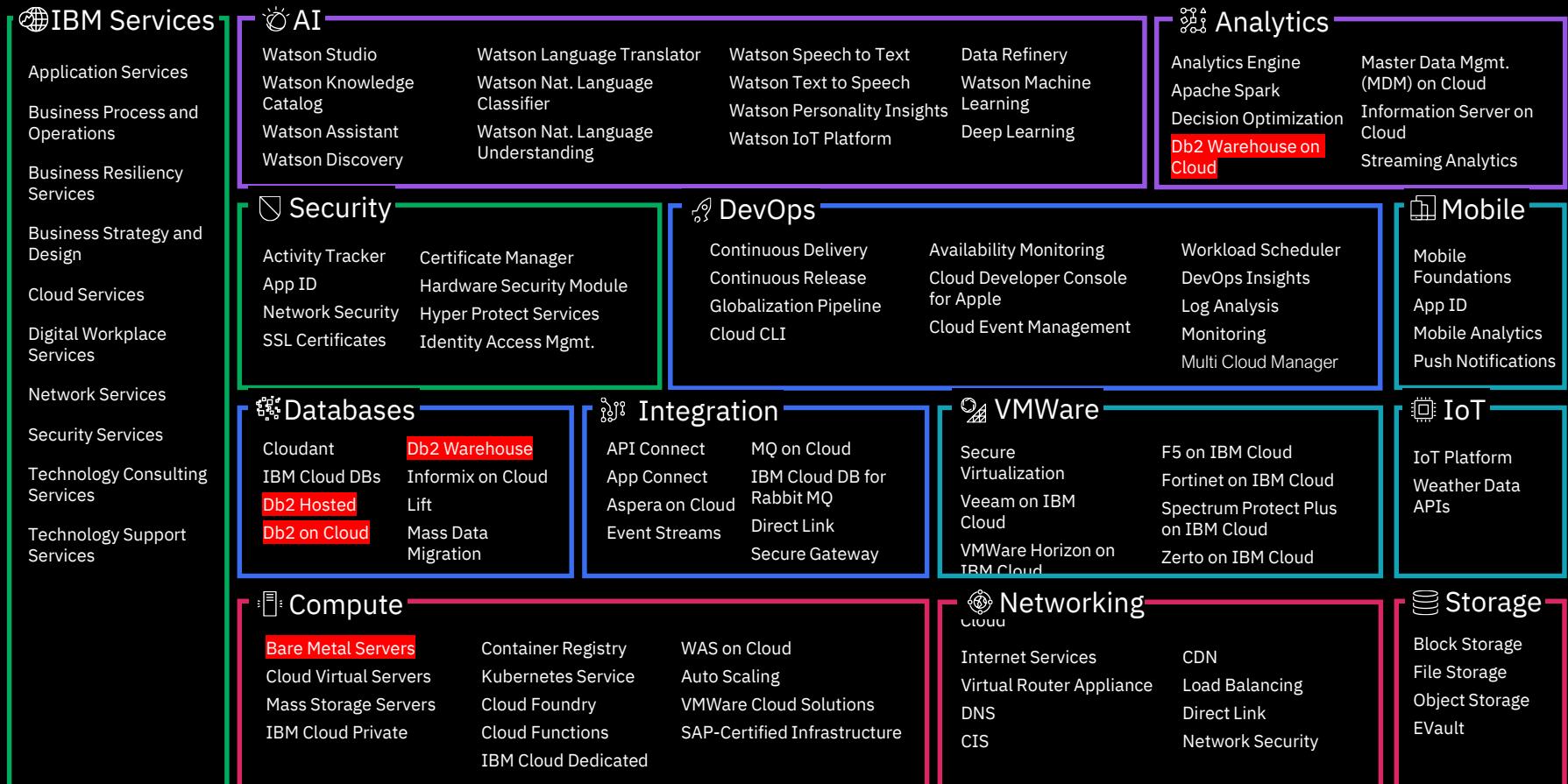
雲端專家

馮建國 (Gordon Fung)

IBM Cloud One Architecture



IBM Cloud – full stack platform for cloud-native apps



IBM Cloud Infrastructure

Designed for your data.

AI ready.

Secure to the core.

IBM Cloud is the cloud for business.



A cloud infrastructure that meets you where you are and takes you where you want to go

Customized



Best-in-class, powerful compute, storage, & network infrastructure for any workload and any budget size — from born-on-cloud to Fortune 500 enterprises

Open



First to build on a foundation of open source (Kubernetes, OpenWhisk, Cloud Foundry), paving the way for others

Trusted



Expertise in over 20 industries, standardized approach for auditable consistency, and global and regulated industry compliance

Visionary



First to see and build for future-proofing with Watson — the oldest AI at 7-years-old — blockchain, and a single architecture platform

Data Centers: Globally local

Built with multiple deployment options for your unique workload needs

Choose where to deploy from nearly 60 locations in 19 countries

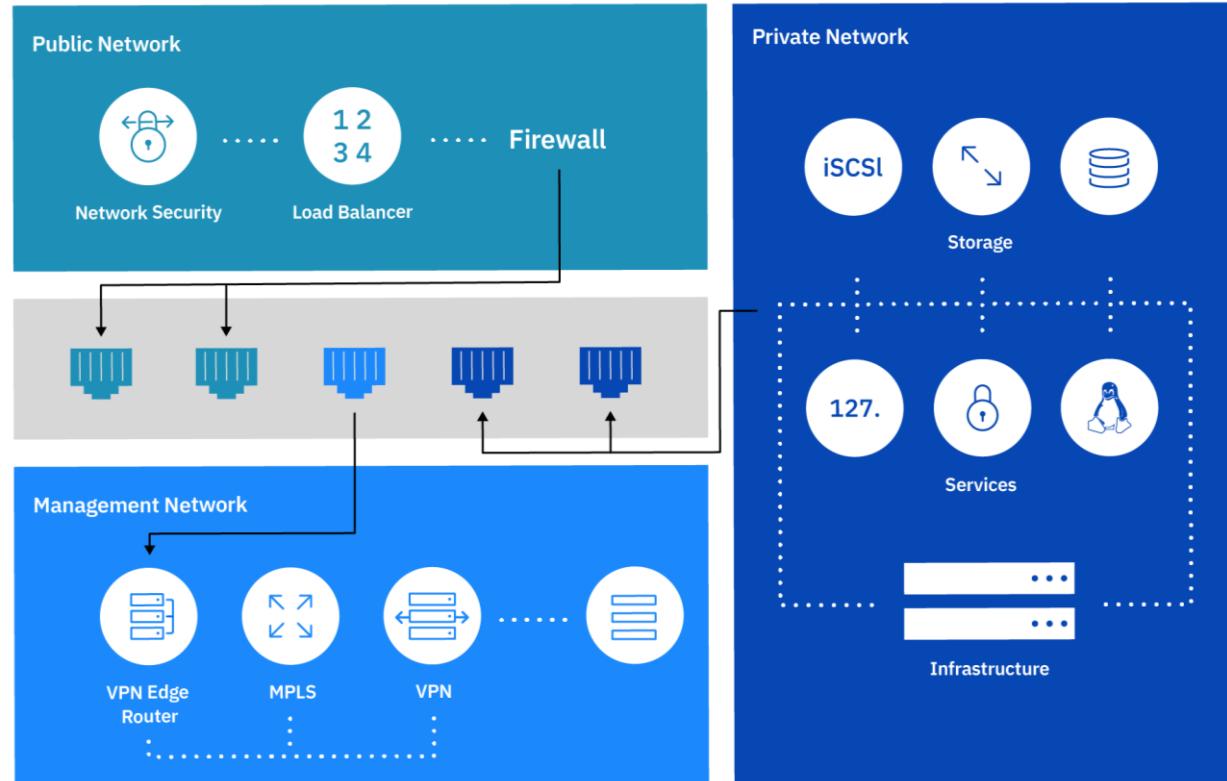


“The ability to access IBM’s global network of cloud data centers, which are all connected by a high-speed fiber network, is extremely attractive to us.”
-Rob Platzer, chief technology officer, *Bitly*

Unique, triple-layer network architecture

Public, private, and management traffic travel on separate networks, giving you unmatched control, security, and speed.

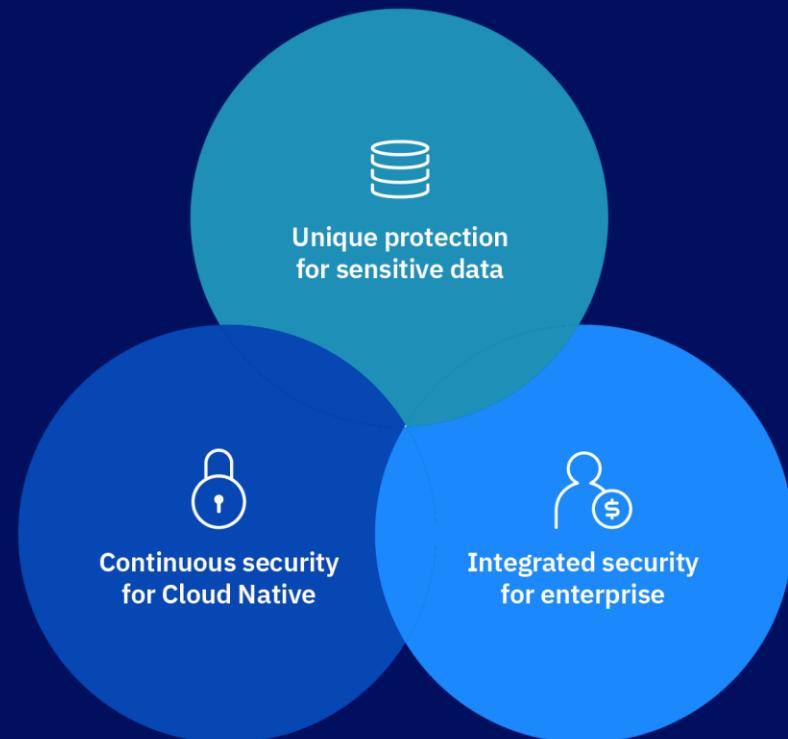
The private network connects your services in all data centers, free of charge.



End to end security for cloud native and enterprise workloads

Secure to the core: **Technology**

- Comprehensive cloud security offering portfolio
- API ready services for cloud integration



End to end security for cloud native and enterprise workloads

Secure to the core: **Expertise**

- Deep security and regulatory compliance expertise
- Managed services for security operations and intelligence



Infrastructure-as-a-Service Highlights

Smart partnerships for a better cloud



VMware, SAP, and Intel power cloud for the custom workloads your business needs

Built for security



High assurance, enterprise-strong cloud security portfolio and expertise to help you adopt IBM Cloud with confidence

Fast provisioning



Spin up bare metal or virtual servers in 30 minutes or less, with network offerings that provide consistent, cutting edge computing speeds

Power and performance



13 Tbps connectivity on a low latency, high resiliency global network with powerful bare metal and VM compute performance

Compute

A high performing cloud starts with a strong compute foundation

Customize to suit your workloads



Pre-configuration to fully customizable server options

Choose a server type



Compute options from high-abstraction to high-control

Provision on demand



Deploy an IaaS bare metal or virtual server in minutes and customize bare metal in 2–4 hours

Compute Infrastructure

SAP Certified Servers



Build, deliver, and run SAP applications in the cloud

Bare Metal Servers



Raw IaaS horsepower for processor-intensive and disk I/O-intensive workloads

Virtual Servers



Fast deployment when resources are needed on the fly

GPU Computing



Handle complex, compute-intensive workloads, including analytics, graphics, and AI

POWER Servers



Develop, test, and run Linux applications

Server Software



Operating systems to control panels to simplify IaaS administration

Bare Metal Servers

Bare Metal Servers

Real challenges and real solutions

High-performance computing

Solve problems faster

Secure data

Match data security needs – previously available with on-premise servers only

High volume data

Gather and store, analyze data, and gain insights to make better business moves

AI

65% more machine learning with latest GPUs to find new value in your data

Bare Metal Servers Family Benefits

Powerful, Accessible Data & Analytics



Use Bare Metal servers for high performance data and analytics workloads

Choice with Consistency



Bare Metal servers are available in all data centers

DevOps Productivity



Use Bare Metal servers for high performance needs in production environments

Hybrid Integration



Customize Bare Metal to look exactly like your on premise solution or add to it

Cognitive Solutions



Use Bare Metal servers for high performance Cognitive solutions

Bare Metal Servers

The power you demand for your processor — and disk I/O-intensive workloads

- **Performance:**

Eliminates multi-tenant resource conflicts with competing work streams

- **Control:**

Complete control of physical hardware

Power from the ground up — dedicated to you.

- **Solve problems faster**

- Powerful
- On-demand
- Customizable



Bare Metal Processor Options

Single Socket

Ideal for:

Entry-level web hosting
Development sandbox
Simple email servers

Dual Socket

Ideal for:

Hosting resellers
Moderately-sized websites
SMB back office apps

Quad Socket

Ideal for:

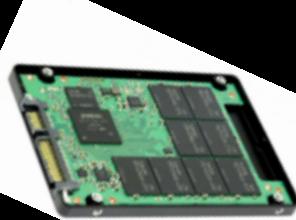
High transaction apps
Virtualization
Disaster recovery

Octo Socket

Ideal for:

Everything quad socket servers offer plus in-memory computing with large database applications. *Only available with SAP offering.*

Bare Metal Hard Drive Options



SSD SED

- High performance, low latency, enterprise-class storage
- Drive capacities up to 3.8TB
- Ideal for high-performance and data-intensive applications

SAS

- Includes 3.0Gb/s interface with 16MB cache and 15K RPM rotation speeds
- High performance speed and reliability
- Ideal for gaming, database, streaming media, and mission-critical servers

SATA

- Each unit includes up to 6.0Gb/s interface with 64MB cache (SATA III)
- Drive capacity ranges 1TB to 10TB
- Each unit includes up to 6.0Gb/s interface with 64MB cache (SATA III)
- Ideal for web, mail, or high-capacity storage servers

3D XPoint™ Technology

- High performance cell and array architecture that can switch states 1000x faster than NAND
- 10x denser than conventional memory
- Storage and memory converged

SAP Certified Servers for HANA and Applications

| SAP Certified HANA servers | SAP Certified NetWeaver servers | Other Components |
|---|---------------------------------------|---|
| 8 Socket 8890v4 4, 8, 12* TB RAM | 4 Socket 8890v4 1 TB RAM | 1 Socket 1270v6 32, 64 GB RAM |
| 4 Socket 8890v4 1, 2, 4, 6* TB RAM | 2 Socket 6140 192, 384, 768 GB RAM | 1 Socket 1270v6 32, 64 GB RAM |
| 2 Socket 6140 192, 384, 768 GB RAM | 2 Socket 2690v4 512 GB RAM | SUSE SLES 12 SP2 RHEL 6.x or 7.x Windows Server |
| SUSE SLES 12 SP2 RHEL 6.7, 7.4 for HANA VMware 6.0, 6.5 | 2 Socket 2690v3 128, 256 GB RAM | DB2, MSSQL VMware 6.0, 6.5 |
| | | Network Gateways HW or SW options |
| | | Firewalls HW or SW options |
| | | Backup Veeam, Object Storage, Endurance Storage |
| | | Virtual Servers BOBJ, AD, Jump, Dev/Test |

Virtual Servers

Virtual Servers

Real challenges and real solutions

Dynamic Workloads

Not all workloads are the same—some require different resources

- Small, medium, large sizes
- Various isolation types
- Data stored where you need

Flexibility

Allows for dynamic resizing depending on data

- Fast provisioning times
- Hourly or monthly models

Predictability

High and predictable performance

- No oversubscription of vCPU or RAM
- Guaranteed 2.0 GHz or faster

Virtual Servers Family Benefits

Ease of use



Improved selection process from a broader spectrum of public virtual server flavors

Lower provisioning times



Pre-configured virtual servers based on workloads to easily select a best fit

More control and visibility



Single tenant virtual server offerings allow clients in heavily regulated industries overcome cloud adoption barriers

Cost savings



Servers dedicated to specific workloads to minimize under- or over-utilized resources

Virtual Servers

Real challenges and real solutions

Virtual servers give you the ability to change your cloud environment as fast as business moves.

- **Choice:**

Single-tenant eliminates resource conflicts. Hourly and monthly options for short-term and long-term applications.

- **On-demand:**

Provision virtual servers in minutes to combat workload spikes.

- **Performance:**

2.0Ghz or faster with no oversubscription on core or RAM.

Quickly deploy and scale cloud infrastructure on demand

- Flexible
- On-demand
- Powerful



Virtual Servers

Virtual servers give you fast access to compute resources to meet any workload

Public

Multi-tenant offering with rapid provisioning and scalability

Dedicated Instance

Single tenant offering with rapid provisioning, allowing further control and flexibility in virtual server deployments

Dedicated Host

Virtual servers dedicated to customers providing the most control by enabling workload placement and flexibility in virtual server deployments

Virtual Server Families and Applications

Balanced



Common cloud workloads requiring a balance of vCPU and RAM

Compute



Front end, batch-processing workloads, requiring more compute than memory

Memory



Caching, in-memory, database solutions, requiring more memory than compute

Balanced Local



Common cloud workloads requiring a balance of vCPU and RAM along with local storage (SSD and HDD options) and performance

GPU Computing

GPU Computing

Real challenges and real solutions

AI



Add GPUs to enable up to 65% more machine learning than traditional servers*

Big Data



Take on massive data analytics computations

GFX Applications

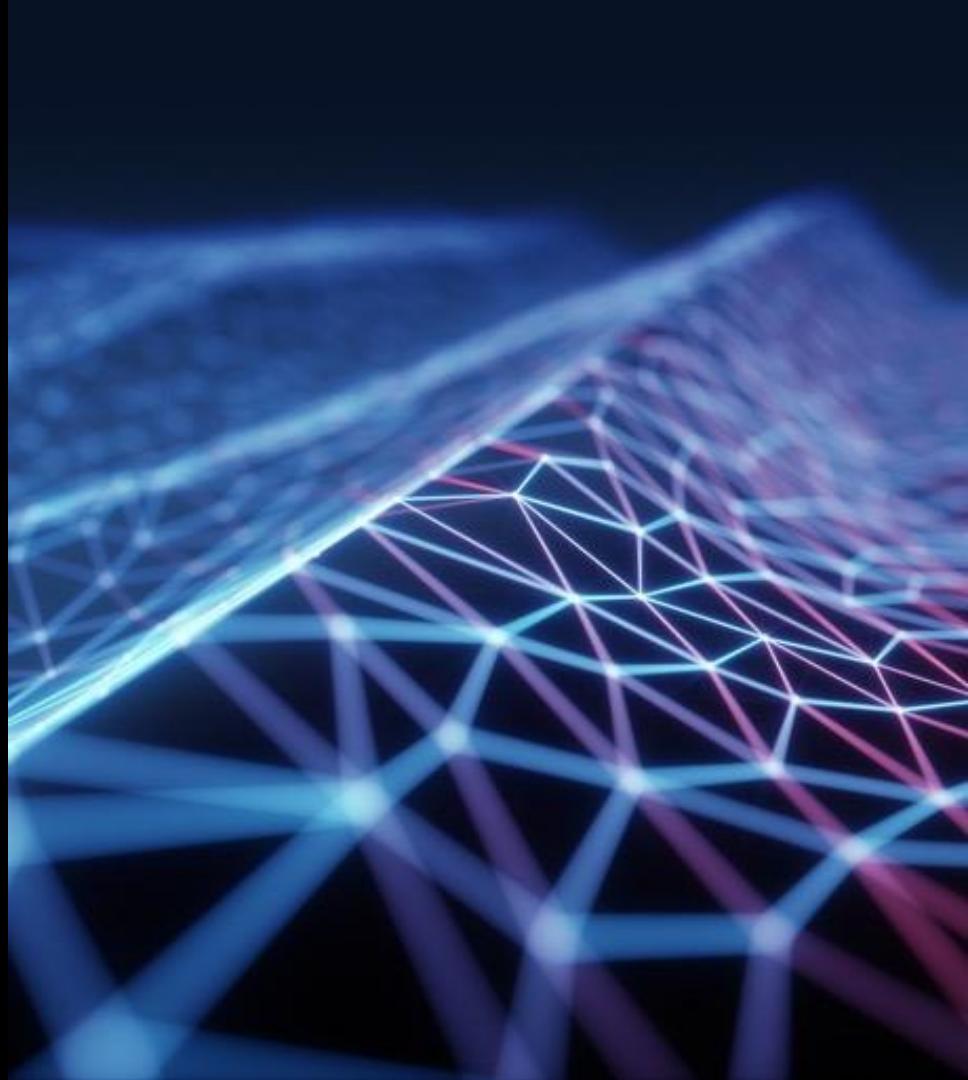


Get blazing speeds for graphic-intensive workloads like 3D CADs and data rendering for gaming

GPU Computing Benefits

The processing power for high performance computing, deep learning, machine learning, AI, Virtual Desktops (VDI):

- **Powerful:**
Solve complex problems faster and with less power than CPUs
- **Fully integrated:**
GPUs seamlessly integrate into our cloud infrastructure, API, and management tools



GPU Computing

NVIDIA Tesla P100/K80

Applications: AI, deep learning

Get up to 50x performance
over the Tesla K80

Enable up to 65 percent more
machine learning*

NVIDIA Grid K2

Applications: Professional-grade graphics

- Ramp up any graphics applications that require blazing speed
- *NEW* Now available by the hour

NVIDIA Tesla M60

Applications: Data analysis,
scientific computation

Massive data analytics computations

NEW Now available by the hour

GPU Computing use cases

Virtual desktop infrastructure

- Scale, secure, standardize, and provide enhanced performance with GPU enabled offerings

Financial services

- Performing large and complex financial transactions

Gaming

- Process and render data and graphics for high game performance

Scientific research

- Solve complex molecular modeling calculations or analyze massive amounts of seismic data

Healthcare

- Log on to your desktop from any workstation within the network facility without slowing down traffic

Graphic design

- Experience smooth, multimedia-rich applications, including 3D-intensive programs

Direct Link

Direct Link

Real challenges and real solutions

Native access to key Resources

With a high speed, direct network link between your data centers and ours, you can move data between servers at the speed of light—plus access key resources such as AI, blockchain, IoT, and more

Super Secure Data Transfer

Moving sensitive data to and from our cloud platform further ensures its security by completely avoiding exposure to the public internet at all times.

Hybrid Workload Support

On-prem apps run off-premises on a public cloud that analyzes data stored on-premises due to residency requirements.

Leverage existing IT investments

IT modernization is the top driver of public cloud adoption, followed by cost savings. Do both by leveraging existing investments while emphasizing cost savings.

Direct Link

IBM Cloud Direct Link helps ensure the security of sensitive data to and from the IBM Cloud. Back up or store huge volumes of data from your data center on IBM Cloud with predictable bandwidth costs. With a dedicated network connection, your transfer rates are fast, consistent and reliable.

- **Faster speed, lower latency:**

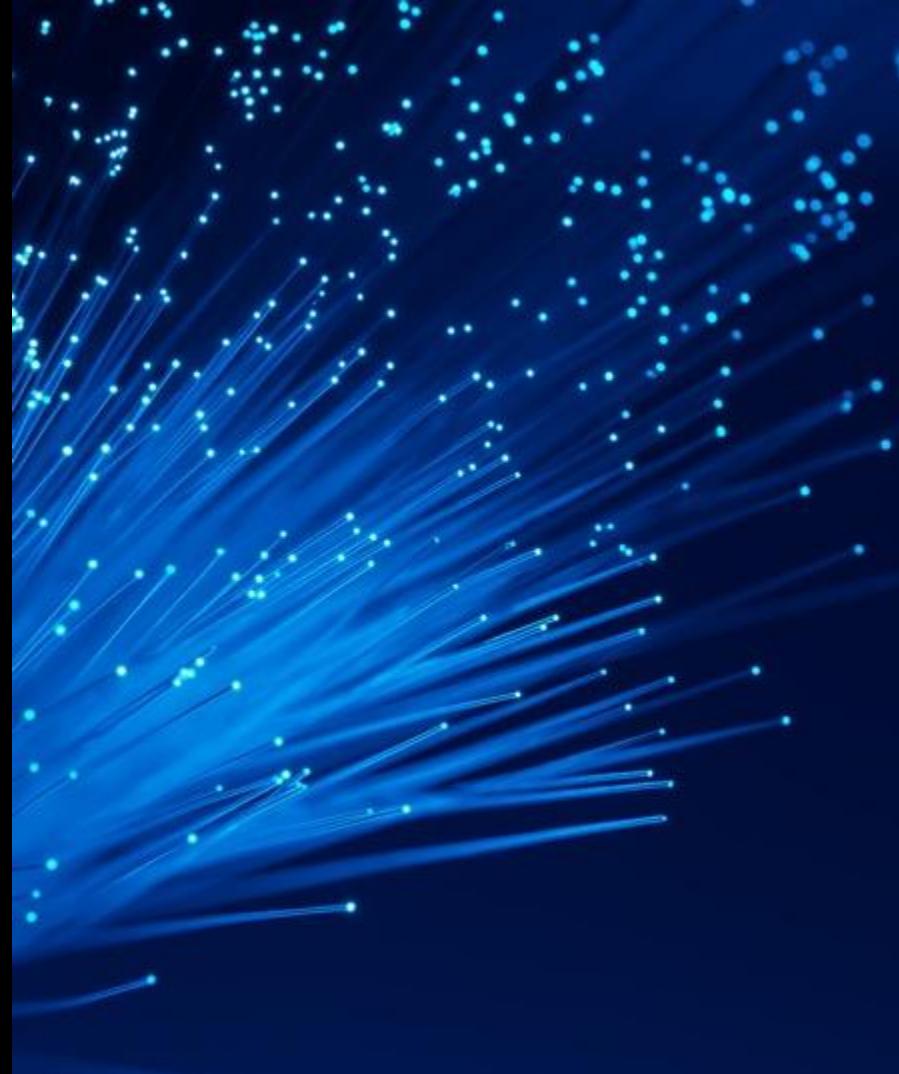
Move data to and from your data center across network connections at speeds up to 10Gbps.

- **Higher security:**

Protect your sensitive, business-critical data by controlling every network hop.

- **More reliability:**

Receive consistent, higher-throughput connectivity between a remote network and your IBM Cloud environments.



Network Security

Network Security

Real challenges and real solutions

E-commerce, Payment card industry

Businesses with security compliance requirements may require additional firewall layers between each tier of your network

Healthcare, Financial Services

Achieve regulatory compliance, improve efficiency, and enhance overall asset management by condensing the number of security groups

Small-Medium Business

81% of all data breaches happen to SMBs*, so protect data with a security plan that lets you control, deploy, and provision network security features quickly

Improved Migration Options

Leverage the WanClouds third-party Configuration Conversion tool to assist in migration from our legacy Vyatta 5400 offering to IBM Cloud Virtual Router Appliance

Network Security Options

Shared Hardware Firewall



- Protection for single servers provisioned on demand without service interruptions.

Dedicated Hardware Firewall



- 1Gbps, single-tenant protection for servers that share the same VLAN
- Provisioned on demand without service interruptions

FortiGate® Security Appliance 10Gbps



- Single-tenant firewall for multiple VLANs on public and private networks
- Provides access to add-ons such as intrusion prevention, anti-virus protection, and web filtering

Security Groups



- Value-added network security solution
- Define security policies at the instance level
- No support for bare metal

Shared Firewall

A shared hardware firewall leverages a multi-tenant enterprise platform to protect an individual server. It delivers virtualized network security through its virtual domain (VDOM) technology, providing separately provisions and managed virtualized security domains.



IBM Cloud – Dedicated Firewall

A dedicated firewall leverages a single-tenant appliance to protect any or all servers on a public VLAN. It can be added to a public VLAN at any time. Firewall rules are applied on a per-IP or per-subnet basis.



FortiGate® Security Appliance

A FortiGate® Security Appliance (FSA) is a dedicated single-tenant network device connected upstream from a server and protects any or all servers on a public VLAN.

Our **FortiGate Security Appliance 10Gbps** offering offers up to 10Gbps on both public and private VLANs for robust perimeter security.



Security Groups

Security groups are a value-added, zero cost solution that easily add instance-level network security to manage incoming and outgoing traffic on both private and public networks.

- Enhanced, instance-level control
- Scalable and customized for your needs
- You set ingress and egress filtering



Which Firewall is for me?

Offerings

| Features | Security Groups | Shared Hardware Firewall | Dedicated Hardware Firewall | FortiGate Security Appliance | FortiGate Security Appliance 10 Gbps |
|--------------------------------------|-----------------|--------------------------|-----------------------------|------------------------------|--------------------------------------|
| | | | | | |
| Stateful Packet Inspection | Yes | Yes | Yes | Yes | Yes |
| Customer managed appliance | No | No | Yes | Yes | Yes |
| VLAN Protection | No | No | Yes | Yes | Yes |
| Ingress Rules | Yes | Yes | Yes | Yes | Yes |
| Egress Rules | Yes | No | No | Yes | Yes |
| NAT Support | No | No | No | Yes | Yes |
| Multi-VLAN Support | No | No | No | No | Yes |
| DMZ and Multi-Tiered Network Support | No | No | No | No | Yes |
| Public and Private Network Support | Yes | No | No | No | Yes |
| SSL VPN Termination | No | No | No | Yes | Yes |
| IPsec VPN Termination | No | No | No | Yes | Yes |
| Open VPN Termination | No | No | No | No | No |
| HA Option | N/A | No | Yes | Yes | Yes |
| Manage from API & Portal | Yes | Yes | Yes | Appliance GUI | Appliance GUI |
| 10Gbps Support | N/A | No | No | No | Yes |
| NGFW Add-ons (IPS, AV, WAF) | No | No | No | Yes | Yes |

Storage

Block and File Storage

Deploy full-featured, Flash-backed¹ block storage in granular increments – from 1,000GB to 12,000GB – with customizable deployments, IOPS, and billing.

- **Go global:**

Provision block storage alongside your cloud servers in IBM Cloud data centers worldwide.

- **Easy to work with:**

Stay confident with a higher class of block storage designed to protect, simplify, and cater to your changing needs.

- **Get predictable billing:**

Lock in your costs by the month or by the hour, without the surprise of hidden fees or additional charges.

Now with monthly and hourly billing.



Block and File Storage

20GB to 12TB storage | Max of 48,000 IOPS(2) | Monthly and hourly billing

Choose your deployment:

1) Endurance tiers:

Specify capacity only (IOPS and throughput scale with volume size). Pre-defined for simplicity. Ideal for most workloads.

Example:

500GB volume @ 2 IOPS

500GB * 2 IOPS/GB tier = 1,000 IOPS total

1000 IOPS * 16kb block size = 16MB/s

throughput

\$0.20/GB * 500GB = \$100/month

2) Performance options:

Specify both capacity and IOPS. Ideal for workloads with well-defined performance requirements.

Example:

500GB volume with 250 IOPS

250 * 16kb block size = 4 MB/s throughput

\$0.10/GB * 500 GB + \$0.07/IOP * 250 =

\$50 + \$17.50 = \$67.50 / month

Block and File Storage

Industry essentials come standard

At rest data encryption: Disk level with provider managed keys(5)

Expandable volumes/adjustable IOPS: Accommodate dynamic workload needs on the fly

Flash-backed: Decreased latency/increased throughput(1)

Max durability: Maintain availability and integrity through events without RAID arrays

Granular volume sizes: Lower your costs with TB increments

Customizable IOPS: Tailor assigned levels of IOPS tiers and customizable IOPS for top performance

Hourly or monthly: Create short-term use storage volumes for Dev/Ops, DR testing, etc.(3)

Snapshots and replication: Non-disruptive and automatically copied to an IBM Cloud data center(6)

High availability: Uses redundant networking connections to maximize availability; iSCSI-based Block Storage uses Multipath I/O (MPIO)

Volume duplication: Make updates offline, use for DR/Ops or as the golden template

Object Storage

Real challenges and real solutions

Data Transfer

Fast, secure, reliable transfer of data to Object Storage

- Migrate large volumes of unstructured data to cloud storage
- Archive data to cloud from on-premises storage systems
- Replicate for disaster recovery sites in the cloud



Safe enterprise collaboration

A secure solution for global file access and workloads

- Mobile device sync
- Cloud drive and VDI services
- Remote data protection & backup for endpoints and servers
- Regulatory compliance
- Archive for inactive NAS data



Content repository and archiving

Eliminate data silos & increase the usability of your data across modern applications

- Repository for video, images, project data (Object, NAS, Legacy Storage)
- Repository for data used by IBM Spark as a Service, IBM Analytics Engine & Data Science
- Media asset repository
- Medical image repository



Object Storage Benefits

Store and access your data from anywhere in the world via self-service portals and APIs. Get enterprise availability and security with cloud economics and scale. Pay only for what you use, and leverage IBM Cloud Object Storage with your applications, or integrate with other IBM Cloud services, including analytics, compute, and cognitive.

- **Use it your way:**

Create a backup, archiving, or multimedia content repository solution. Store unstructured data for analytics, IoT, social, cognitive and mobile applications.

- **Always-on availability:**

Choose the level of resiliency that's right for you.

- **Simple, predictable billing:**

Pay only for what you use across multiple storage classes.

Help save costs with price caps for dynamic data access.



Object Storage IBM recognized in July 2017 Gartner Magic Quadrant for Public Cloud Storage Services, Worldwide

Gartner does not endorse any vendor, product, or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

IBM Cloud Object Storage

Industry-leading flexibility, scalability, and simplicity



On-Premise

- Single tenant
- Design-specific to client needs
- Total control of system



Dedicated

- Single tenant (compliant)
- No data center space required
- Flexible configuration options
- OPEX vs CAPEX



Public

- Multi-tenant
- Usage-based pricing
- Elastic capacity
- No data center space required.
- Fully managed
- OPEX vs CAPEX

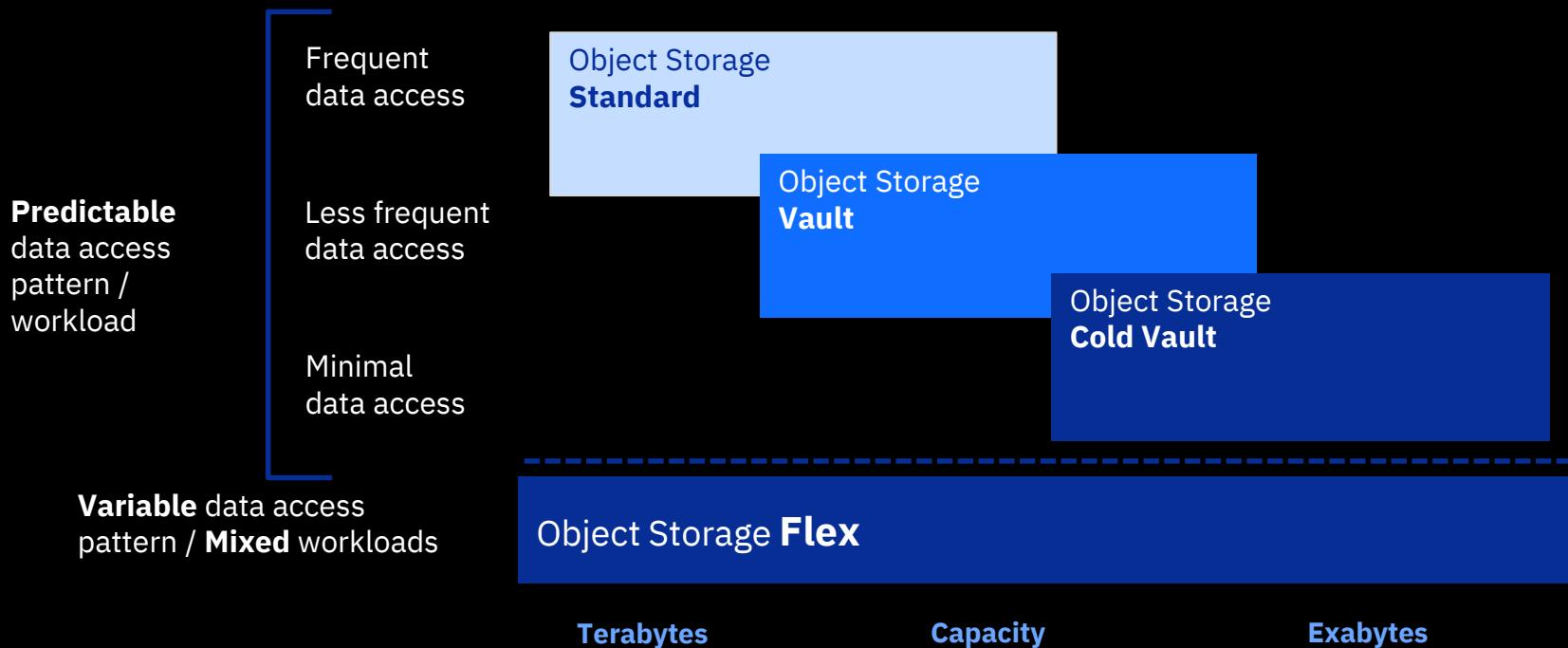


Hybrid

Consistent, uniform, and open technology across on-premises, dedicated, and public cloud makes it easier and more efficient to manage data, workloads, and business processes

Object Storage

Public cloud services designed for today's dynamic workloads

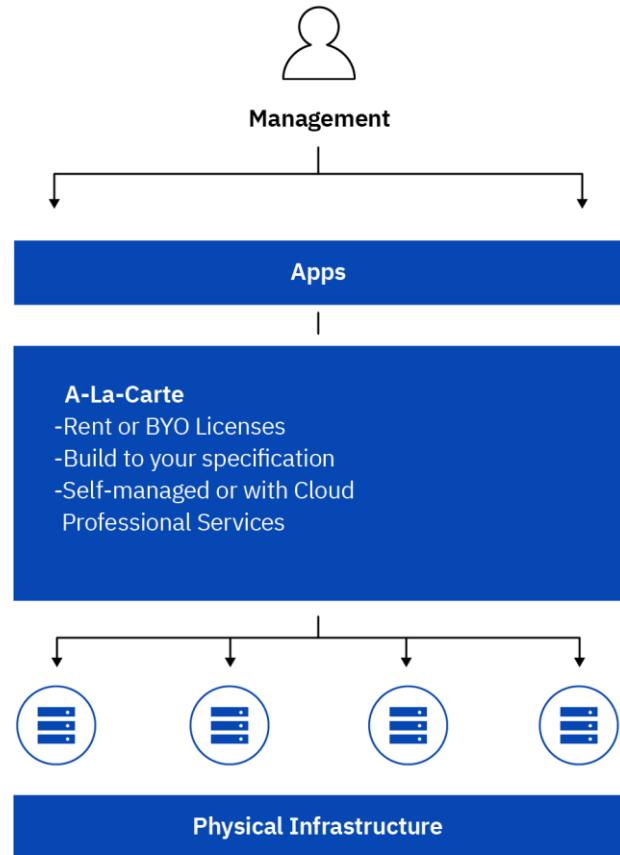


VMware

VMware vSphere® on IBM Cloud

Benefits

- Purchase or bring your VMware licenses – Per CPU licensing
- Build your own custom Private VMware Cloud on IBM Cloud
- Manage environment to your specifications





2019 IBM Cloud
用戶實作課程 冬季班

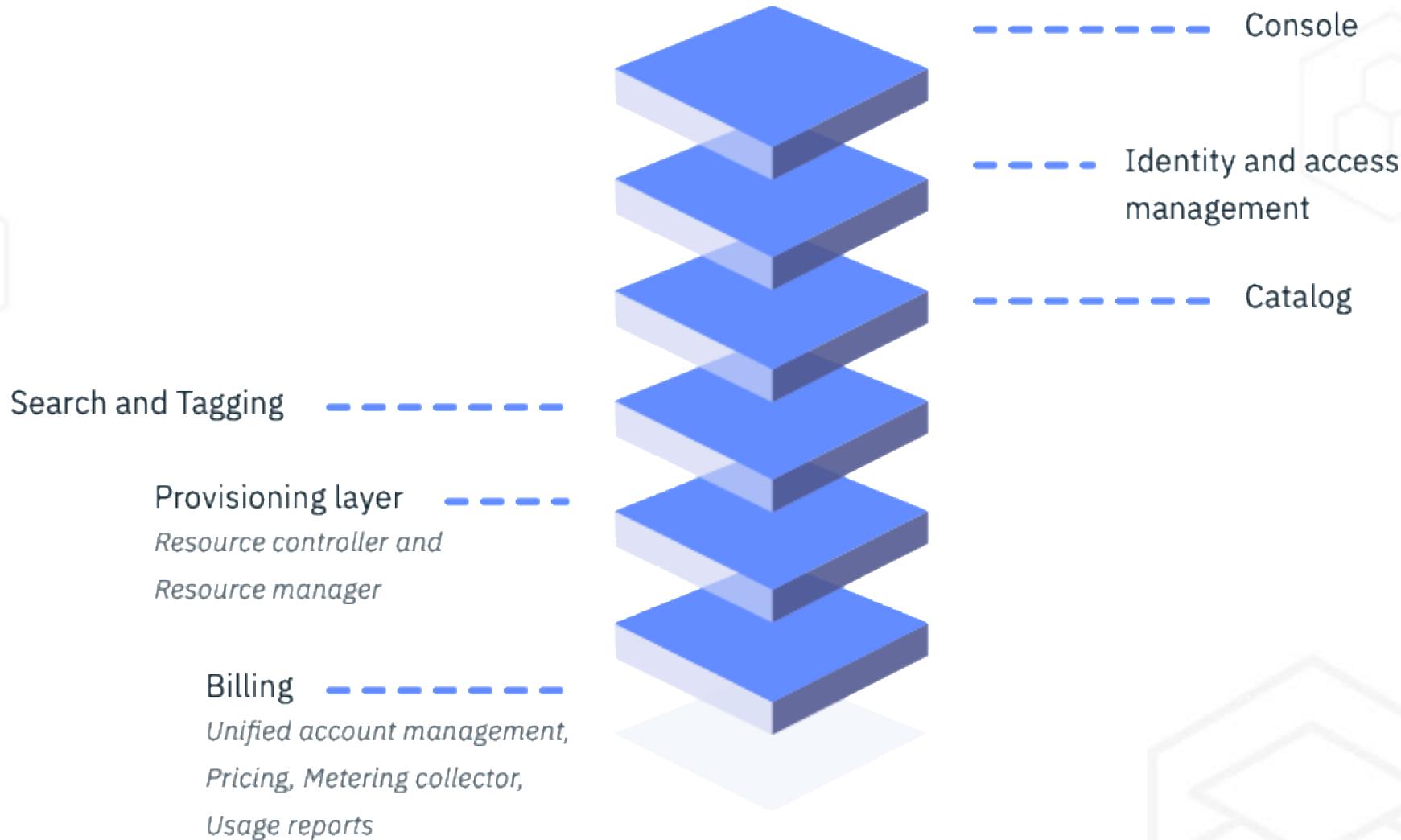
IBM Cloud 架構設計說明

IBM Cloud Unit

雲端專家

馮建國 (Gordon)

IBM Cloud Platform



<https://www.ibm.com/cloud/garage/architectures>

Multicloud

Explore architectures that provide multicloud solutions.



Private cloud

Leverage the benefits of the public cloud with enterprise control.



Public cloud

Use public cloud to solve real-world problems.



Multicloud management

Automate and manage your multicloud and multivendor infrastructure.

Built for AI

Explore architectures that focus on AI solutions.



AI

Gain business advantage by unlocking new intelligence from structured and unstructured data.



Data and analytics

Store, analyze and report on data by using analytic engines to drive actionable insights and visualization.

Popular application styles

Build a specific type of application that is functionally constrained by the problem you're solving.



Microservices

Take a cloud-native approach to building mobile and web applications with a microservices architecture.



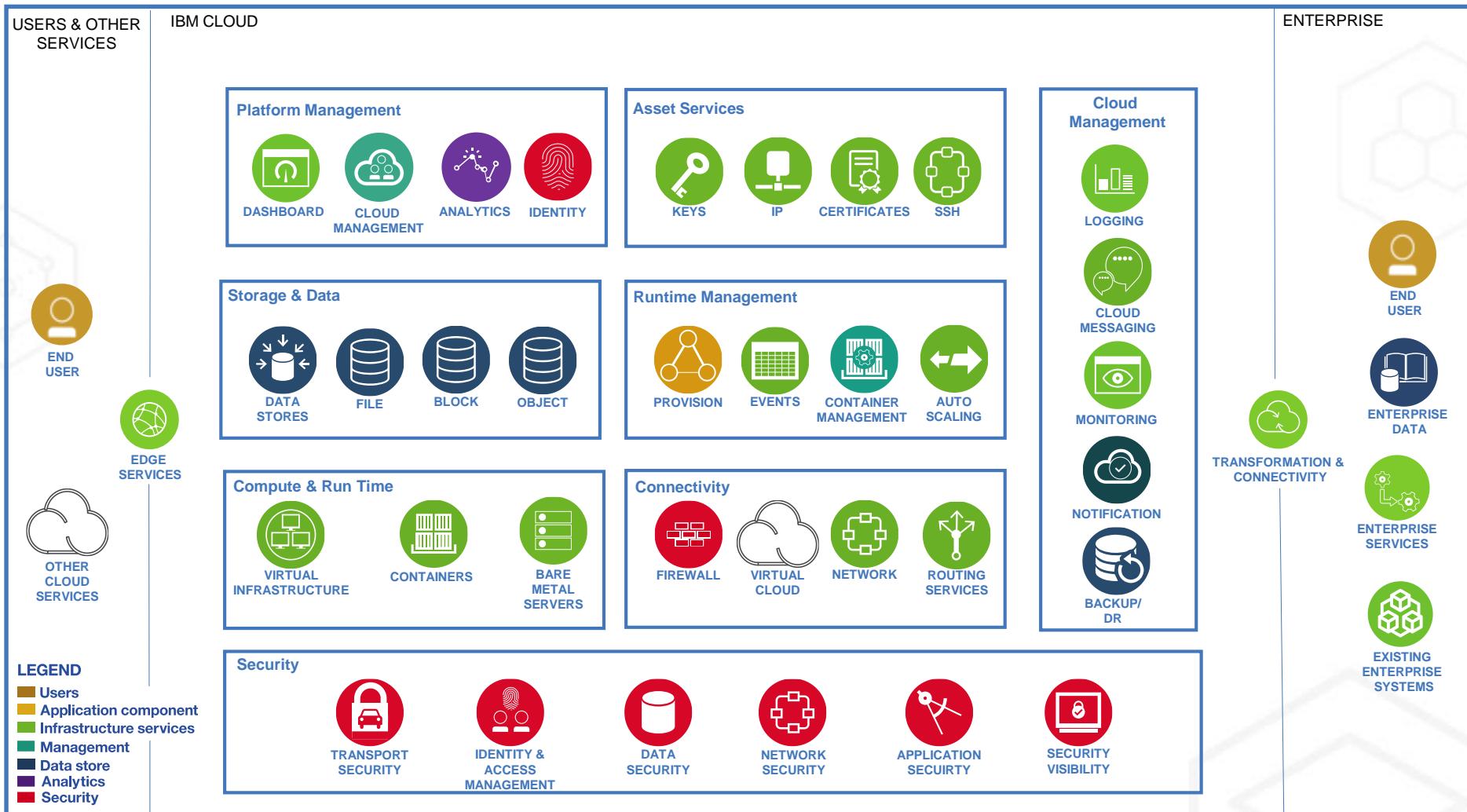
Web applications

Quickly gain the experience and confidence to build and deploy web applications in the cloud.

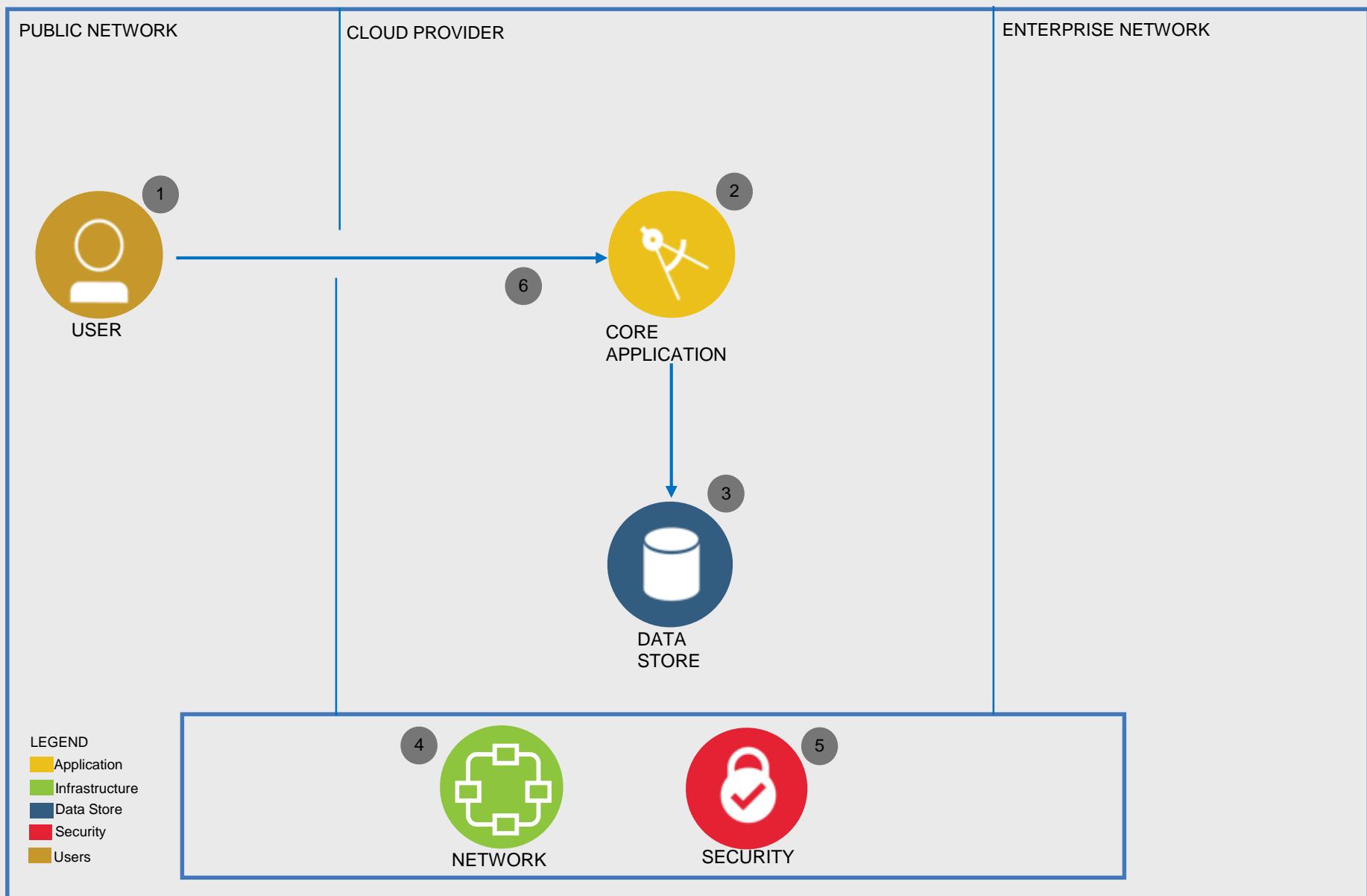


Blockchain

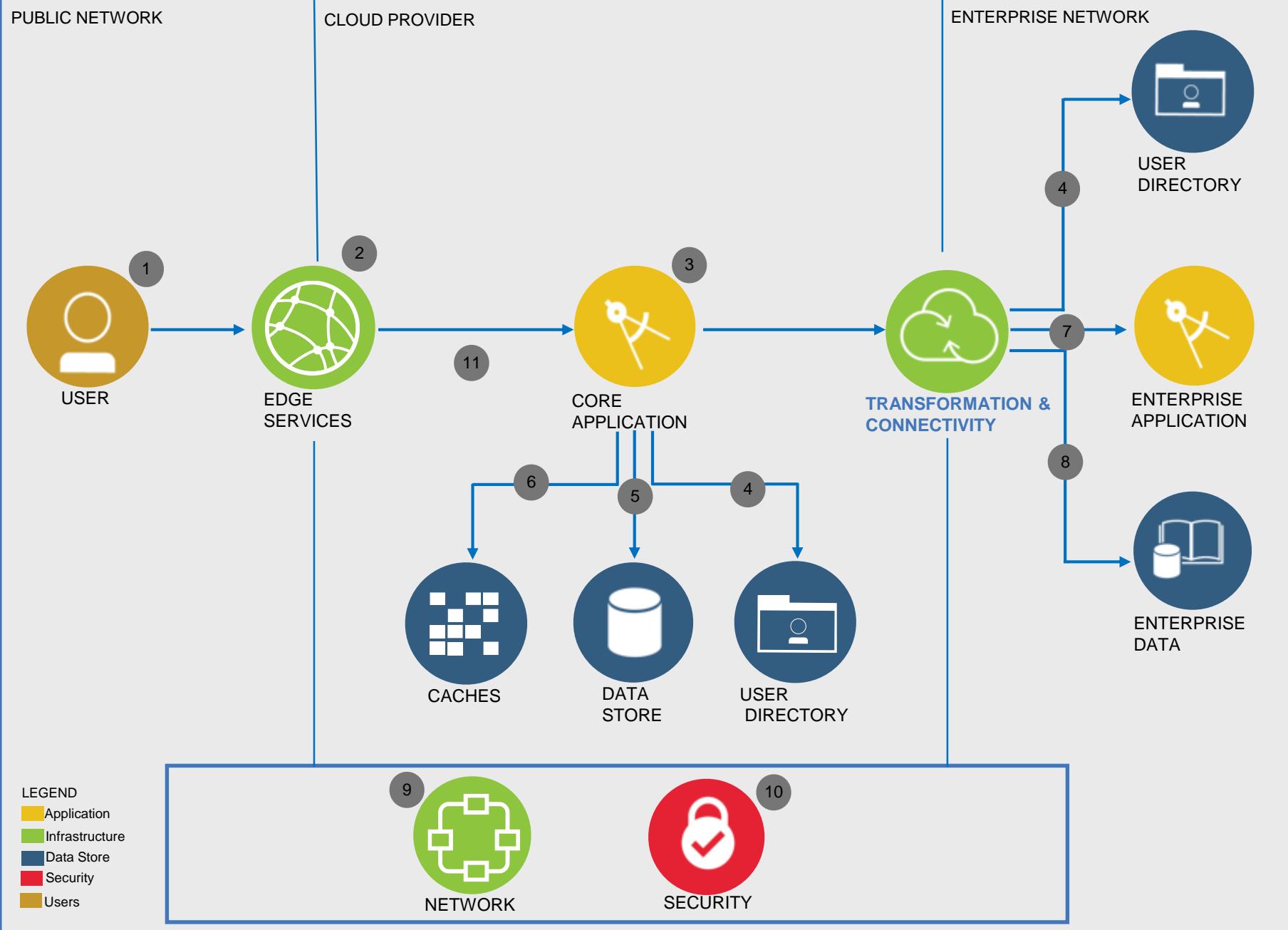
Record a history of transactions in a shared, immutable ledger for transactional applications.



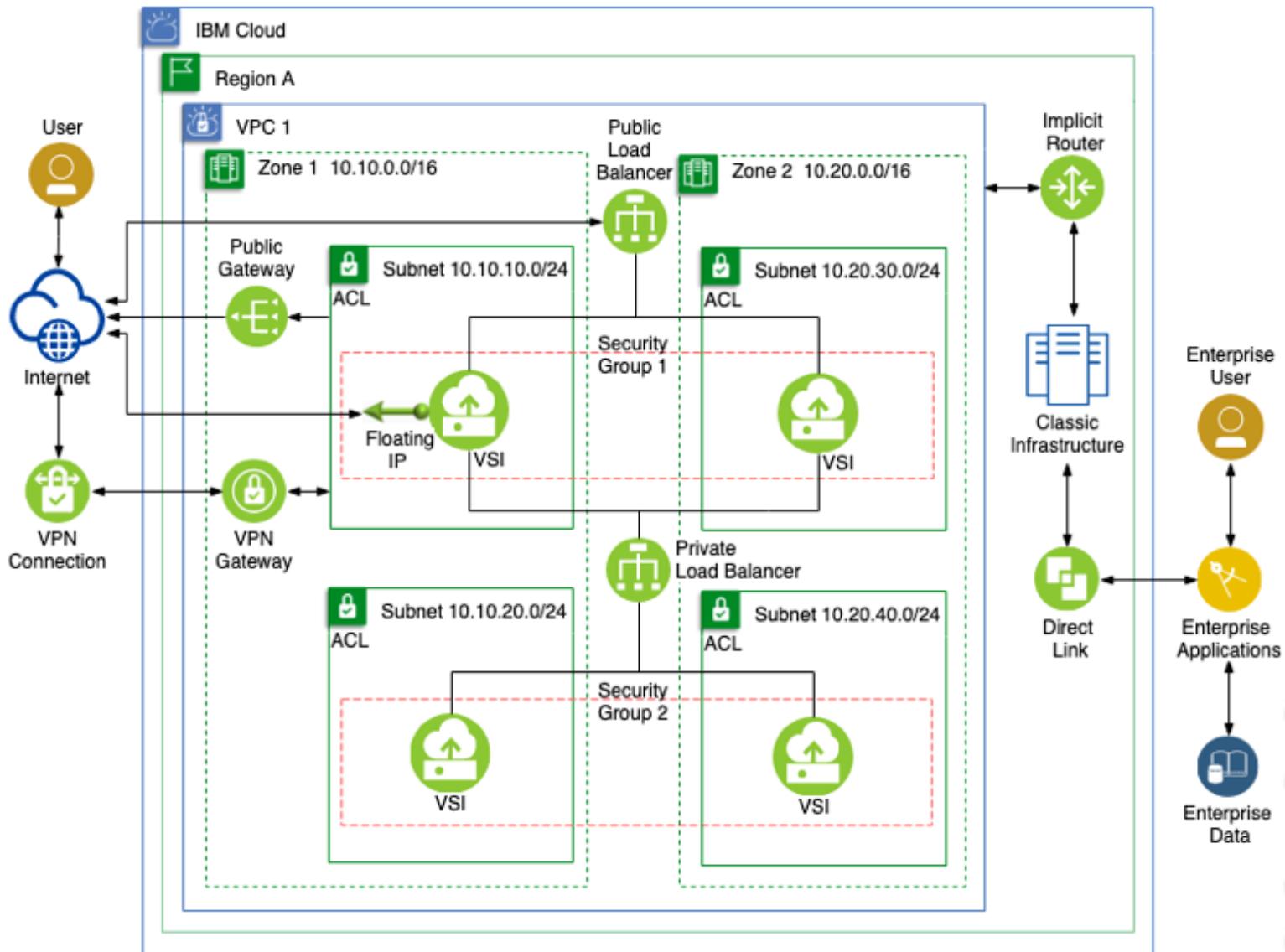
Advanced Web application basic reference architecture



Advanced Web application advanced reference architecture



IBM Cloud VPC Overview





2019 IBM Cloud
用戶實作課程 冬季班

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

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

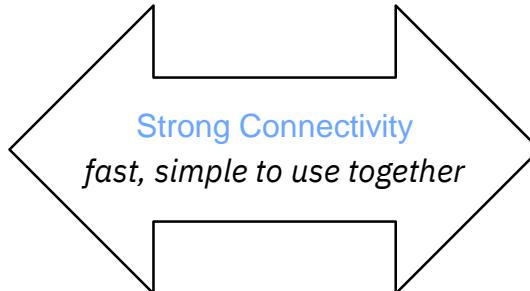
Faster, More Scalable Provisioning

Provision more resources, faster

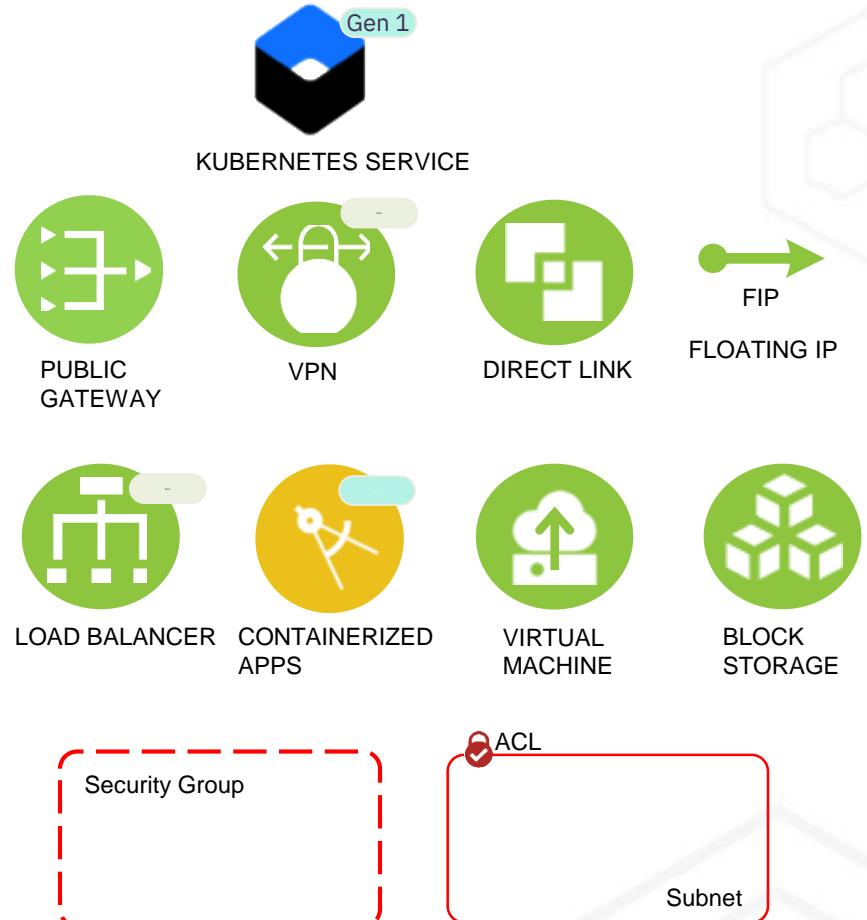
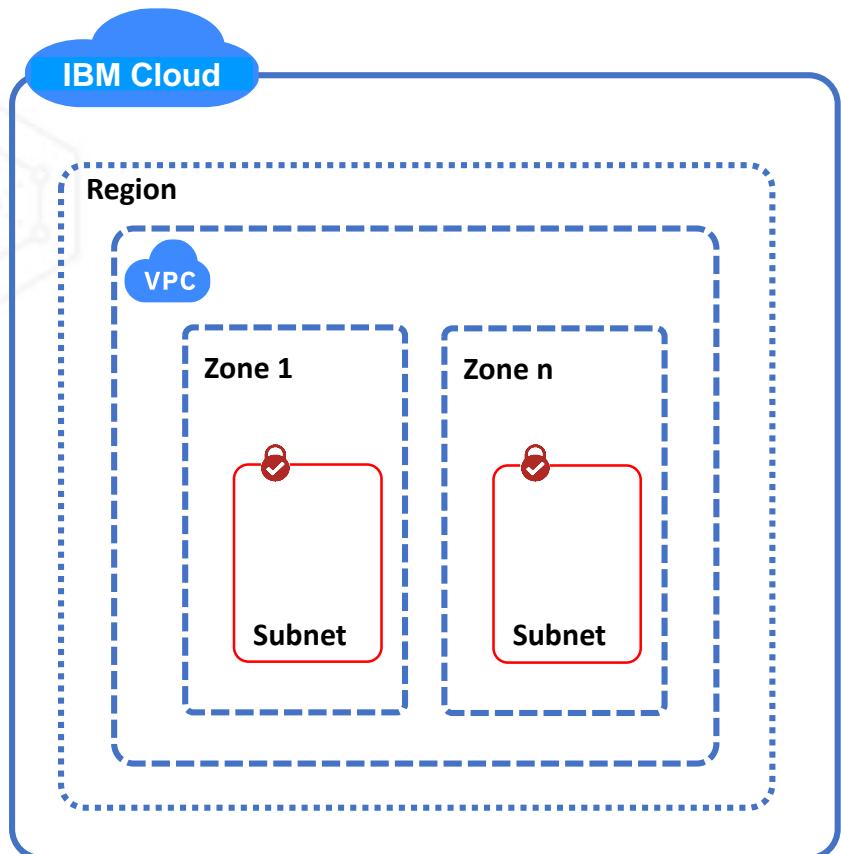
Virtual Networking

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

PUBLIC
NETWORK

CLOUD
NETWORK



INTERNET

Region – US South

VPC

Zone 1



Subnet 1
10.0.1.0/24

Zone 2



Subnet 3
10.0.3.0/24



Subnet 2
10.0.2.0/24



Subnet 4
10.0.4.0/24

ENTERPRISE
NETWORK



ON PREMISE

KEY



VIRTUAL
MACHINE



BLOCK
STORAGE



REGION



ZONE



SUBNET

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 | ACLs | Gen 2 |
|------|-----------------------------------|------|-----------------------------------|
| - | 30 per region | - | 25 per VPC |
| - | 20 ingress rules per ACL | - | 25 ingress rules per ACL |
| - | 20 egress rules per ACL | - | 25 egress rules per ACL |
| SGs | Gen 1 | SGs | Gen 2 |
| - | 500 per account | - | 25 per VPC |
| - | 5 per network interface | - | 25 rules per Security Group |
| - | 50 rules per Security Group | - | 5 remote rules per security group |
| - | 5 remote rules per security group | - | 100 NICs per SG |

For up-to-date quotas always refer to the [Cloud Docs page](#)

VPC Features

Network Security – ACLs and SGs

PUBLIC
NETWORK

CLOUD
NETWORK



INTERNET

Region – US South

VPC



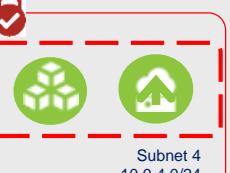
Subnet 1
10.0.1.0/24



Subnet 3
10.0.3.0/24



Subnet 2
10.0.2.0/24



Subnet 4
10.0.4.0/24

ENTERPRISE
NETWORK



KEY

VIRTUAL
MACHINE



BLOCK
STORAGE



REGION



ZONE



SUBNET



ACL



SECURITY
GROUP



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

Internet Connectivity



Classic Infrastructure:

- Vyatta / VRA VPN
- Juniper vSRX
- Direct Link

Available

Gen 1

Gen 2

Public Gateways

- 1 per VPC per zone
- 1 per VPC per zone

Address Prefixes

- 5 per VPC per zone
- 5 per zone

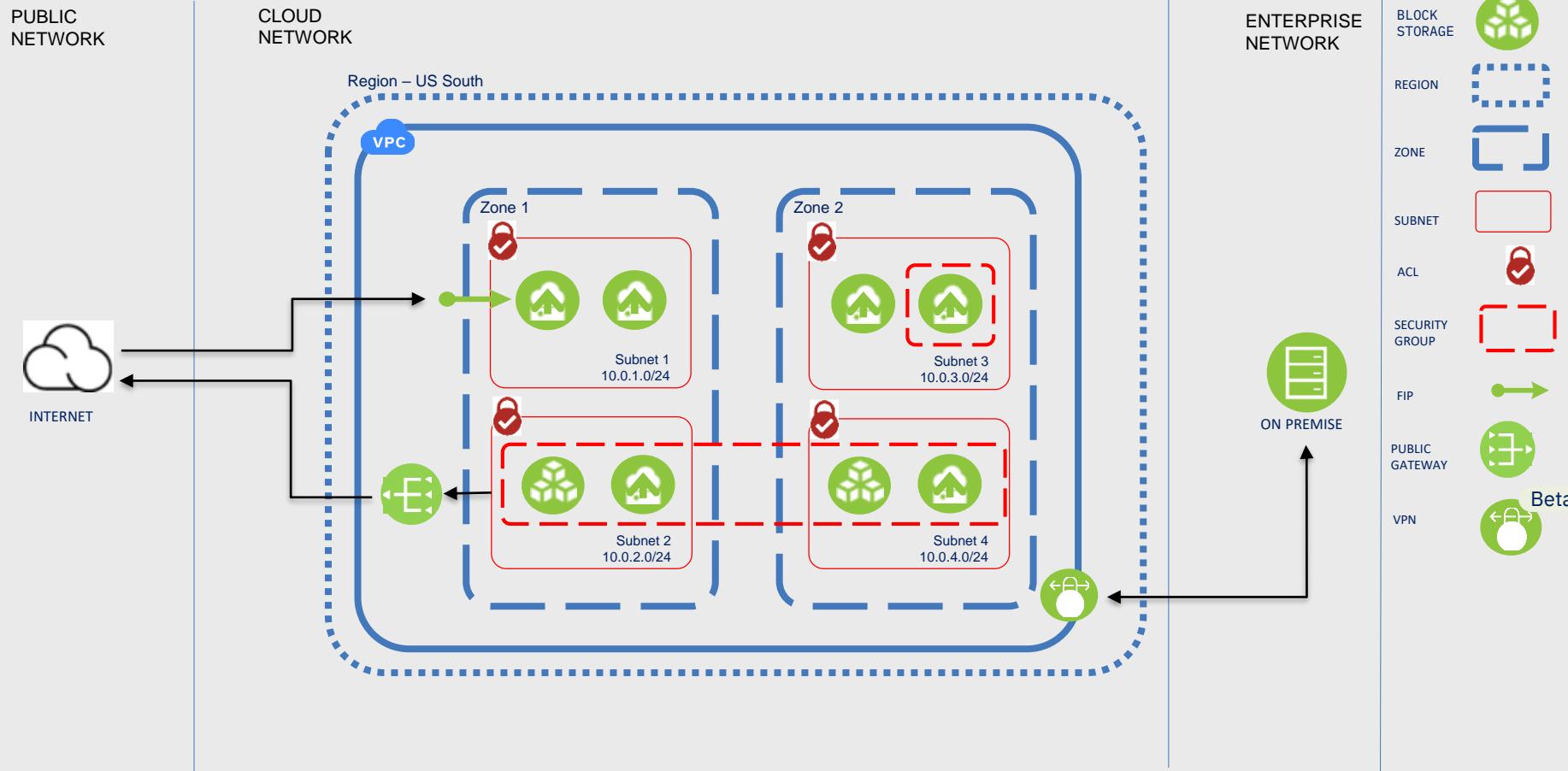
FIP

- 100 per zone per account
- 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

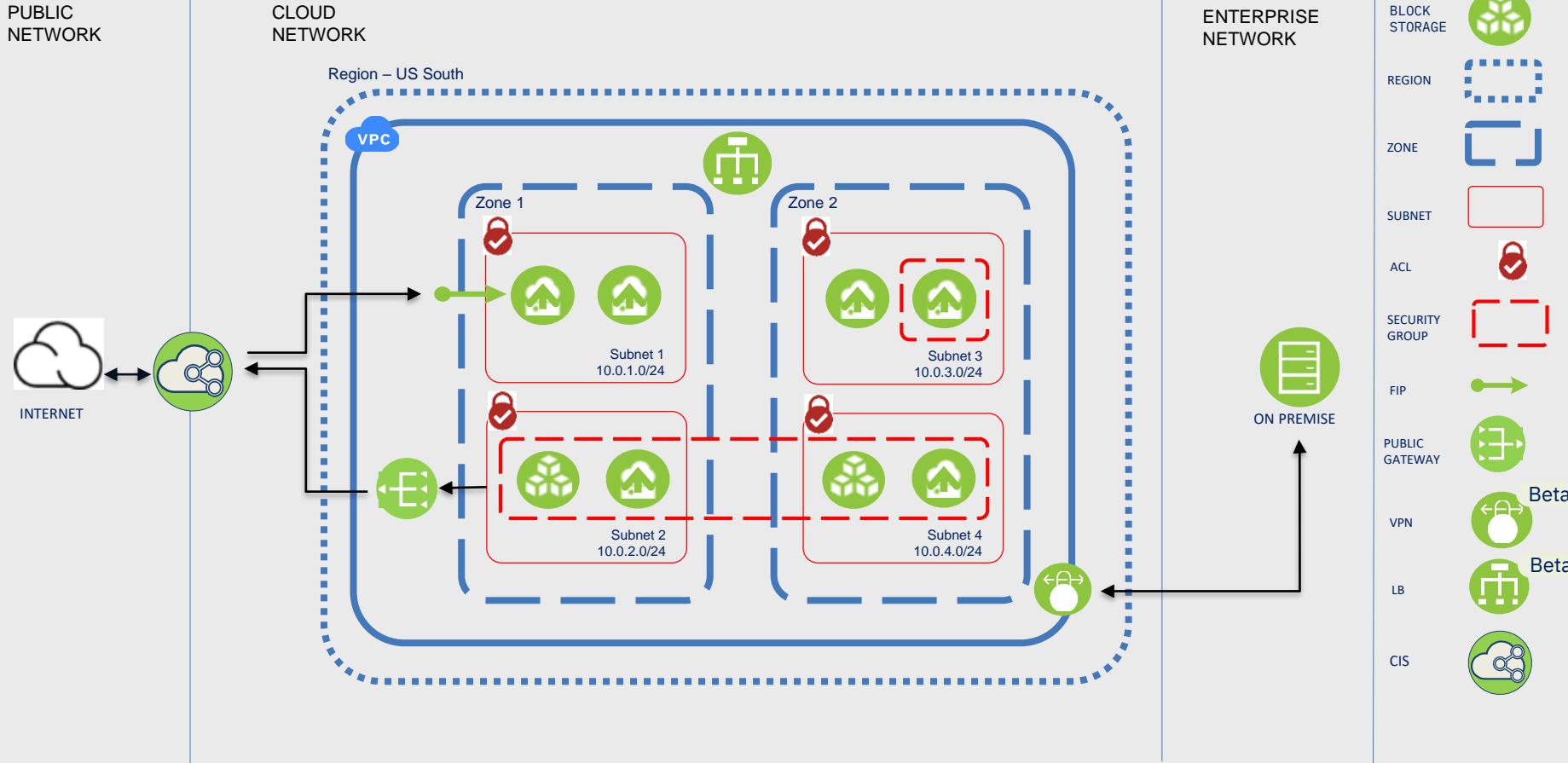
CIS

- 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, 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

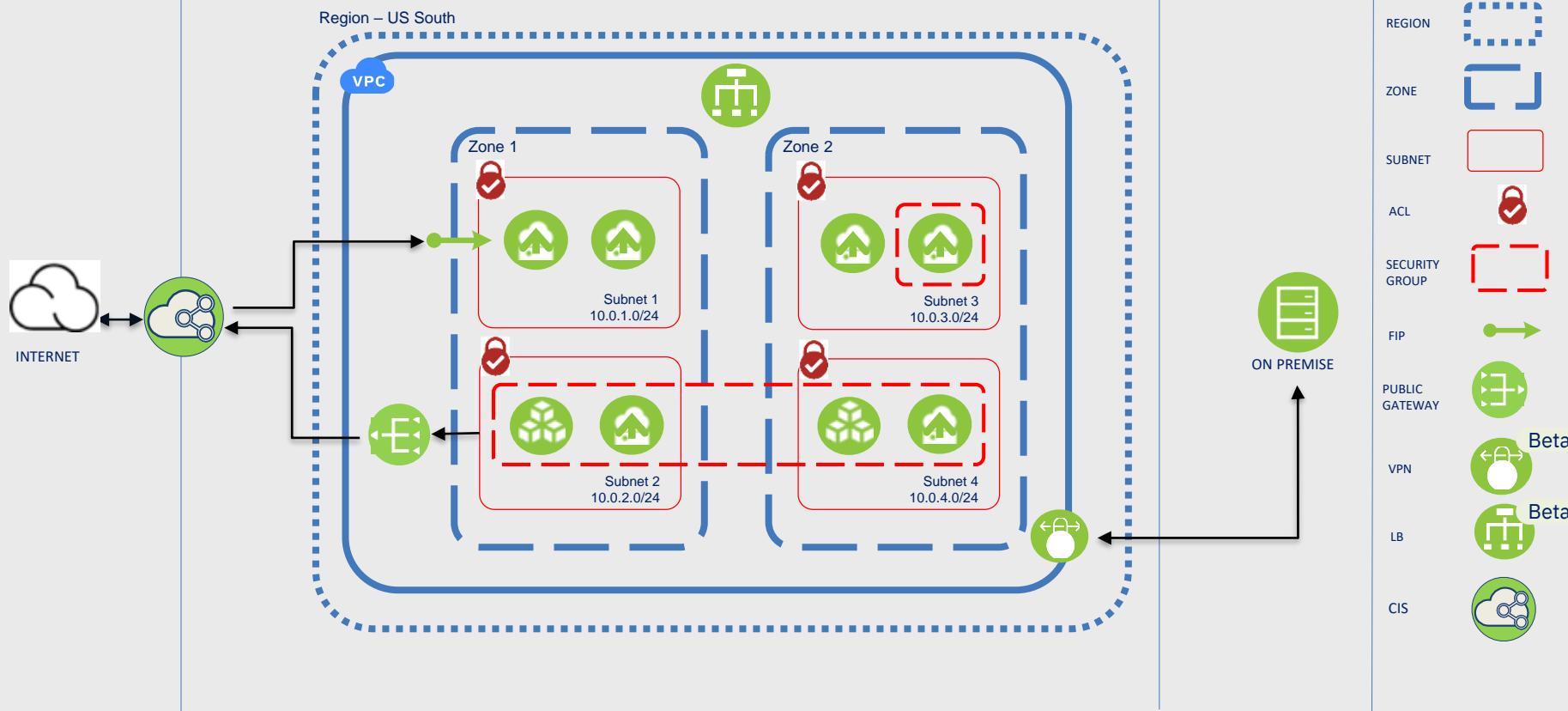
For up-to-date quotas always refer to the [Cloud Docs page](#)

VPC Features

Compute & Storage

PUBLIC
NETWORK

ENTERPRISE
NETWORK



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

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)

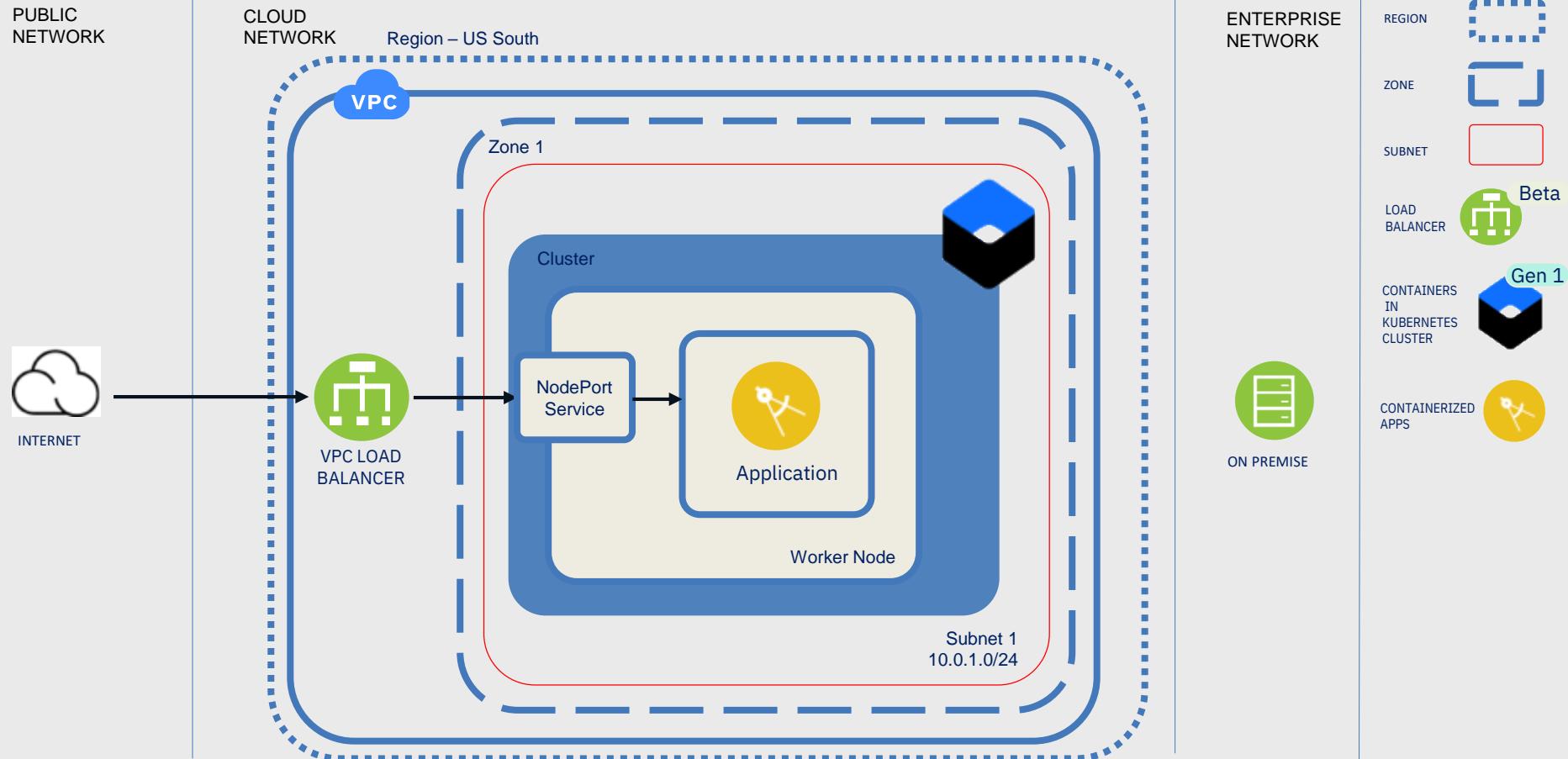
IKS Support for VPC Network ACLs and Kubernetes NetworkPolicy

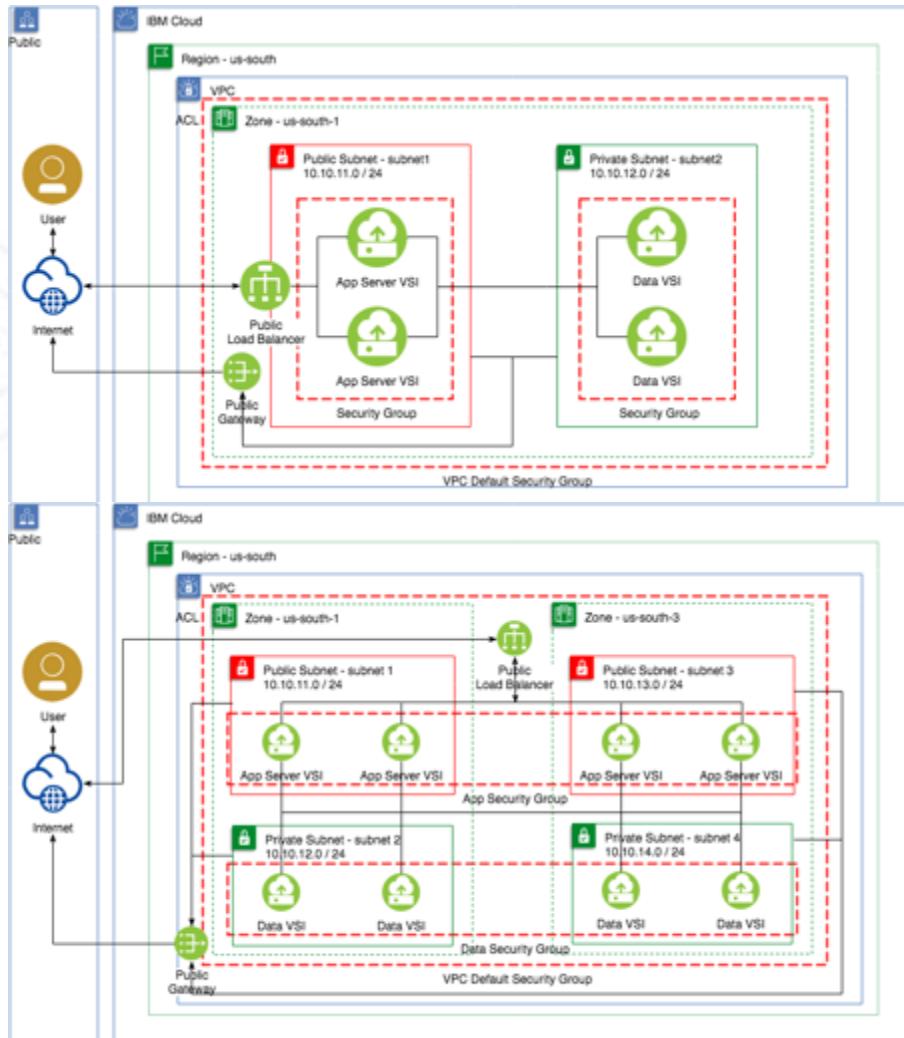
- Create VPC subnets for IKS clusters and create network ACLs for easy host level traffic control.
- Use Kubernetes NetworkPolicy for container/Pod level network access control.

- **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](#)

IKS on VPC Features





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



Developer Productivity, Choice, Control, & Consistency

Speed



Portability



Performance &
Control



Cloud Functions

"Serverless" / Event Driven Apps



Cloud Foundry

Open PaaS Environment



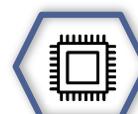
Containers & Kubernetes

Maximum Portability



Virtual Server or VMware

Leverage Existing Images & Tools



Bare Metal

Maximum Performance & Control

Language/
Framework

.js  java 

.py  .php

.go 

.rb 

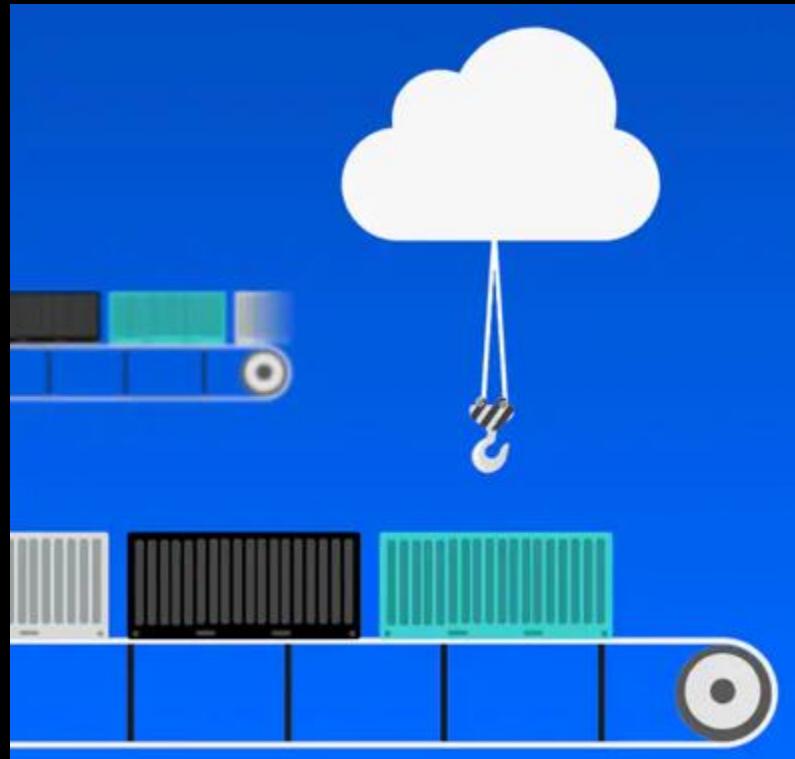
express

 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



Intelligent
Scheduling



Self-healing



Horizontal scaling



Service discovery
& load balancing



Automated
rollouts and
rollbacks

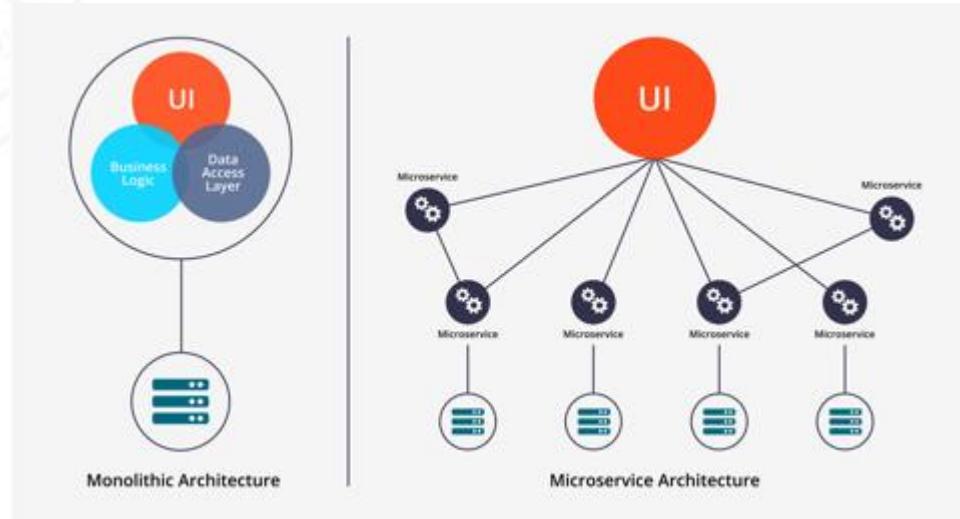


Secret and
configuration
management

Business value of containerization and Kubernetes:

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

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.

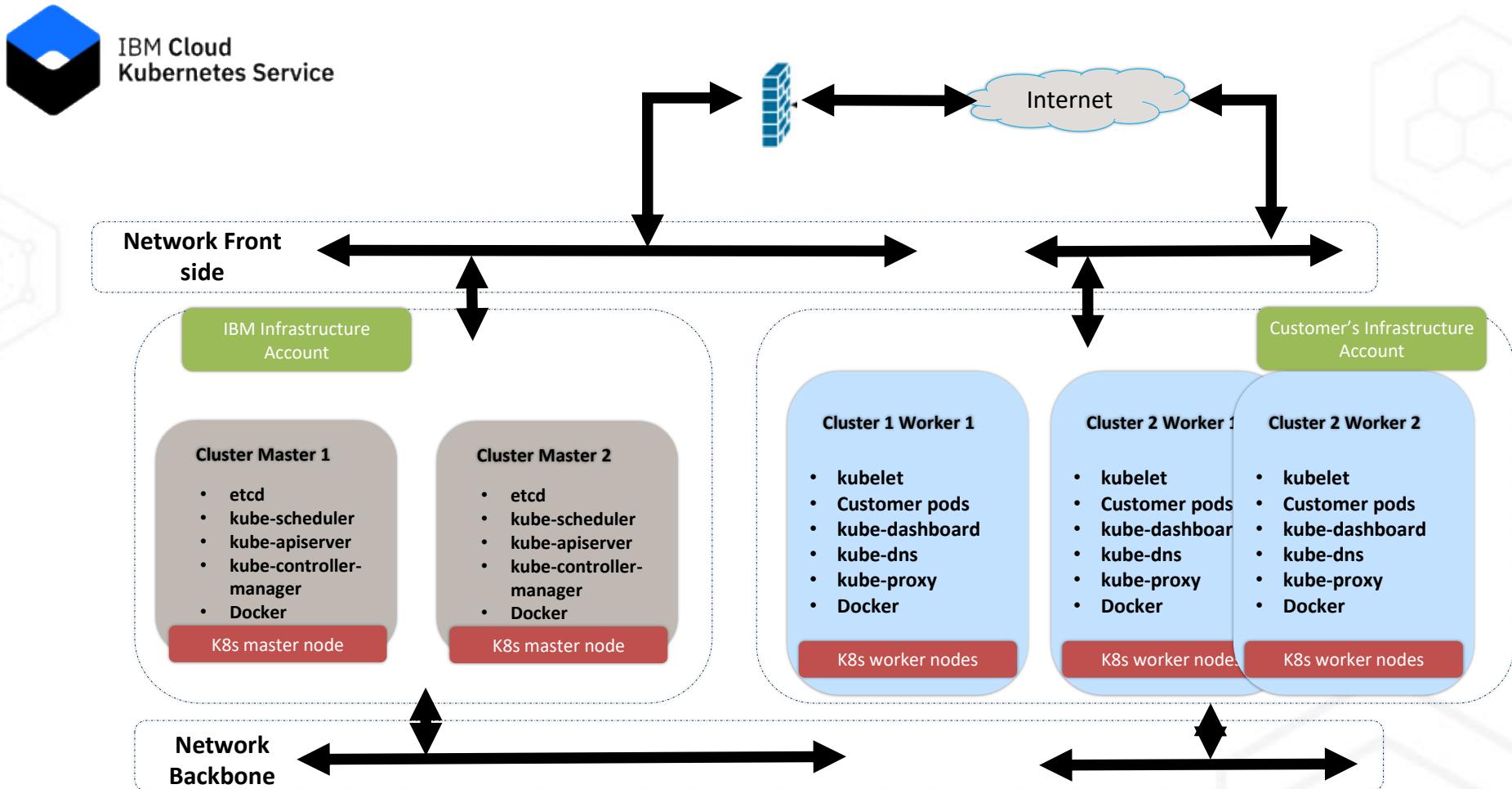
Workload flexibility

6 IBM Cloud Regions, 35+ Datacenters



https://console.bluemix.net/docs/containers/cs_regions.html#region-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 |



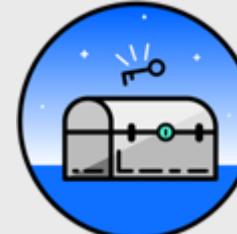
IKS Capabilities



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

Region: US-East

Cluster type: Standard

Location:

- Availability: Single Zone (selected)
- Multizone

Zone:

- None
- node01 (selected) No VLANs Exist: VLANs will be created for you.
- node04
- node06
- node07

Default worker pool

Configure a set of worker nodes with the same attributes to create a default worker pool. Don't worry, you can always update your pool later, or add pools with different configurations to your cluster.

Kubernetes version:

- 1.10.3 (selected)
- 1.9.7 (stable, Default)

1 →

3 →

Region: US-East

Cluster type: Standard

Location:

- Availability: Single Zone (selected)
- Multizone

Zone:

- Private VLAN: node01 (selected) No VLANs Exist: VLANs will be created for you.
- node06
- node07

Public VLAN:

- wk034
- wk036
- wk037

Default worker pool

Configure a set of worker nodes with the same attributes to create a default worker pool. Don't worry, you can always update your pool later, or add pools with different configurations to your cluster.

Kubernetes version:

- 1.10.3 (selected)
- 1.9.7 (stable, Default)

2 →

Multizone Cluster

Encrypt local disk

Worker nodes:

- 3

x 3 zones = 9 workers total

Finalize and create cluster

Almost done! Give your cluster a unique name.

Cluster name: mycluster

Create Cluster

4 →



Simplified Cluster Management

Resource list

Create resource

Collapse all | Expand all

| Name | Group | Location | Offering | Status | Tags |
|---------------------------------|---------------------------|-----------|--------------------|-----------|-----------|
| Filter by name or IP address... | Filter by group or org... | Filter... | Filter... | Filter... | Filter... |
| > Devices (30) | | | | | |
| ▽ Kubernetes Clusters (6) | | | | | |
| iks_cluster1 | default | Dallas 10 | Kubernetes Service | Normal | ... |
| iks_cluster2 | default | Dallas 12 | Kubernetes Service | Normal | ... |
| iks_cluster3 | default | Dallas 10 | Kubernetes Service | Normal | ... |
| iks_cluster4 | default | Dallas 12 | Kubernetes Service | Normal | ... |
| iks_cluster5 | default | Dallas 13 | Kubernetes Service | Normal | ... |
| wanclouds | default | Dallas 13 | Kubernetes Service | Normal | ... |

Clusters / iks_cluster1 ● Normal

Kubernetes Dashboard (Beta) ↗

Access Overview Worker Nodes Worker Pools Integrations

Summary

Cluster ID: b0d7d10x240f4b4f9493db7453b7858
Kubernetes version: 1.12.3_1531
Zones: dsl12, dsl13, dsl13
Owner: creseen@us.ibm.com
Ingress subdomain: ikscluster1.us-south.containers.mybluemix.net, ikscluster1.us-south.containers.appdomain.cloud
Resource group: default
Logs: View ↗
Metrics: View ↗
Key protect (Beta): Enable

Worker Nodes (8)

100% Normal

Worker Nodes

Search

| | Name | Status | Worker Pool | Zone | Private IP | Public IP | Kubernetes Version |
|---|------|--------|-----------------|-------|--------------|-----------------|--------------------|
| > | w2 | Normal | iks_workerpool3 | dsl13 | 10.73.90.157 | 10.9.61.47.363 | 1.12.3_1531 ⓘ |
| > | w3 | Normal | iks_workerpool2 | dsl10 | 10.177.26.11 | 10.9.46.74.245 | 1.12.3_1531 ⓘ |
| > | w4 | Normal | iks_workerpool3 | dsl12 | 10.185.22.14 | 10.9.48.228.183 | 1.12.3_1531 ⓘ |
| > | w7 | Normal | iks_workerpool2 | dsl12 | 10.185.22.6 | 10.9.48.228.188 | 1.12.3_1531 ⓘ |
| > | w9 | Normal | iks_workerpool2 | dsl10 | 10.177.26.53 | 10.9.46.74.254 | 1.12.3_1531 ⓘ |
| > | w10 | Normal | iks_workerpool2 | dsl13 | 10.73.90.189 | 10.9.61.25.29 | 1.12.3_1531 ⓘ |

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.

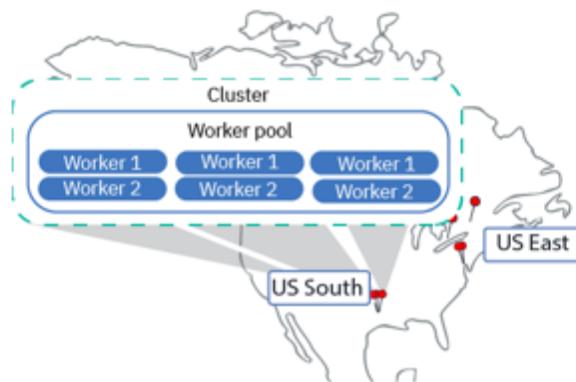
In an SZR, those masters are distributed across different hosts, ensuring availability during upgrades of Kubernetes versions or physical host level access.

Clustering

1 Single zone cluster



2 Multizone cluster



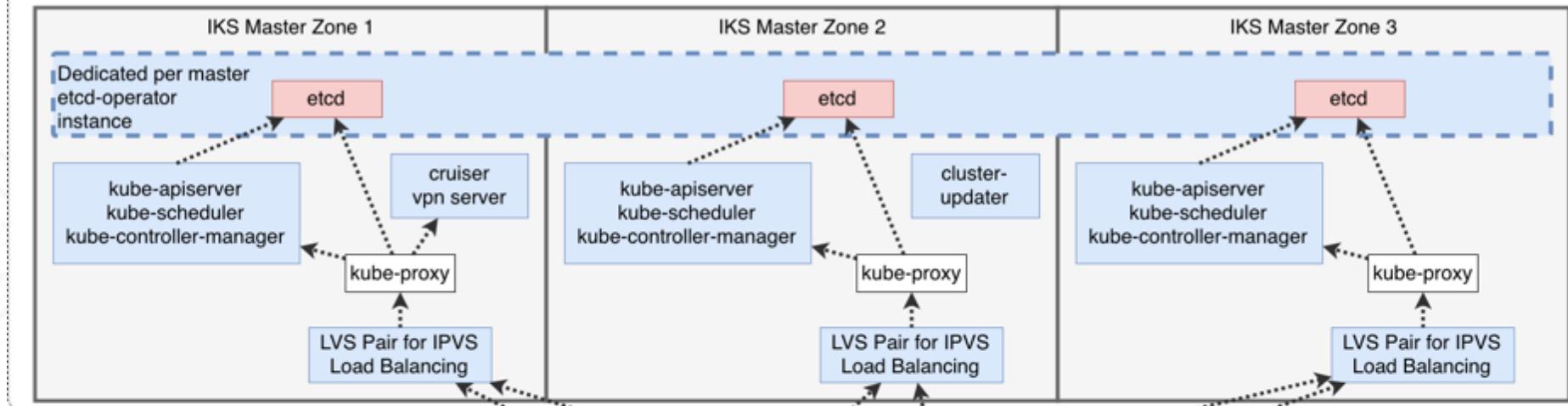
3 Multiple clusters with global load balancer



Cluster high availability

HA Masters Architecture

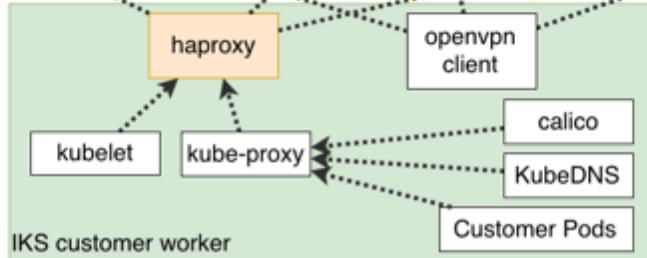
IKS IaaS



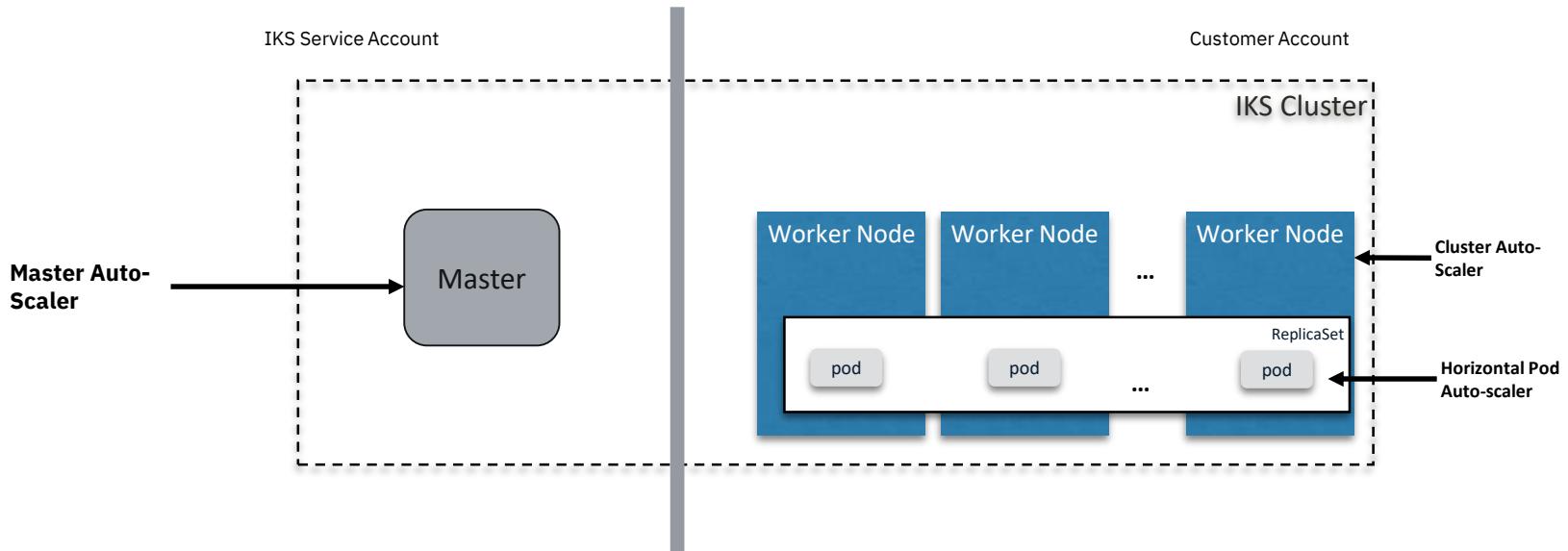
Note:

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.

Customer IaaS



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



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)

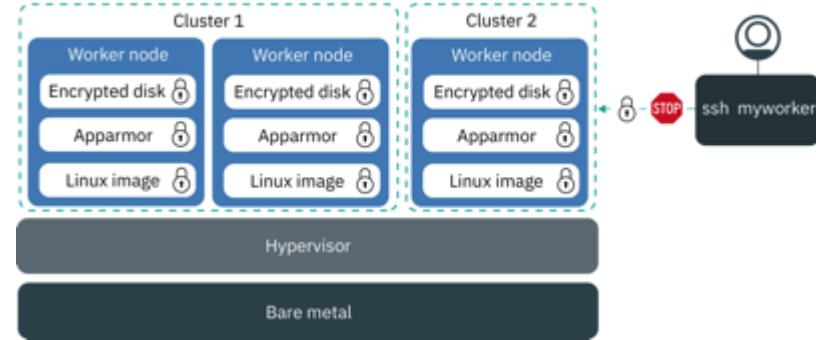


Image scanning and enforcement

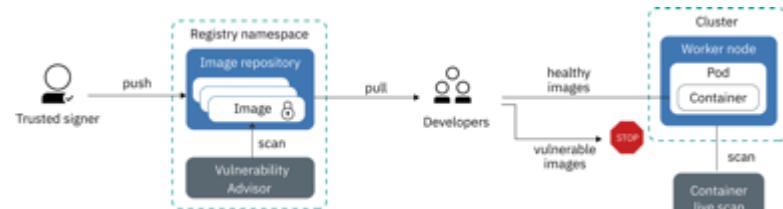
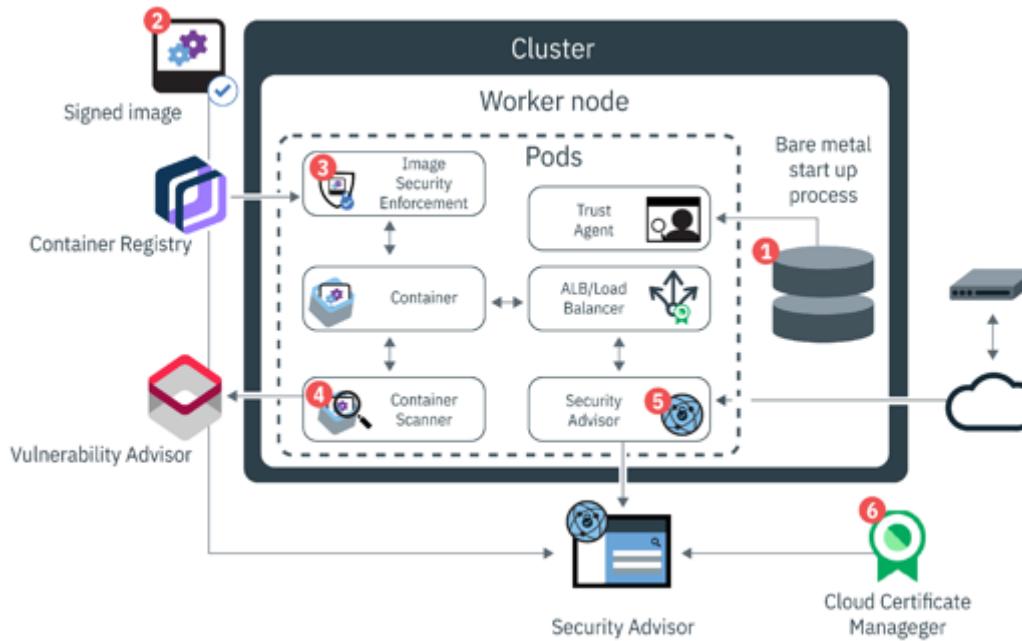


Image Security Enforcement in IBM Cloud Kubernetes Service

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**

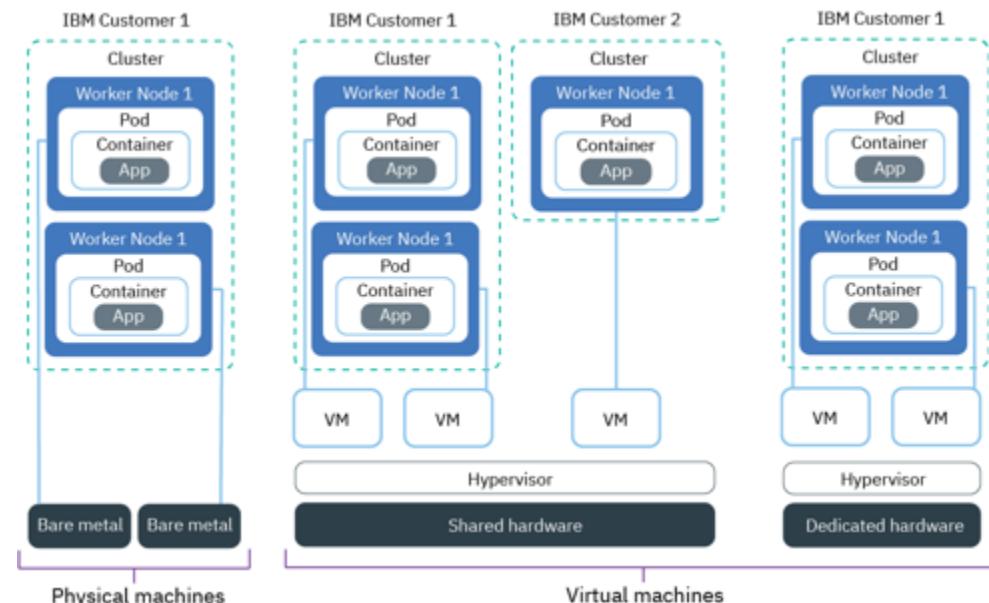
- Single-tenant virtual server instance, running on multi-tenant hypervisor and hardware
- Lower cost

- **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

The screenshot shows the Kubernetes Dashboard's Overview page. The top navigation bar has 'kubernetes' (blue), 'Search' (grey), and 'CREATE' (blue) buttons. Below the navigation, there are tabs for Cluster, Namespaces, Nodes, Persistent Volumes, Roles, Storage Classes, DaemonSets, Deployments, Pods, and ReplicaSets. The 'DaemonSets' tab is selected. The main content area shows 'Workloads' and 'Workloads Statuses' sections. The 'Workloads Statuses' section contains four pie charts: 'Daemon Sets' (100%), 'Deployments' (40.0% green, 59.9% grey), 'Pods' (49.0% green, 51.0% grey), and 'Replica Sets' (31.0% green, 68.9% grey). The 'Daemon Sets' table lists two entries: 'logstash-agent' and 'nginx-agent'. The 'Deployments' table lists five entries: 'nginx-v1', 'nginx-v2', 'nginx-v3', 'nginx-v4', and 'nginx-v5'. Both tables include columns for Name, Labels, Pods, Age, and Images.

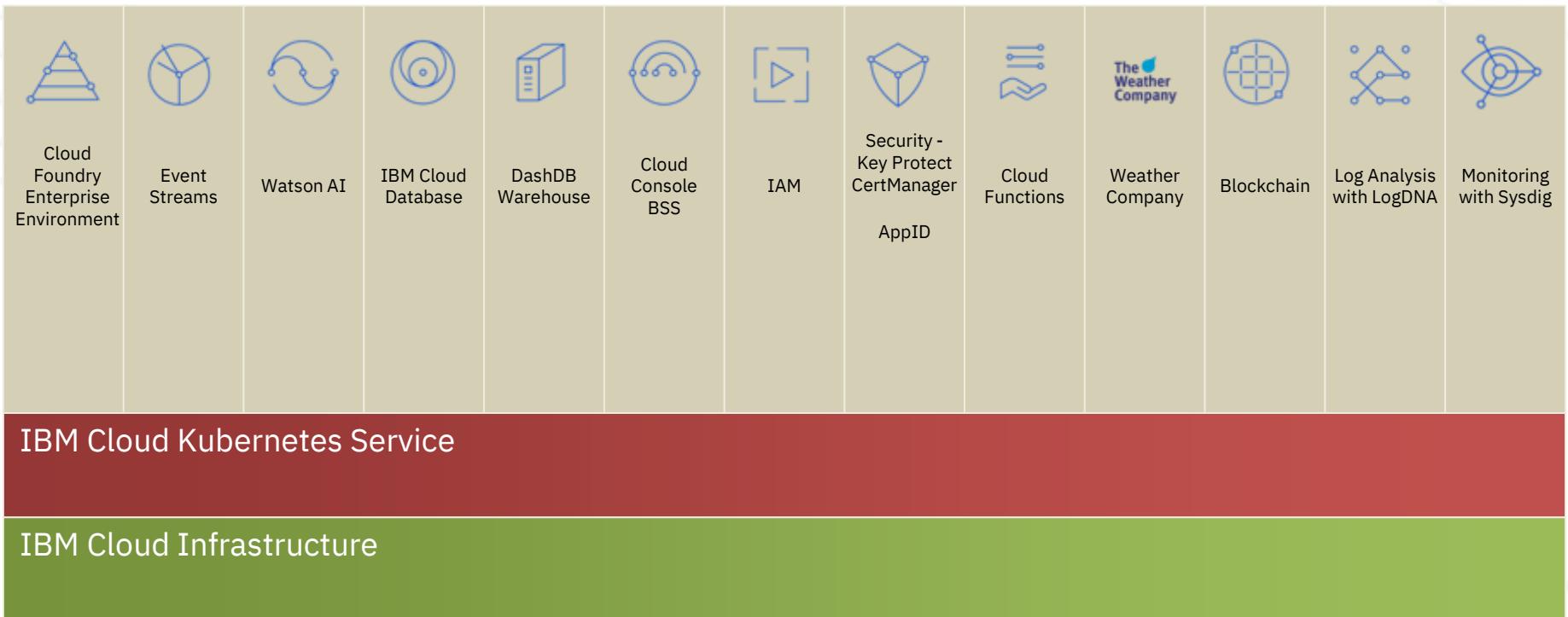
The screenshot shows the Grafana interface with the following details:

- Left sidebar:** Includes a search bar, a "Clusters and Nodes" section with a dropdown menu, and a "Metrics Explorer" icon.
- Top navigation:** Shows the title "Explore" and the current dashboard "Kubernetes Health Overview".
- Search bar:** Contains the query "kubernetes.cluster.name = null and kubernetes.node.name = null and kubernetes.pod.name = null".
- Panel 1: Request Count by Deployment**
 - Y-axis: Requests per second (0.00 to 100.00).
 - X-axis: Time (2017-01 to 2017-02).
 - Graph: A blue line chart showing a constant request count around 80 requests per second.
- Panel 2: Response Time By Deployment**
 - Y-axis: Response time in milliseconds (0 to 200 ms).
 - X-axis: Time (2017-01 to 2017-02).
 - Graph: A red line chart showing response times fluctuating between 100ms and 150ms.
- Panel 3: Net Error Count by Deployment**
 - Y-axis: Error count (0 to 10).
 - X-axis: Time (2017-01 to 2017-02).
 - Graph: A blue line chart showing error counts fluctuating between 2 and 5.
- Panel 4: Top Deployments (container count)**
 - Y-axis: Container count (0 to 1000).
 - X-axis: Deployment names (kafka, redis, etcd, metrics-server, kubelet).
 - Chart: A horizontal bar chart where all four deployments have a count of 1000.
- Panel 5: Top Namespaces (container count)**
 - Y-axis: Container count (0 to 1000).
 - X-axis: Namespace names (kafka, redis, etcd, metrics-server, kubelet).
 - Chart: A horizontal bar chart where all five namespaces have a count of 1000.
- Panel 6: Pod Container Results by Deployment**
 - Text: "No data available! There is no data for this panel."
- Panel 7: Top Pods: CPU %**
 - Y-axis: CPU usage percentage (0 to 100 %).
 - X-axis: Pod names (kafka-0, kafka-1, kafka-2, kafka-3, redis-0, redis-1, etcd-0, etcd-1, metrics-server-0, kubelet-0, kubelet-1, kubelet-2, kubelet-3).
 - Chart: A horizontal bar chart showing CPU usage for each pod, with values ranging from 0% to approximately 10%.
- Panel 8: Top Pods: Memory Usage**
 - Y-axis: Memory usage percentage (0 to 100 %).
 - X-axis: Pod names (kafka-0, kafka-1, kafka-2, kafka-3, redis-0, redis-1, etcd-0, etcd-1, metrics-server-0, kubelet-0, kubelet-1, kubelet-2, kubelet-3).
 - Chart: A horizontal bar chart showing memory usage for each pod, with values ranging from 0% to approximately 30%.
- Panel 9: Top Pods: File System %**
 - Y-axis: File system usage percentage (0 to 100 %).
 - X-axis: Pod names (kafka-0, kafka-1, kafka-2, kafka-3, redis-0, redis-1, etcd-0, etcd-1, metrics-server-0, kubelet-0, kubelet-1, kubelet-2, kubelet-3).
 - Chart: A horizontal bar chart showing file system usage for each pod, with values ranging from 0% to approximately 10%.

The screenshot shows a log search interface with the following details:

- Log Search Bar:** All Tags, All Sources, All Apps, All Levels.
- Left Sidebar:** Includes sections for Dashboards, Metrics, Logs, Metrics, Functions, and Data Sources. The "Logs" section is currently selected.
- Log Results:** A large list of log entries. Each entry includes a timestamp (e.g., 2023-05-10T12:00:00Z), a source ID (e.g., /subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/rg-test/providers/Microsoft.Web/sites/testapp), and a log message. The log messages are truncated for brevity.

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

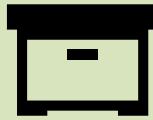


Cross Region offering with all-inclusive pricing, no additional charges for multiple regions

Cloud Data Use Cases



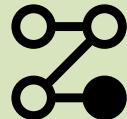
Backup



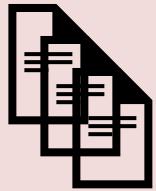
Archive



NAS to Cloud



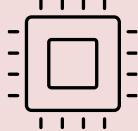
Migration



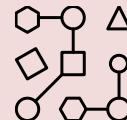
Content Management



Cloud Native



Modern Apps/ IoT/ SaaS



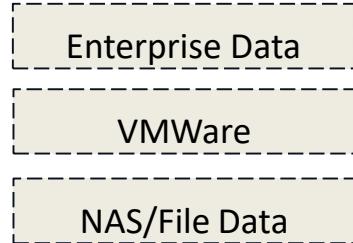
Analytics

Why Cloud Data Services

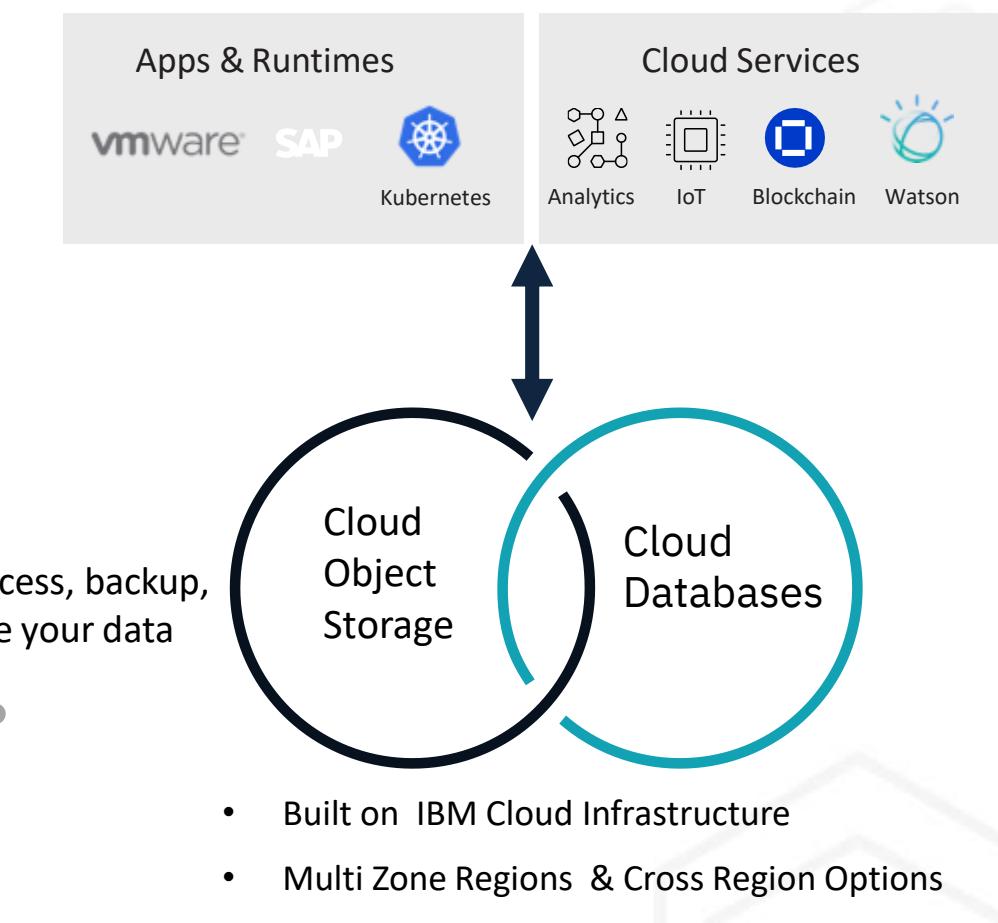
Secure resilient data storage destination for on prem to cloud and cloud native workloads



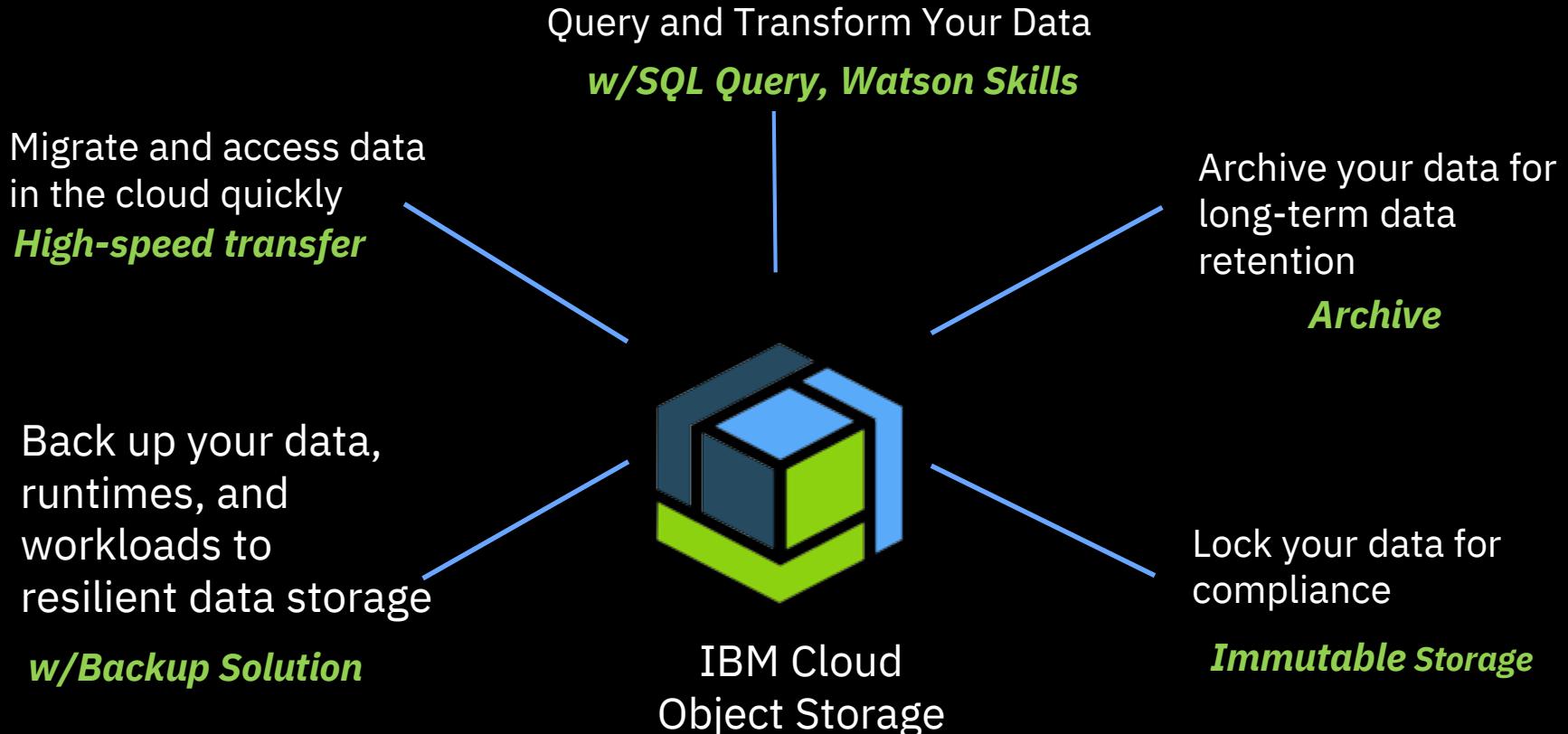
On-Premises



Store, access, backup,
& archive your data



Cloud Object Storage Data Flow



Flexible storage tiers

Predictable and consistent
data access pattern



Standard
(Active)



Vault
(Less Active)



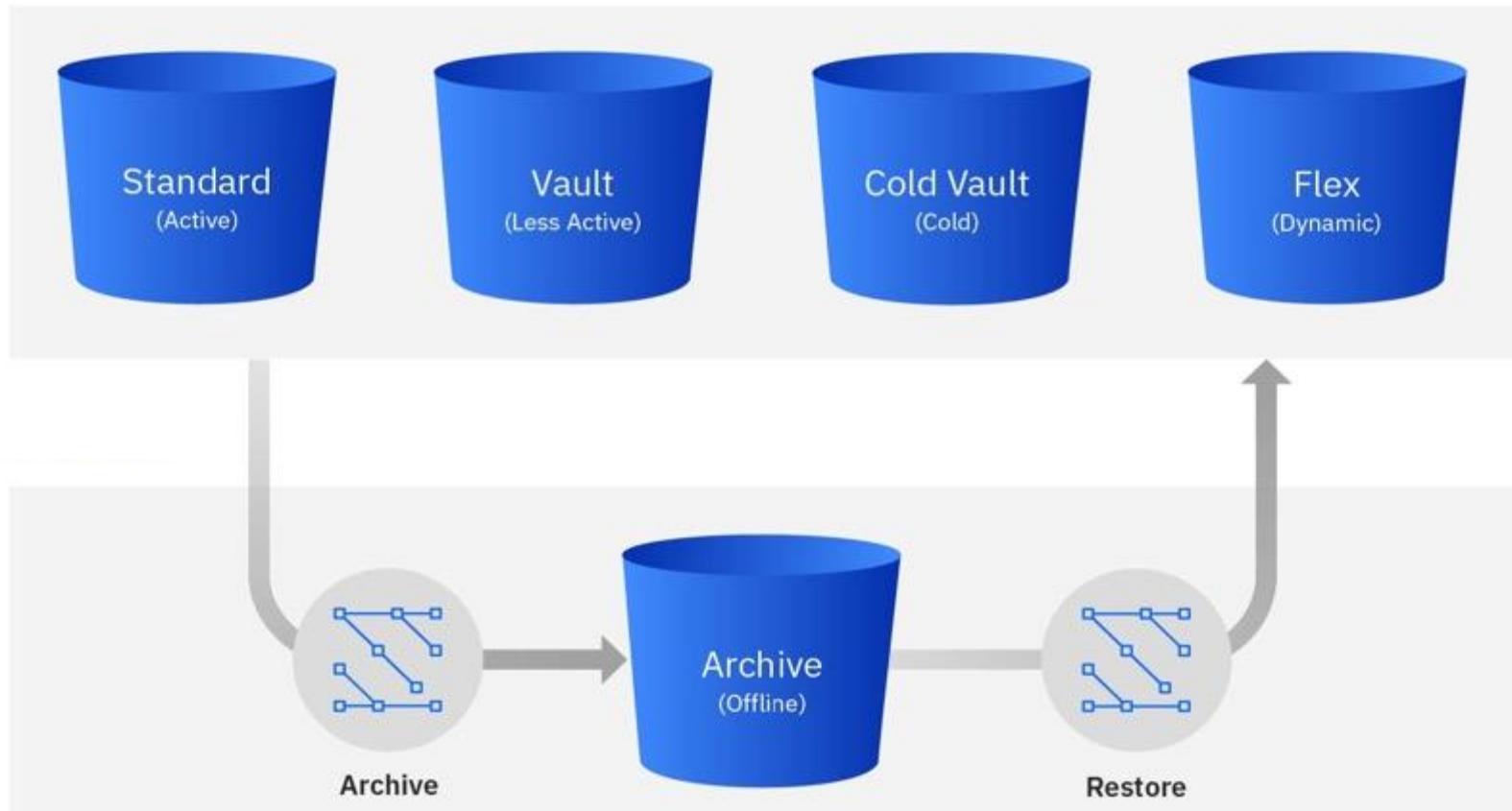
Cold Vault
(Cold)

Unpredictable
or variable data
access pattern



Flex
(Dynamic)

Low cost Archive for Long Term Data Retention

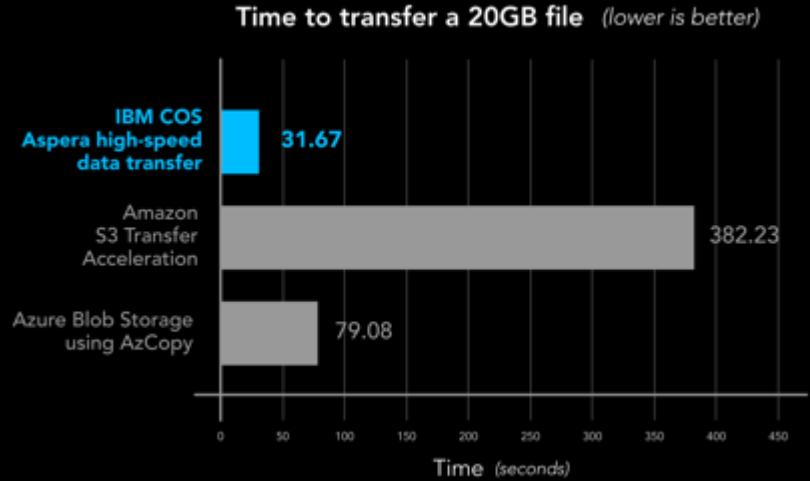


Cloud Object Storage: Aspera high-speed transfer

- 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



Designed to protect
data and maintain
availability



Multi Zone Regions and
Cross Regional worldwide
locations



Redundant
network paths and
redundant system
components

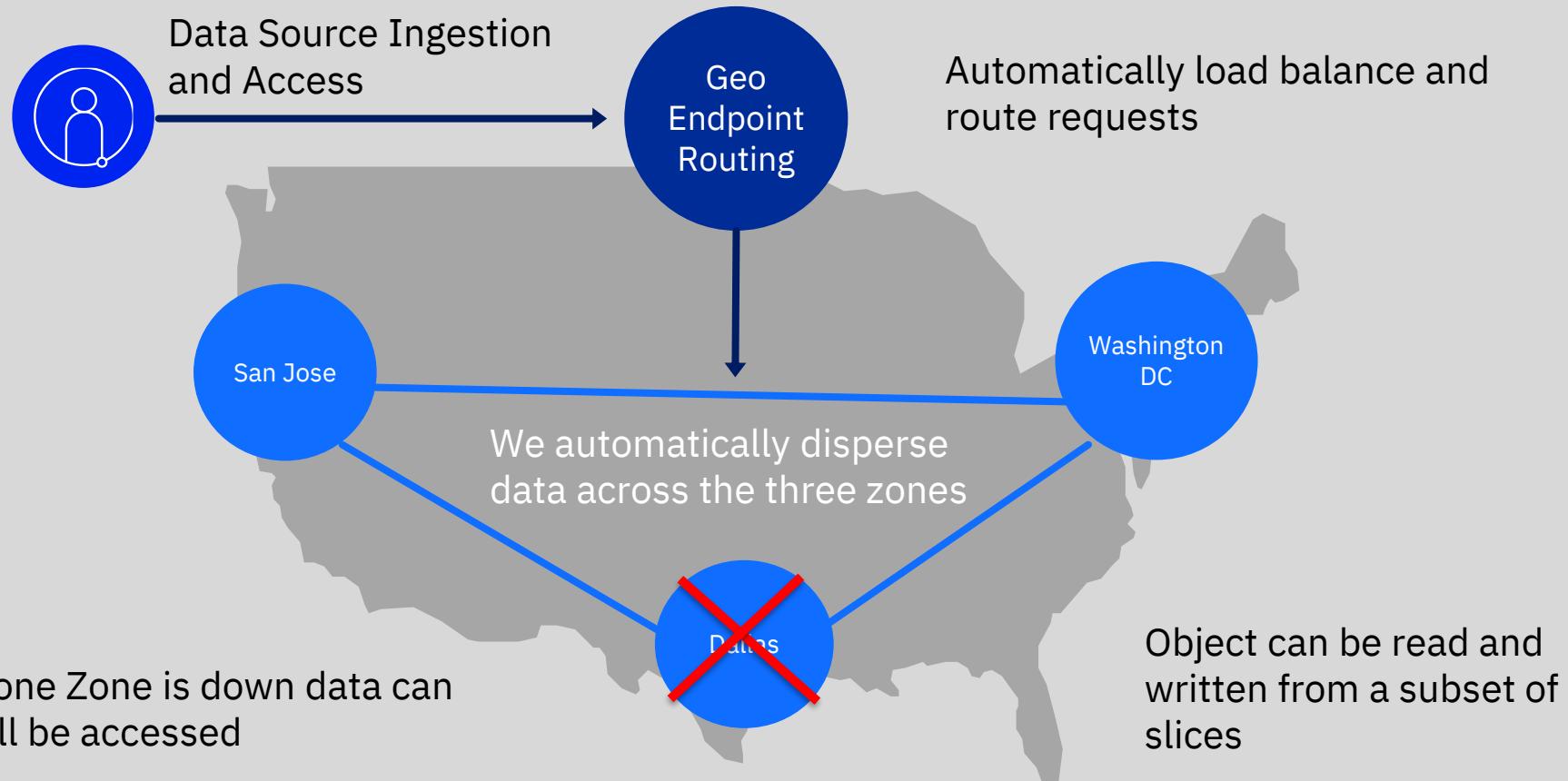


Storage flexibility
with storage tiers
and Archive



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

Cross Region Resiliency



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

120

* New 2019 locations highlighted *

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



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

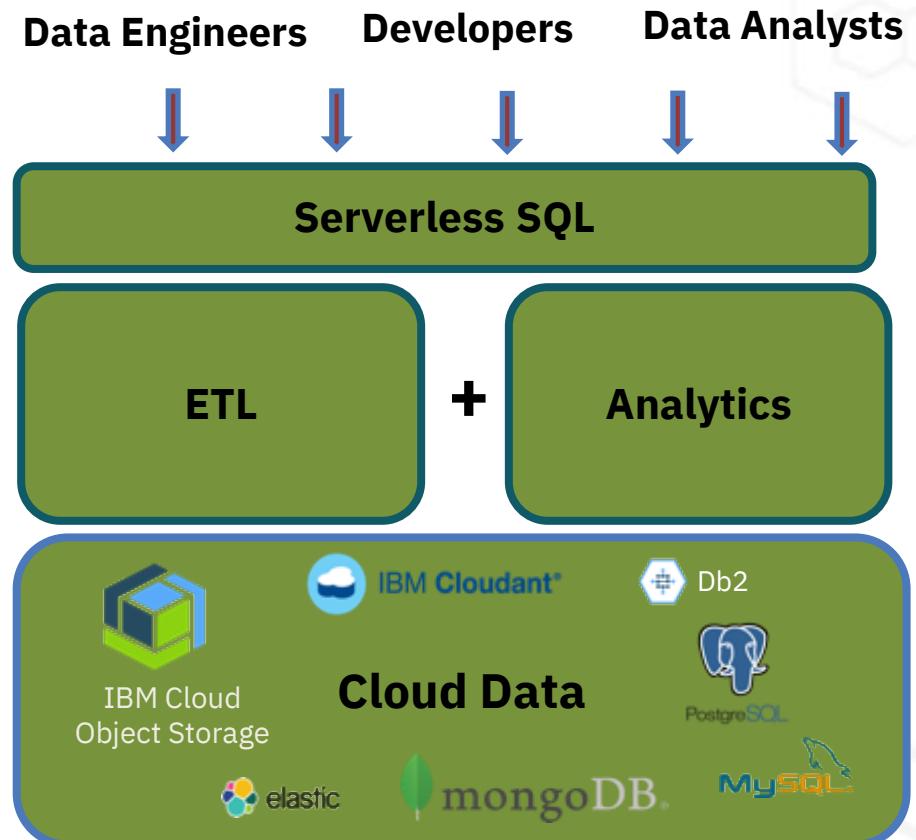


BLOCKCHAIN

CONTAINER
REGISTRYINTERNET 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

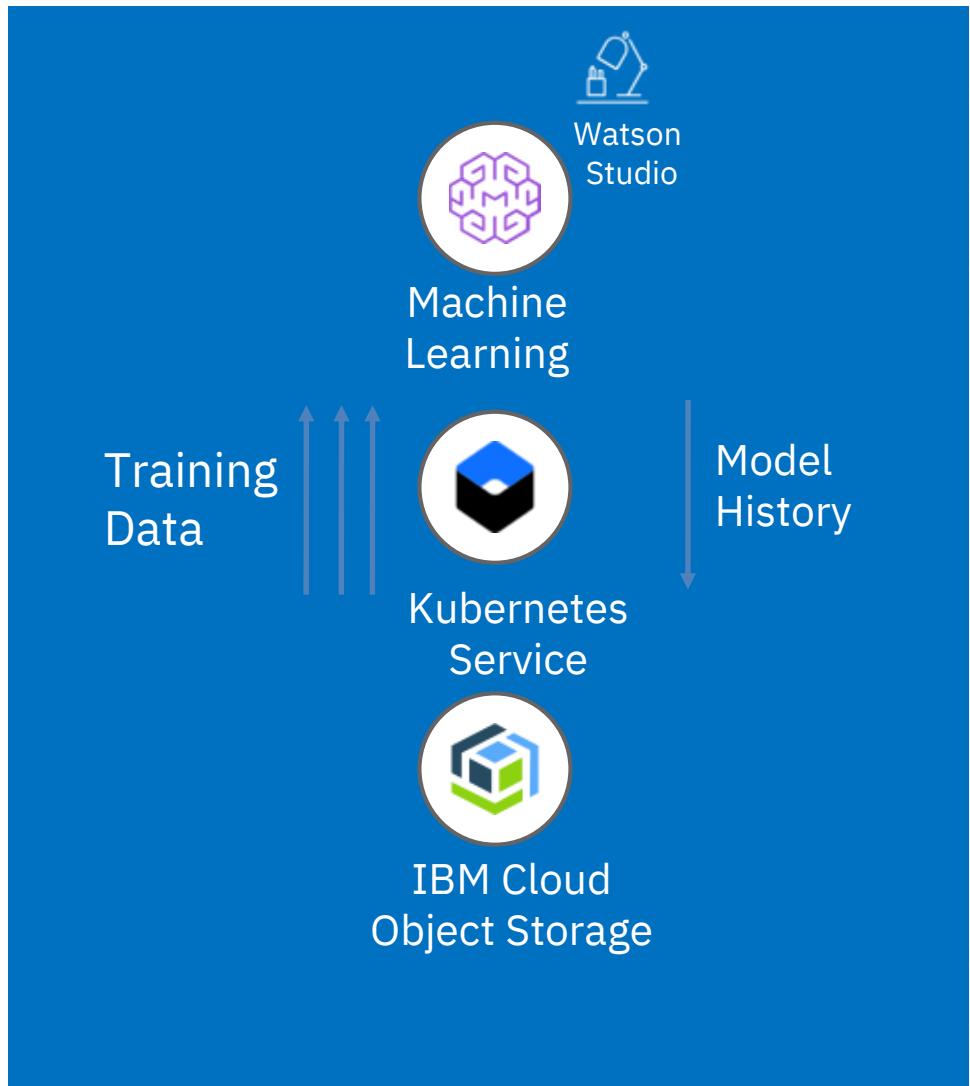


Apply advanced AI

Cloud Object Storage

Directly learn from data in Cloud Object Storage

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





2019 IBM Cloud
用戶實作課程 冬季班

THANK YOU

