Lesson 15

Implementing Secure Cloud Solutions

Topic 15A

Summarize Secure Cloud and Virtualization Services

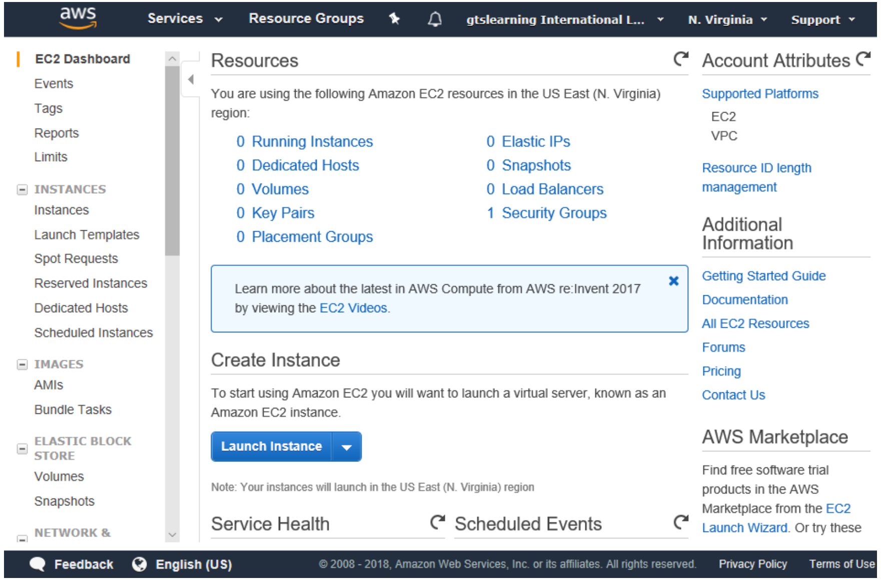
Syllabus Objectives Covered

- 2.2 Summarize virtualization and cloud computing concepts

Cloud Deployment Models

- Public (multi-tenant)
    - Cloud service providers (CSPs)
    - Shared between subscribers
    - Multi-cloud
- Hosted private
    - Private instance operated by a CSP but dedicated to a single customer
- Private
    - Wholly owned and operated by the organization
    - On-premises vs. off-premises
- Community
- Hybrid

Cloud Service Models



Resources

You are using the following Amazon EC2 resources in the US East (N. Virginia) region:

0 Running Instances	0 Elastic IPs
0 Dedicated Hosts	0 Snapshots
0 Volumes	0 Load Balancers
0 Key Pairs	1 Security Groups
0 Placement Groups	

Learn more about the latest in AWS Compute from AWS re:Invent 2017 by viewing the EC2 Videos.

Create Instance

To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.

Note: Your instances will launch in the US East (N. Virginia) region

Service Health

Scheduled Events

Account Attributes

Supported Platforms
EC2
VPC

Resource ID length management

Additional Information

Getting Started Guide
Documentation
All EC2 Resources
Forums
Pricing
Contact Us

AWS Marketplace

Find free software trial products in the AWS Marketplace from the EC2 Launch Wizard. Or try these

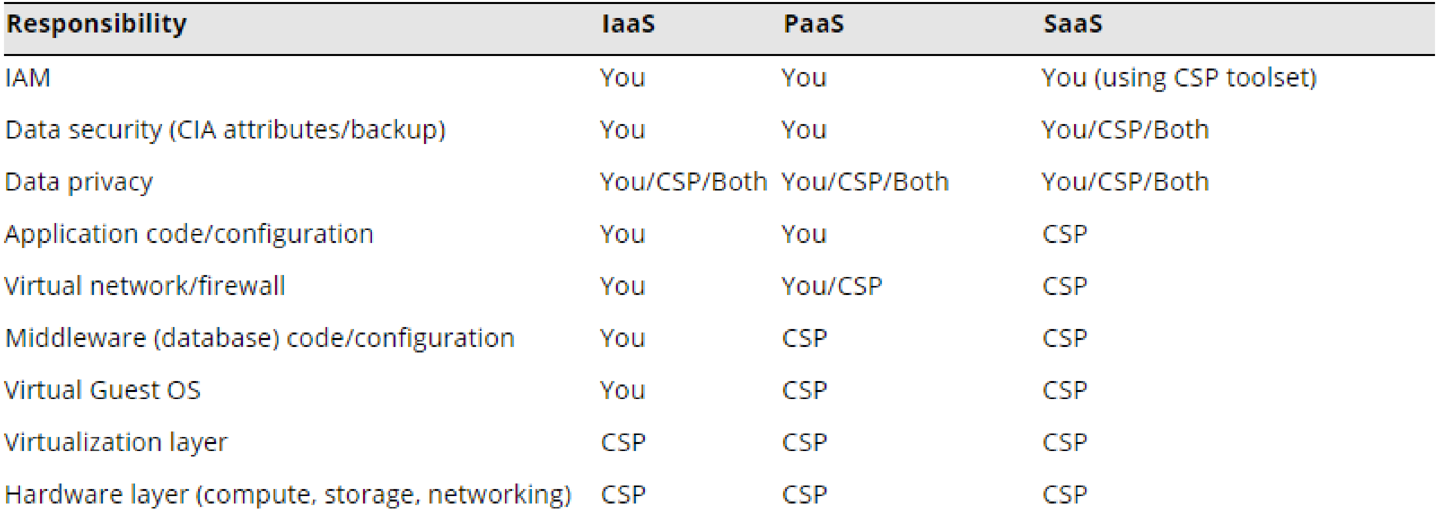
© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Screenshot used with permission from Amazon.com.

- Anything as a service (XaaS)
- Infrastructure as a Service (IaaS)
  - Unconfigured compute, storage, and network resources
- Software as a Service (SaaS)
  - Fully developed applications
- Platform as a Service (PaaS)
  - Pre-configured OS and database/middleware instances

Anything as a Service

- Specific IaaS, PaaS, or SaaS solutions for business needs
- Security in the cloud
- Security of the cloud
- Cloud responsibility matrix

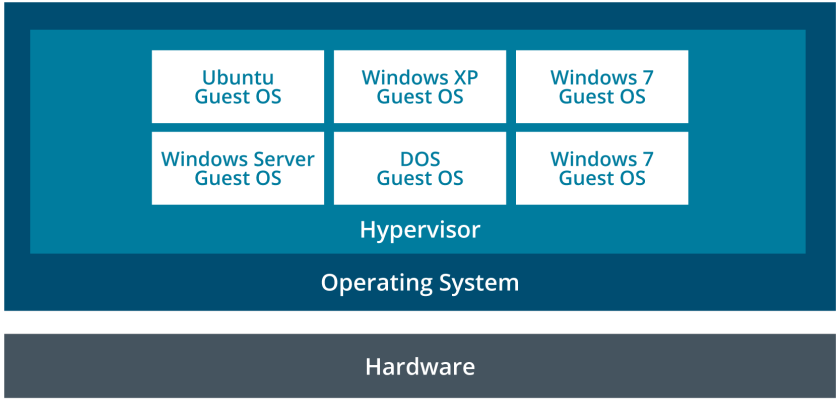


Responsibility	IaaS	PaaS	SaaS
IAM	You	You	You (using CSP toolset)
Data security (CIA attributes/backup)	You	You	You/CSP/Both
Data privacy	You/CSP/Both	You/CSP/Both	You/CSP/Both
Application code/configuration	You	You	CSP
Virtual network/firewall	You	You/CSP	CSP
Middleware (database) code/configuration	You	CSP	CSP
Virtual Guest OS	You	CSP	CSP
Virtualization layer	CSP	CSP	CSP
Hardware layer (compute, storage, networking)	CSP	CSP	CSP

Security as a Service

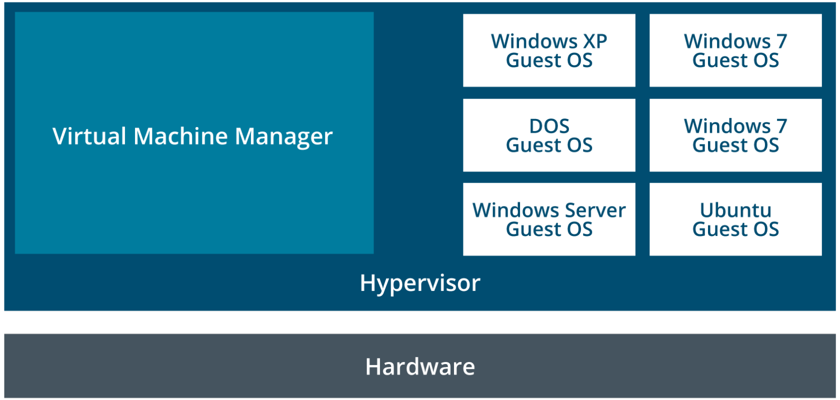
- Consultants
  - Third-party expertise and perspective
- Managed Security Services Provider (MSSP)
  - Turnkey security solutions
- Security as a Service (SECaaS)
  - Cloud-deployed security assessment and analysis
  - Cyber threat intelligence and machine learning analytics

Virtualization Technologies and Hypervisor Types



- Virtualization platform
  - Host hardware
  - Hypervisor/Virtual Machine Monitor (VMM)
  - Guest operating systems, Virtual Machines (VM), or instances

- Type II hypervisors (host-based)
- Type I hypervisors (bare metal)

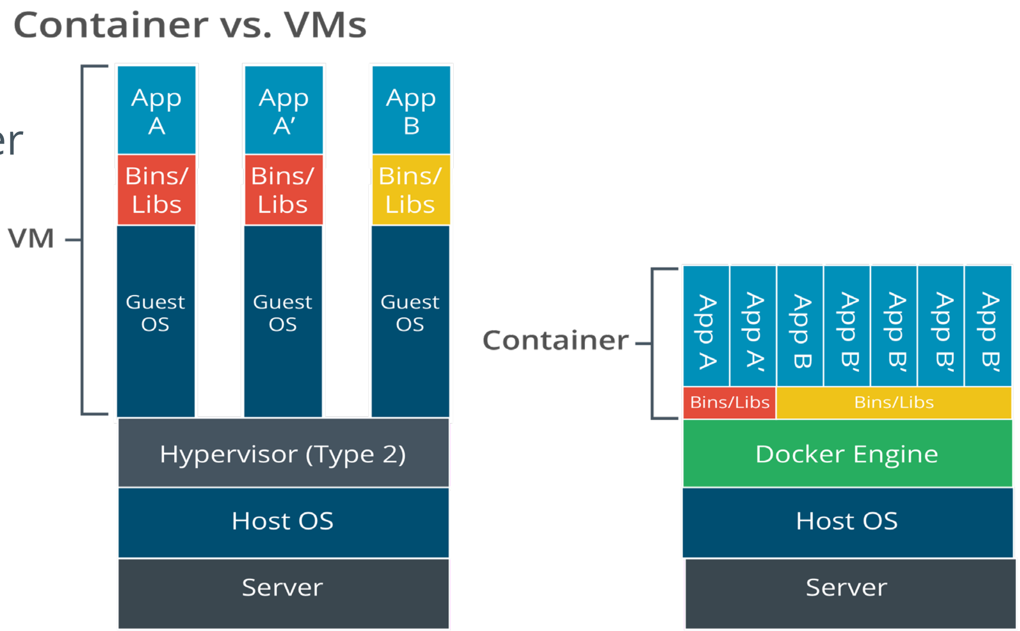


Virtual Desktop Infrastructure and Thin Clients

- Virtual Desktop Infrastructure (VDI)
- Storing images of clients (OS + applications) on a central server
- Virtual Desktop Environment (VDE) images are loaded by thin clients
- Allows for low-power client devices
- Centralizes control over client desktops
- Allows for almost completely hosted IT infrastructure

Application Virtualization and Container Virtualization

- Application virtualization
  - Hosting or streaming individual software applications on a server
  - XenApp, App-V, ThinApp
- Container virtualization (application cells)
  - Resource separation at the OS level
  - Cannot run different OS VMs
  - Docker



VM Escape Protection

- Reduce impact of successful exploits
- Ensure careful placement of VM services on hosts/within network
- Respect security zones (DMZ)

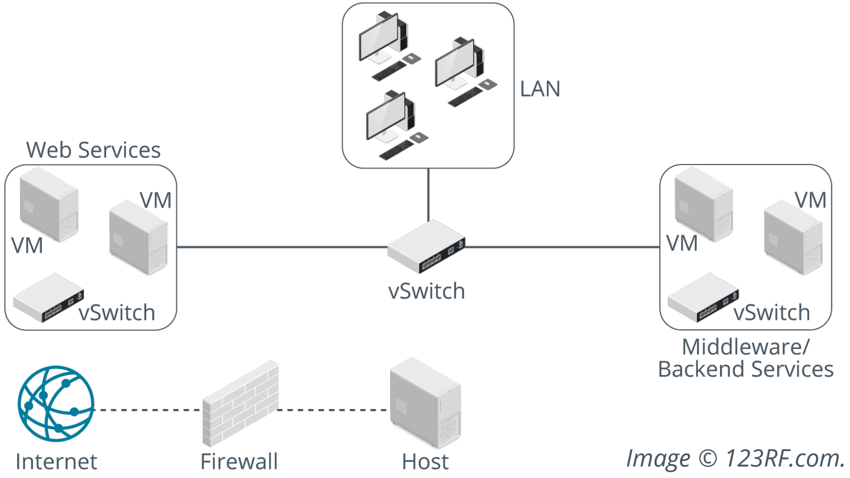
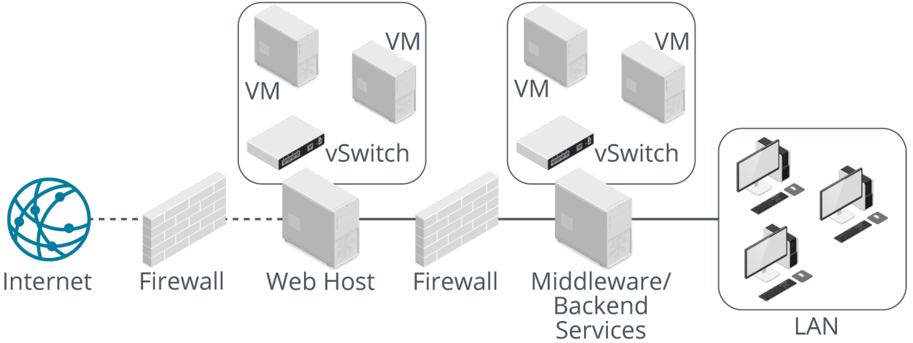


Image © 123RF.com.



Images © 123RF.com.

VM Sprawl Avoidance

- Guest OS security
  - OS environment must still be maintained
- Rogue VMs
  - System sprawl and undocumented assets
  - Virtual machine life cycle management (VMLM)
  - Use template-based VM creation

Topic 15B

Apply Cloud Security Solutions

Syllabus Objectives Covered

- 1.2 Given a scenario, analyze potential indicators to determine the type of attack (Cloud-based versus on-premises only)
- 2.2 Summarize virtualization and cloud computing concepts
- 3.6 Given a scenario, apply cybersecurity solutions to the cloud

Cloud Security Integration and Auditing

- Obtaining and integrating cloud security data
  - Attack indicators and correlation
- Responsibility matrix and SLAs
  - Security of the cloud
  - Security in the cloud
- Reporting
- Legal and compliance responsibilities
- Insider threat

Cloud Security Controls

- Same types of security controls
  - IAM, endpoint protection, resource policies, firewalls, logging, ...
- Cloud native controls vs. third-party solutions
  - CSP web console, CLI, and API
  - Vendor virtual instances
- Application security and IAM
  - Secure development/coding
  - Security accounts/groups/roles
- Secrets management
  - Block use of root account
  - Use MFA for privileged accounts
  - Protect API keys

Cloud Compute Security

- Compute
  - Processing resources for cloud workloads (CPU and RAM)
  - Virtual machines and containers
  - Dynamic resource allocation
- Container security
- API inspection and integration
  - Number of requests
  - Latency
  - Error rates
  - Unauthorized and suspicious endpoints
- Instance awareness
  - Logging and monitoring to mitigate cloud sprawl

Cloud Storage Security

- Storage
  - Persistent storage capacity
  - Performance characteristics for storage tiers
  - Input/output operations per second (IOPS)
- Permissions and resource policies
  - JavaScript Object Notation (JSON)
- Encryption
  - Symmetric media encryption key
  - CSP-managed keys versus customer-managed
  - Separation of duties for CSP-managed keys

```
"Statement": [ {
  "Action": [
      "*"
  ],
  "Effect": "Allow",
  "Principal": "*",
  "Resource":
"arn:aws:s3:::515support
- courses   - data/*"
} ]
```

High Availability

- High availability
  - Virtualization layer provisions dynamic allocation and redundancy
  - 99.99%+ uptime
- Replication
  - Copying data between media, servers, or sites
  - Performance tiers
- High availability across zones
  - Local
  - Regional
  - Geo-redundant storage (GRS)

Cloud Networking Security

- Cloud networking types
  - Operating and managing cloud systems
  - Virtual networks between VMs and containers within the cloud
  - Virtual networks publishing cloud services
- Virtual private clouds (VPCs)
  - Segmented virtual networks
  - Can contain multiple IPv4 and IPv6 subnets
- Public and private subnets
  - Internet gateway and default route
  - Public IP addresses
  - NAT gateway
  - VPN

VPCs and Transit Gateways

- Routing between subnets
  - Can use traditional access control lists
  - Can use vendor security appliance instances
- Multiple VPCs for segmentation
  - Between VPCs in the same account
  - Between different accounts
  - To on-premises networks
- Peering relationships
  - One-to-one connections
- Transit gateways
  - Virtual router

VPC Endpoints

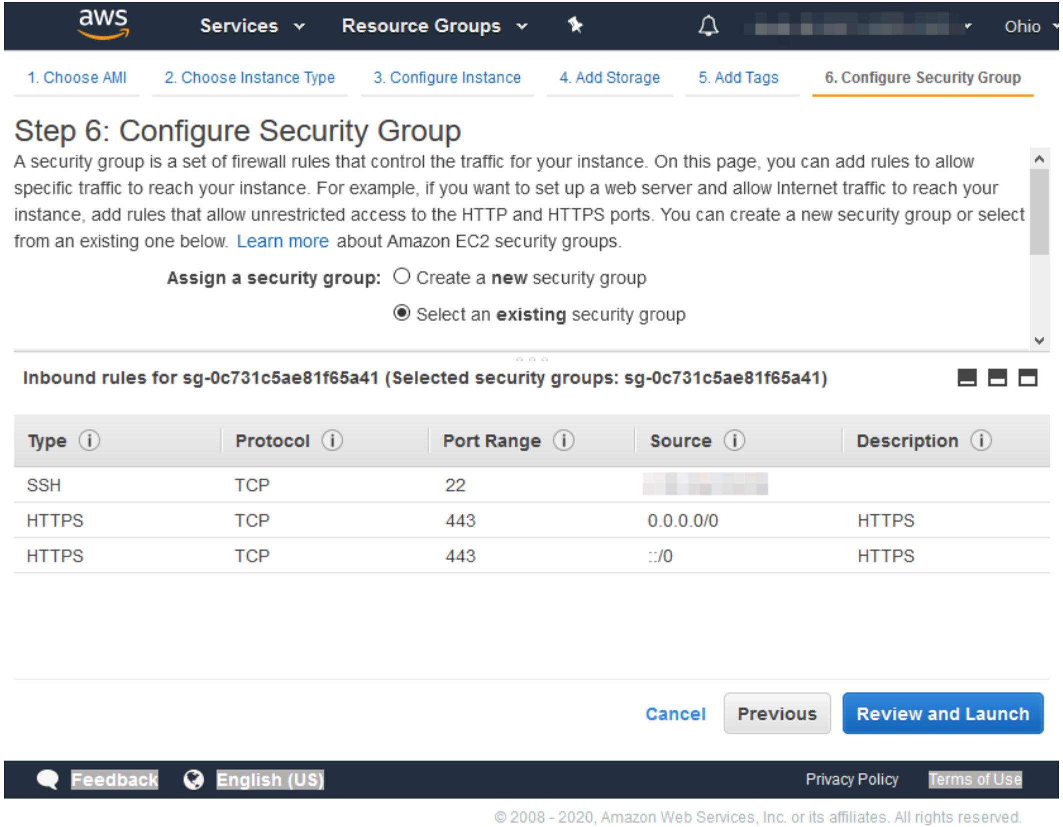
- Publishing a service over cloud internal network
- Avoids exposing traffic to the Internet
- Gateway endpoint
  - Connect instances to S3 and DynamoDB services
  - Added as route
- Interface endpoint
  - AWS PrivateLink
  - Service VPC or default Amazon service published with a DNS name
  - VPC endpoint interface added to each service consumer VPC
  - Instances within the consumer VPC access the service via the VPC endpoint interface

Cloud Firewall Security

- Need for segmentation
  - Load balancing workloads
  - Isolating data processing
  - Compartmentalizing data access
- Open Systems Interconnection (OSI) layers
  - Network layer (layer 3)
  - Transport layer (layer 4)
  - Application layer (layer 7)
- Cloud native versus vendor controls
  - Deploy host-based firewall within instance
  - Deploy vendor firewall/security appliance as instance
  - Transaction and volume costs for cloud native solutions

Security Groups

- Basic stateful packet filtering for instances
- Default security group
- Custom groups
  - Custom group with no rules drops all network traffic
  - Can be assigned to multiple instances
  - Instances in the same subnet can be assigned different security groups
  - Multiple security groups can be assigned to the same instance



Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ○ Create a **new** security group
● Select an **existing** security group

Inbound rules for sg-0c731c5ae81f65a41 (Selected security groups: sg-0c731c5ae81f65a41)

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	[redacted]	
HTTPS	TCP	443	0.0.0.0/0	HTTPS
HTTPS	TCP	443	::/0	HTTPS

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Screenshot used with permission from Amazon.com.

Cloud Access Security Brokers

- Mediate access to cloud services by enterprise users across all types of devices
- Implemented as proxy or via API
- Next-Generation Secure Web Gateway
  - Secure access service edge (SASE)

Topic 15C

Summarize Infrastructure as Code Concepts

Syllabus Objectives Covered

- 2.2 Summarize virtualization and cloud computing concepts

Services Integration and Microservices

- Monolithic client/server applications
- Service-oriented architecture (SOA)
  - Atomic services with defined input/output interfaces
  - Loosely decoupled
- Microservices
  - Each service capable of independent development and deployment
  - Highly decoupled
- Services integration and orchestration
  - Enterprise service bus versus orchestration
  - Automating automation
  - Uses scripts and service APIs to provision a workflow
  - Cloud orchestration platforms

Application Programming Interfaces

- Means by which external entities interact with a service
- Simple Object Access Protocol (SOAP)
  - XML format messaging
  - Web Services (WS) standards
- Representational State Transfer (REST)
  - RESTful APIs
  - HTTP operation/verb
  - Noun endpoints accessed as URLs

Serverless Architecture

- Service provision is wholly abstracted from the hardware, OS, and platform layers
  - AWS Lambda
  - Google Cloud Functions
  - Microsoft Azure Functions
- All hardware, OS, and platform management is security of the cloud
- Heavily reliant on orchestration

Infrastructure as Code

- All configuration and provisioning is performed by scripting/automation/orchestration
- Elimination of inconsistency (snowflakes and configuration drift)
- Idempotence
  - Making the same call with the same parameters will always produce the same result

Software-Defined Networking

- Physical and virtual appliances that can be fully automated
  - Control plane/policy definitions
  - Data plane/network controller
  - Management plane
- SDN policy > northbound API > network controller > southbound API > firewall appliance
- Network functions virtualization (NFV)

Software-Defined Visibility

- Near real-time collection, aggregation, and reporting of data
- Baseline monitoring and anomaly detection
- Supports east/west and zero trust
- Security orchestration and automated response (SOAR)

Fog and Edge Computing

- Embedded and IoT devices deployed at the network edge
- Strong requirements for availability and low latency
- Fog computing
  - Provision greater processing resource between the edge and data center
  - Prioritize data for analysis and alert conditions
- Edge computing
  - Defines additional zones and processing nodes
  - Edge device zone
  - Edge gateways
  - Fog nodes
  - Data center

Lesson 15

Summary