Platform and Infrastructure Security for CCSP®

Primary Cloud Platform and Infrastructure Services

Dr. Lyron H. Andrews
CISSP/CCSP/SSCP/CRISC/CISM/CCSK

www.linkedin.com/in/drlyronhandrews/

Overview

- **Enumerate the primary services of cloud computing and use**
- **Analyze risks associated with cloud platform and infrastructure**
- **Discuss mitigation strategies to reduce risks to cloud computing**

CCSP Certification Examination

Domains	Weights
1. Cloud Concepts, Architecture and Design	17%
2. Cloud Data Security	20%
3. Cloud Platform and Infrastructure Security	17%
4. Cloud Application Security	17%
5. Cloud Security Operations	16%
6. Legal, Risk and Compliance 13%	13%

Cloud Service Descriptions

BRROM

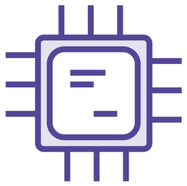
“Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

-NIST SP-800-145

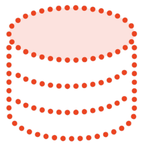
“ (e.g., networks, servers, storage, applications, and services)”
-NIST SP-800-145

Primary Cloud Services

Network



Compute



Storage

Virtualization

Management Plane

Virtualization

Capabilities of Virtualization

Allows for resource pooling of storage, compute, and networking

Allow provider to share underlying resources with multiple tenants

The key virtualization mechanism in cloud is the hypervisor

Two Types of Hypervisor

Type II

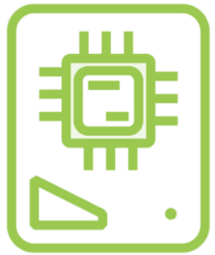
OS or hosted application hypervisor

Type I

Modern cloud hypervisor

Type I Hypervisor

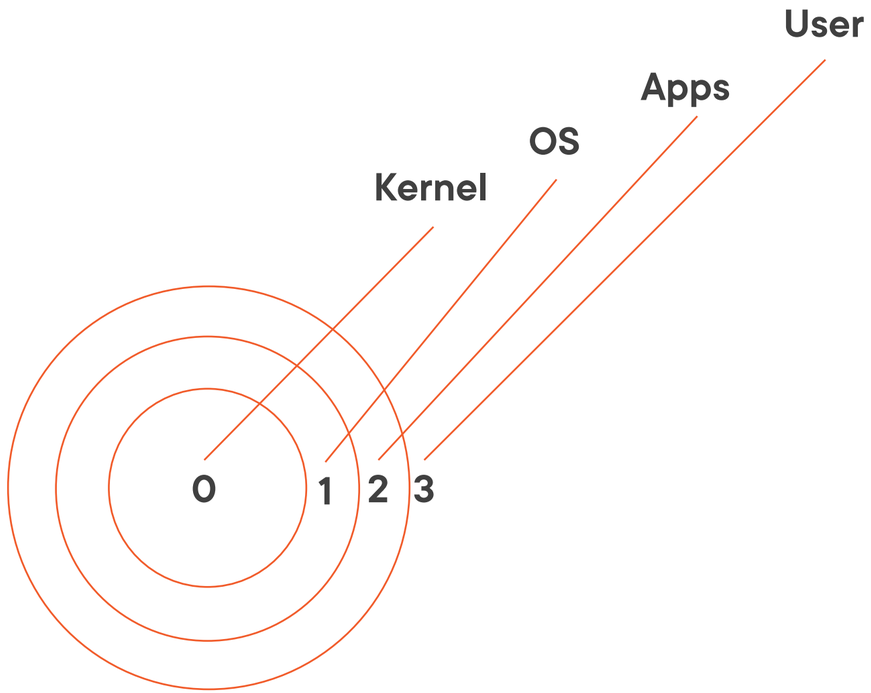
Bare-metal, embedded, or native



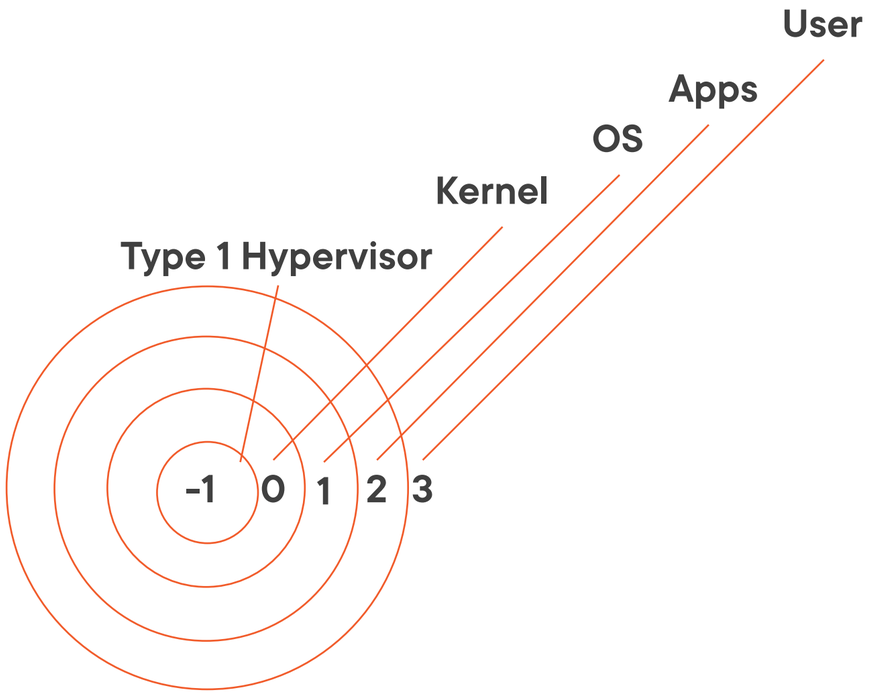
Work directly on hardware

Small form factor; few hundred megabytes

Type I Hypervisor (Continued)



Traditional OS

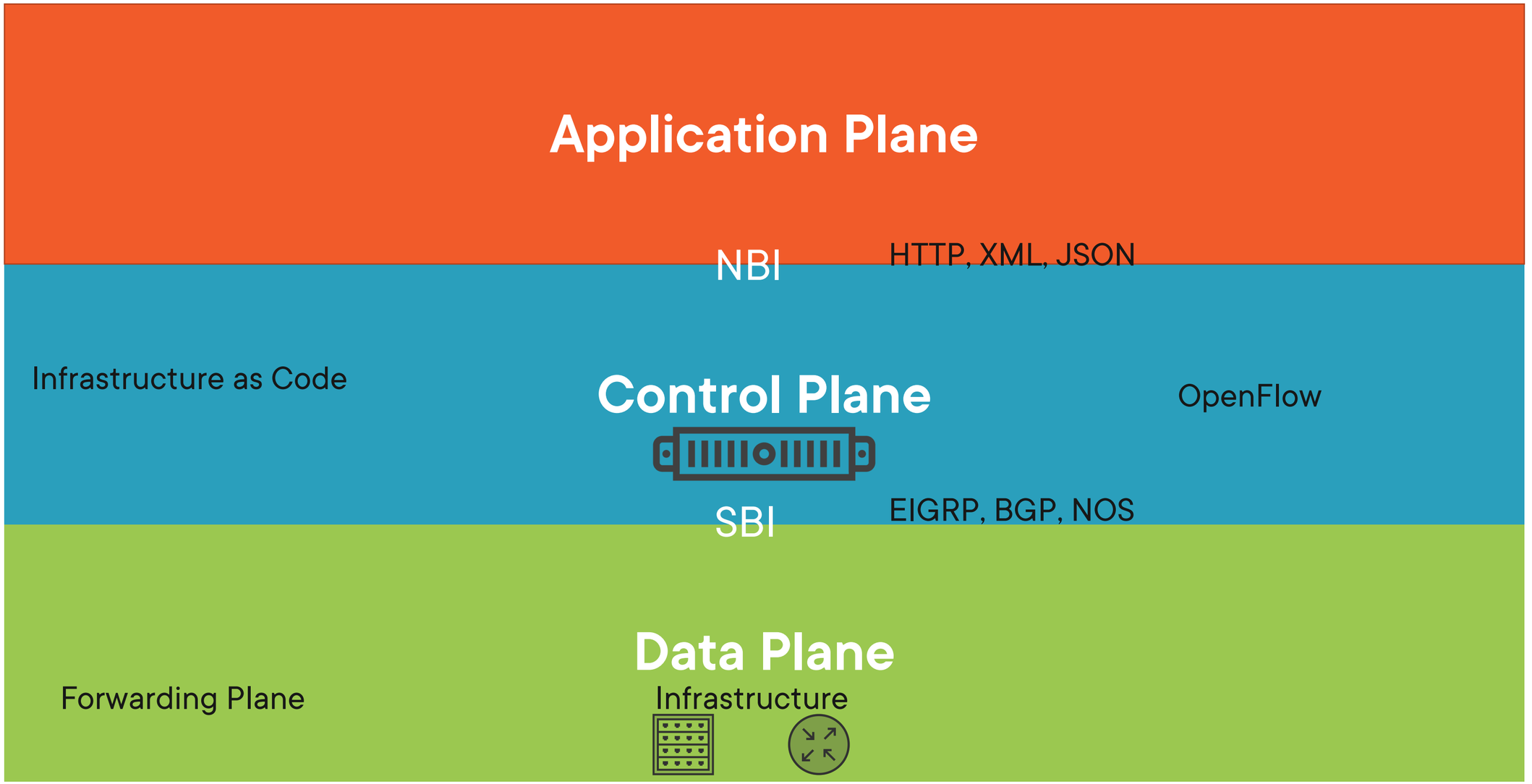


Type I Hypervisor

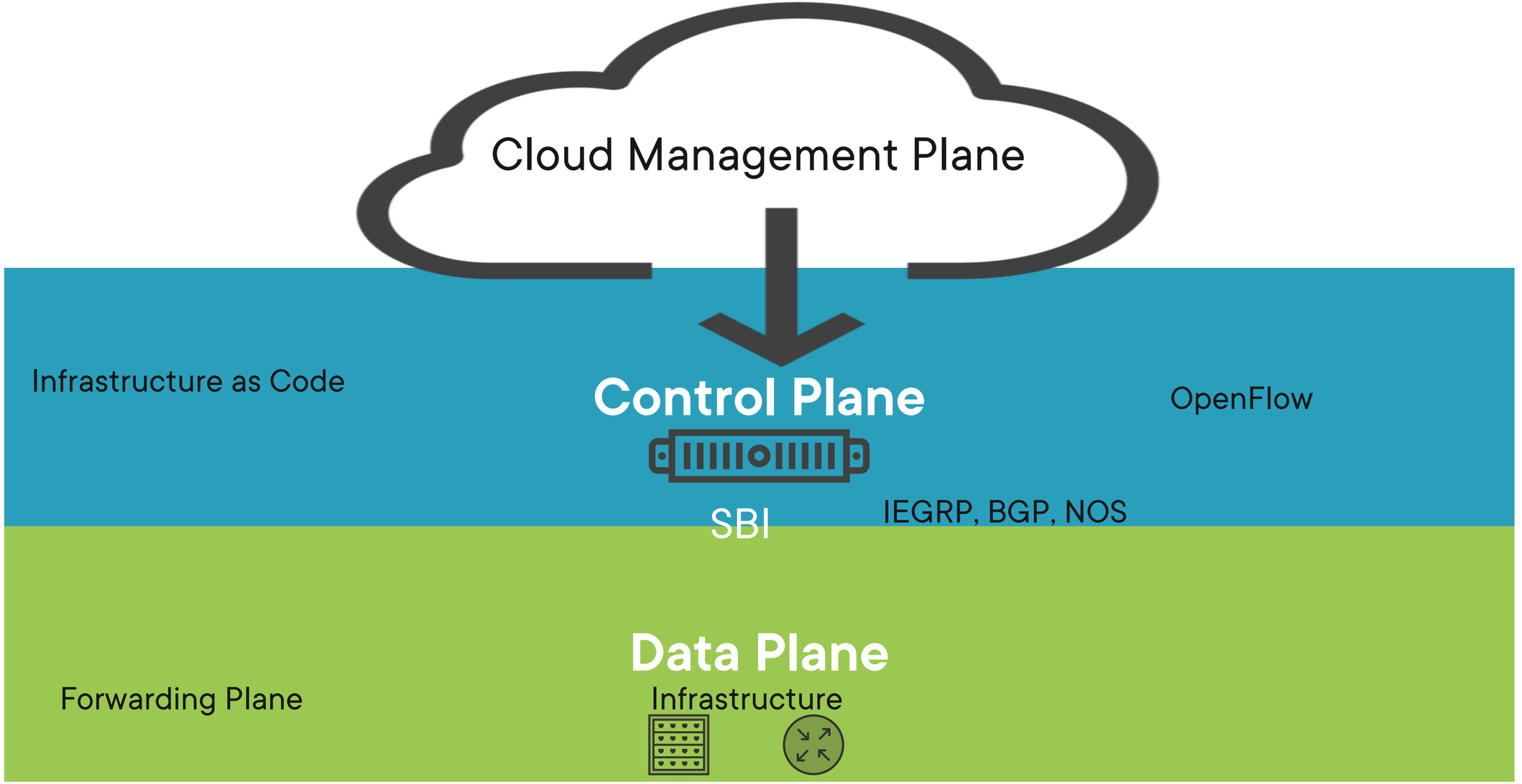
Software Defined Network and Network Function Virtualization

SDN did not begin with what is now considered NFV. Implementations of SDN are replacing MPLS.

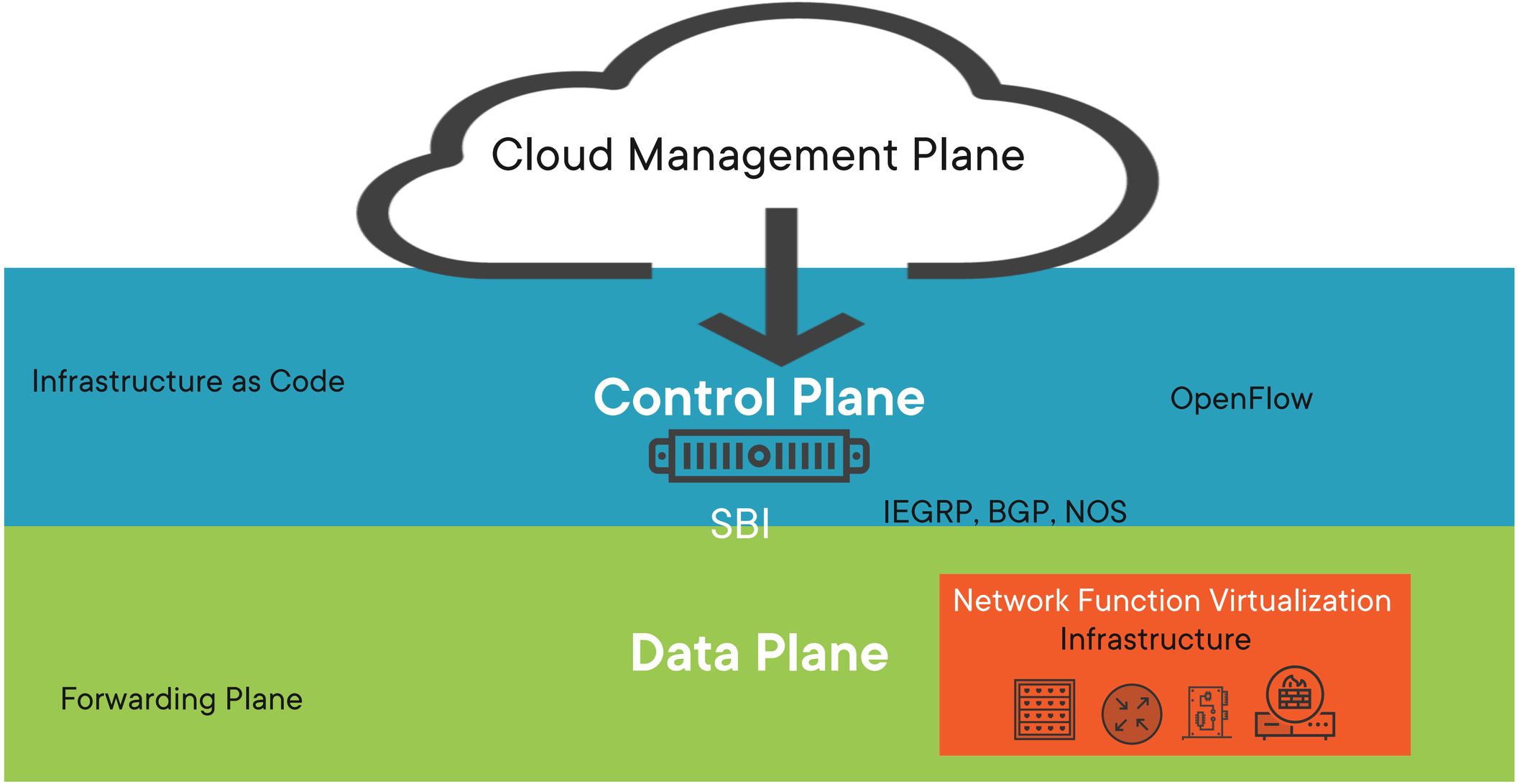
The Planes of SDN



The Planes of SDN



The Planes of SDN



Compute Services

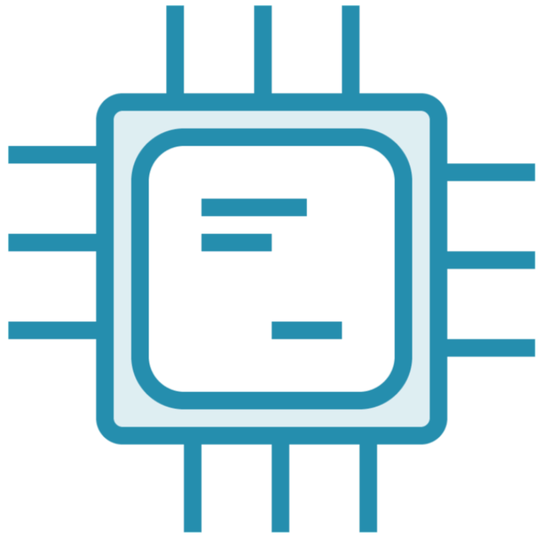
Provider Management of Compute

Reservations

Limits

Shares

Two Elements of Compute



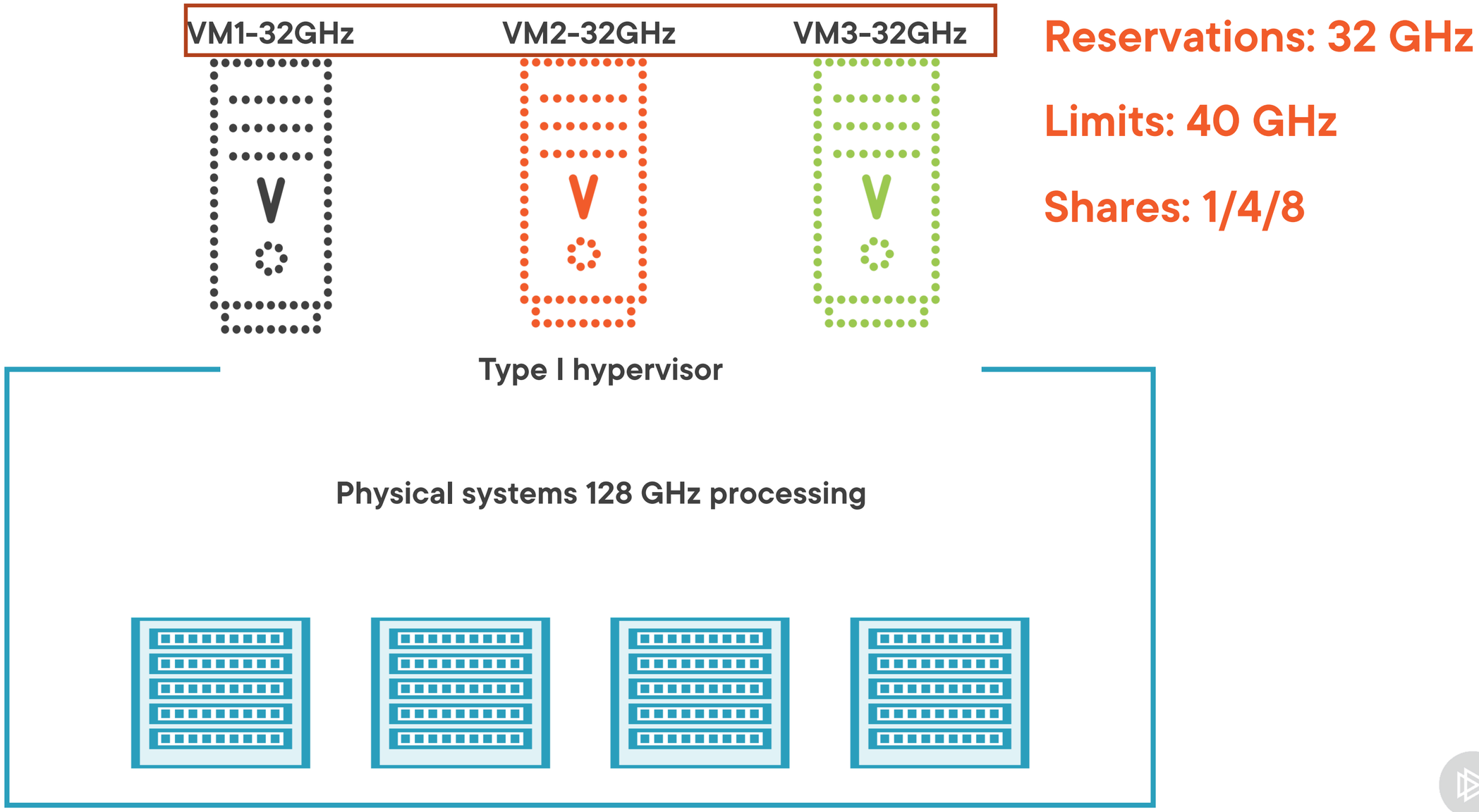
Number of CPUs

Processing power expressed in hertz

Amount of memory

Space expressed in bytes

Provider Compute Management



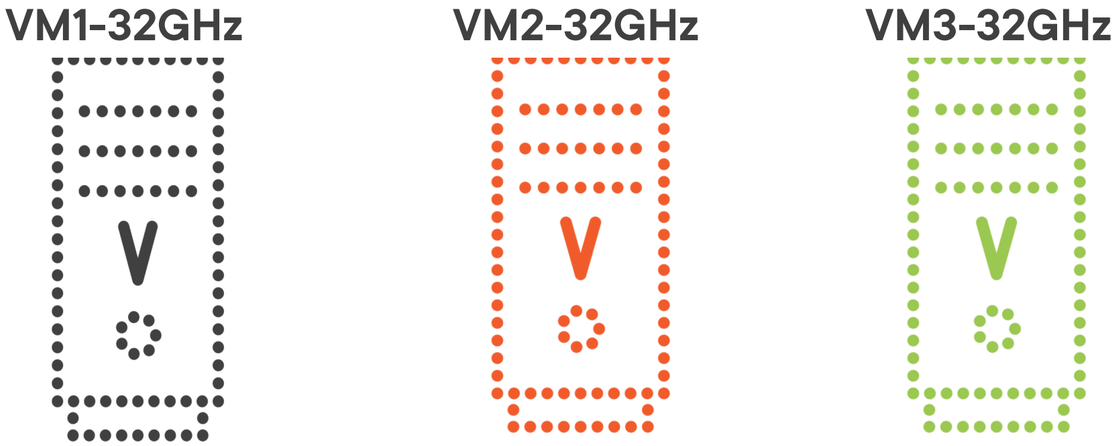
Reservations: 32 GHz

Limits: 40 GHz

Shares: 1/4/8

Provider Compute Management

Shares: 1 | 4 | 8



Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.

Filter by: All instance families | Current generation | Show/Hide Columns

Currently selected: t2.micro (- ECUs, 1 vCPUs, 2.5 GHz, -, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
☐	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
☑	t2	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
☐	t2	t2.small	1	2	EBS only	-	Low to Moderate	Yes
☐	t2	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
☐	t2	t2.large	2	8	EBS only	-	Low to Moderate	Yes
☐	t2	t2.xlarge	4	16	EBS only	-	Moderate	Yes
☐	t2	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
☐	t3	t3.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes

Cancel | Previous | Review and Launch | Next: Configure Instance Details

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.

Filter by: All instance families | Current generation | Show/Hide Columns

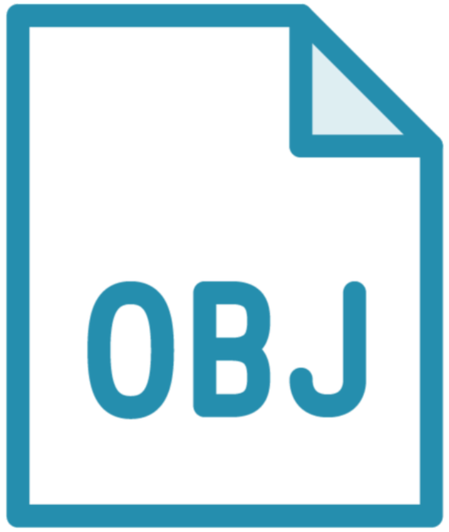
Currently selected: t2.micro (- ECUs, 1 vCPUs, 2.5 GHz, -, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
☐	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
☑	t2	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
☐	t2	t2.small	1	2	EBS only	-	Low to Moderate	Yes
☐	t2	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
☐	t2	t2.large	2	8	EBS only	-	Low to Moderate	Yes
☐	t2	t2.xlarge	4	16	EBS only	-	Moderate	Yes
☐	t2	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
☐	t3	t3.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes

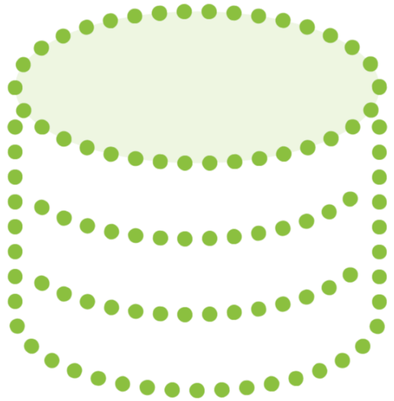
Cancel | Previous | Review and Launch | Next: Configure Instance Details

Storage Services

Basic Storage



Object Storage
Inclusive of files



Volume Storage
Based upon blocks

Primary Cloud Provider's Storage Options

Block	Object
AWS EBS	AWS S3
Google Cloud Persistent Disks	Google Cloud Storage
Azure Disks	Azure Blobs

Volume Storage and Blocks

Compute

SSD/HDD

65536	65536	65536	65536	65536
65536	65536	65536	65536	65536
65536	65536	65536	65536	65536

1. Choose AMI | 2. Choose Instance Type | 3. Configure Instance | **4. Add Storage** | 5. Add Tags | 6. Configure Security Group | 7. Review

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/xvda	snap-06855577a362ab2a4	8	General Purpose SSD (gp2)	100 / 3000	N/A	☑	Not Encrypted

Add New Volume

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.

Shared file systems

You currently don't have any file systems on this instance. Select "Add file system" button below to add a file system.

Add file system

Cancel | Previous | Review and Launch | Next: Add Tags

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/xvda	snap-06855577a362ab2a4	8	General Purpose SSD (gp2)	100 / 3000	N/A	☑	Not Encrypted

Add New Volume

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.

Shared file systems

You currently don't have any file systems on this instance. Select "Add file system" button below to add a file system.

Add file system

1. Choose AMI | 2. Choose Instance Type | 3. Configure Instance | **4. Add Storage** | 5. Add Tags | 6. Configure Security Group | 7. Review

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/xvda	snap-06855577a362ab2a4	8	General Purpose SSD (gp2)	100 / 3000	N/A	☑	Not Encrypted

General Purpose SSD (gp2)
General Purpose SSD (gp3)
Provisioned IOPS SSD (io1)
Provisioned IOPS SSD (io2)
Magnetic (standard)

Add New Volume

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.

Shared file systems

You currently don't have any file systems on this instance. Select "Add file system" button below to add a file system.

Add file system

Cancel | Previous | Review and Launch | Next: Add Tags

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/xvda	snap-06855577a362ab2a4	8	General Purpose SSD (gp2)	100 / 3000	N/A	☑	Not Encrypted

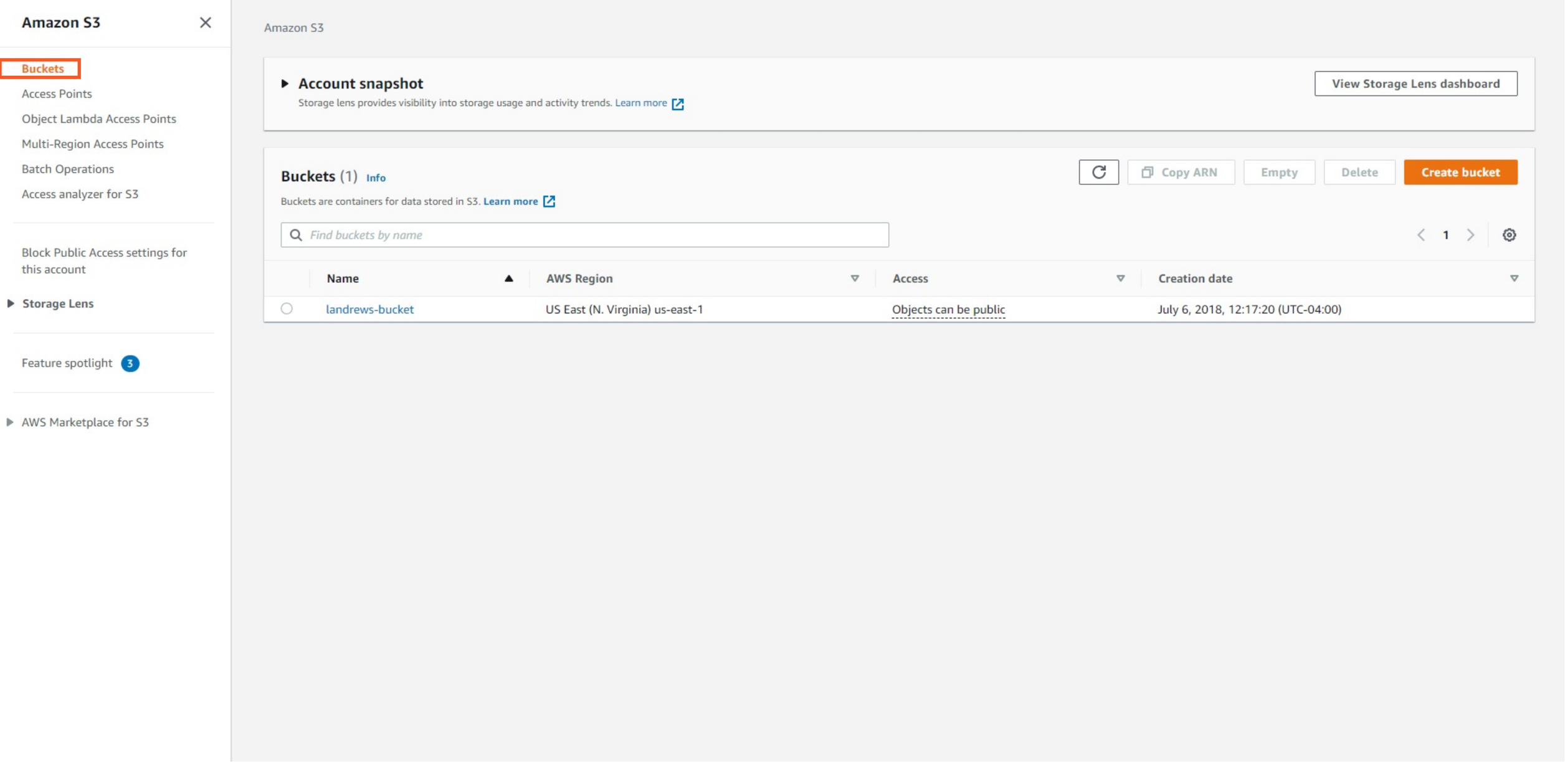
Add New Volume

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.

Shared file systems

You currently don't have any file systems on this instance. Select "Add file system" button below to add a file system.

Add file system



Object storage example

landrews-bucket Info

Amazon S3

Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
Access analyzer for S3

Block Public Access settings for this account

Storage Lens

Feature spotlight 3

AWS Marketplace for S3

Objects | Properties | Permissions | Metrics | Management | Access Points

Objects (3)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Copy S3 URI | Copy URL | Download | Open | Delete | Actions | Create folder | Upload

Find objects by prefix

Show versions

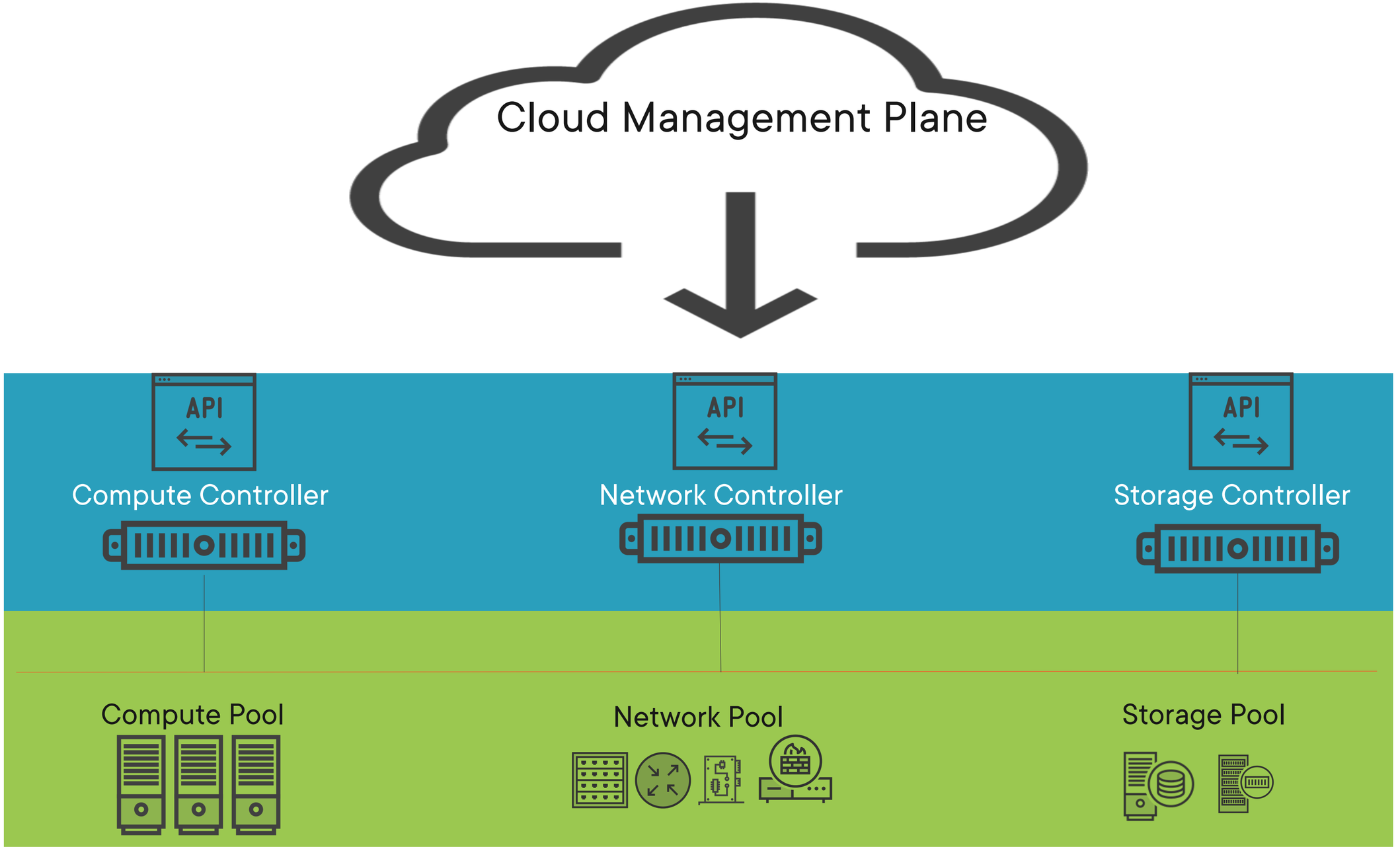
1

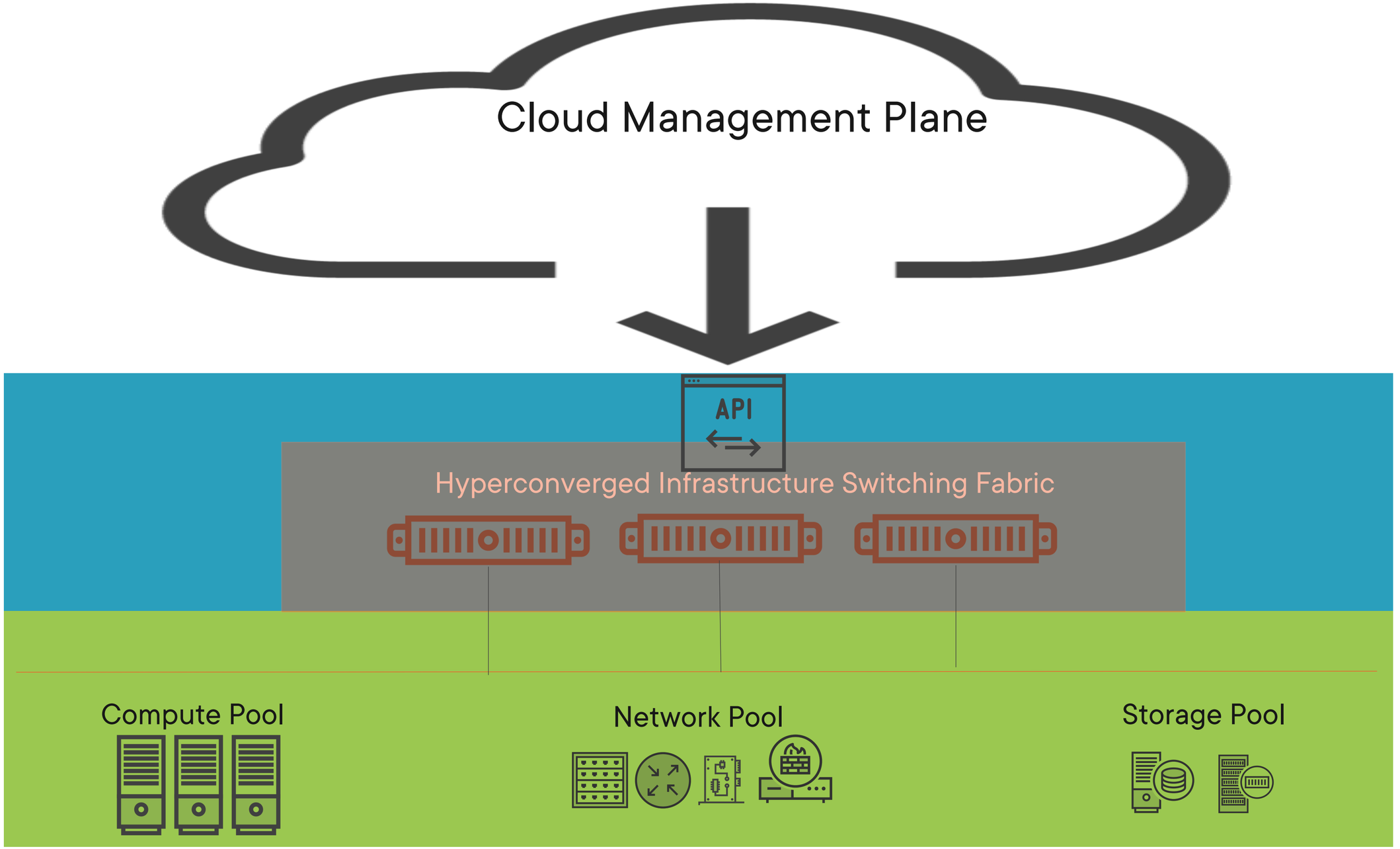
Name	Type	Last modified	Size	Storage class
_Activities.docx	docx	January 26, 2022, 04:17:01 (UTC-05:00)	19.2 KB	Standard
AWSLogs/	Folder	-	-	-
hello.txt	txt	July 6, 2018, 14:54:13 (UTC-04:00)	36.0 B	Standard

Management Plane

Cloud Management Platform Features

- **API integration and consumption**
- **Automation and orchestration**
- **Role-based security**
- **Key management and encryption**
- **Configuration management**
- **Service catalog**
- **Workload provisioning and isolation**


Cloud Management Plane
API
Compute Controller
API
Network Controller
API
Storage Controller
Compute Pool
Network Pool
Storage Pool


Cloud Management Plane
API
Hyperconverged Infrastructure Switching Fabric
Compute Pool
Network Pool
Storage Pool

Cloud Computing Risks

Application and Interface Security

Change Control and Configuration

Data Security and Information Lifecycle Management

Encryption and Key Management

Data Breaches

Application and Interface Security

Change Control and Configuration

Identity and Access Management

Human Resources

Infrastructure and Virtualization Security

Misconfiguration-Inadequate Change Control

Governance and Risk Management

Identity and Access Management

Infrastructure and Virtualization Security

Supply Chain Management, Transparency and Accountability

Lack of Cloud Security Architecture and Strategy

Business Continuity Management and Operational Resilience

Identity and Access Management

Infrastructure and Virtualization Security

Security Incident Management, E-Discovery and Cloud Forensics

Account Hijacking

Identity and Access Management

Encryption and Key Management

Human Resources

Insufficient Identity, Credential, Access and Key Management

Datacenter Security

Data Security and Information Lifecycle Management

Identity and Access Management

Encryption and Key Management

Human Resources

Insider Threat

Application and Interface Security

Identity and Access Management

Insecure Interfaces and APIs

Application and Interface Security

Audit Assurance and Compliance

Business Continuity Management and Operational Resilience

Governance and Risk Management

Weak Control Plane

Cloud Virtualization Risks and Remediation

Virtualization Risk

Vulnerability	Threat
Security Flaws in hypervisor	Guest escape/hyper jacking/VM hopping
Inadequate granularity of controls	Administrative, physical, technical
Oversubscription	VM starved of resource

Major Cloud Provider's Hypervisors

Amazon Web Service

Xen and Nitro

Google Cloud Platform

KVM

Azure

Windows Hyper-V

Amazon Web Services Nitro Security

Nitro Enclaves

NitroTPM

Secure cryptography

Security Governance

Google Cloud KVM Security

Vulnerability search	**Non-QEMU**	**Cryptographic communication**
Code provenance	**Rapid response**	**Policy-based releases**

Azure Hyper-V Security

Isolation

Host-based

Virtualization-based

Integrity of user/kernel mode

Exploit mitigation

ASLR and DEP

Automation

Stack variable

Zero-initialize

Block injections

SaaS, PaaS, and IaaS Risks

Unauthorized workloads initiated

East-West movement of APTs

Improperly trained staff

Application built without security-by-design

Insufficient due-diligence and inadequate granularity of controls

Shadow IT

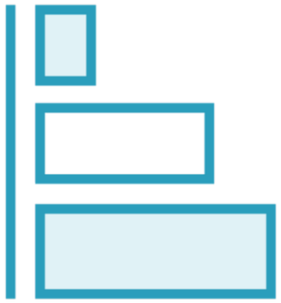
“86% of the compromised Google Cloud instances were used to perform cryptocurrency mining, a cloud resource-intensive for-profit activity. Malicious actors gained access to the Google Cloud instances by taking advantage of poor customer security practices or vulnerable third-party software in nearly 75% of all cases”.

Google-Cloud Threat Intelligence, November 2021. Issue 1

Reduce blast radius of attack by means of implementing zero trust architecture. This includes explicit allowance to resources, micro-segmentation, and telemetry monitoring.

Zero – Trust Cloud Architecture

Five Steps to Zero Trust



Define protect surface

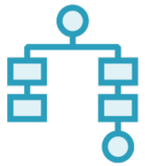
Map transaction flows

Architect Zero Trust Network

Create Zero Trust policy

Monitor and maintain network

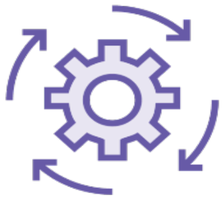
1 - Define Protect Surface



Data – Protected information through regulation and law

Applications – developed and acquired

Assets – systems under management



Services – connectivity protocols

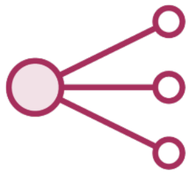
2 - Map Transaction Flows

Determine the critical path of DAAS

Acceptable to begin with approximation

Iteration brings more clarity and granularity

3 - Architect Zero Trust Network



Reference architecture bespoke for business

Granular layer 7 protect surface

Application, user, and content ID management

“I keep six honest serving-men

(They taught me all I knew);

Their names are What and Why and When

And How and Where and Who.

Rudyard Kipling

Just So Stories, 1902

4 - Zero Trust Policy

WHO is asserted ID?

WHAT is accessed on protect surface?

WHEN is asserted ID accessing?

WHERE is destination?

WHY is asserted ID attempting access?

HOW is asserted ID accessing?

5 - Monitor and Maintain

Continue to analyze and evaluate logs

More telemetry data better than less

Promote and investigate User/Entity Behavior Analytics (UBEA)

Summary

Can you describe the separation in capabilities between traditional and cloud computing?

What risks to cloud computing is most important for you to begin mitigating?

Where on the journey to zero-trust are you?

Up Next:
Secure Data Center Design and Supporting Controls