NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Servers & Networking

Cloud Infrastructure Engineering

Nanyang Technological University
& Skills Union - 2022/2023

Course Content

- Quick Check-In
- Dive into the basics of Server Networking
- Dive into the concepts of Server Clustering
  - Differentiate the approaches used for clustering
- Cover concepts of Blacklisting and Whitelisting
  - Differentiate between Blacklisting and Whitelisting

Time	What	How or Why
7:15pm - 7:30pm	Part 1 - Presentation	Server Clustering
7:30pm - 7:50pm	Part 2 - Presentation	Types of Server Clustering
7:55pm - 8:10pm	Part 3 - Presentation	Load Balancer
8:10pm - 8:20pm	Break	
8:20pm - 8:40pm	Part 4 - Presentation	Blacklisting & Whitelisting
8:40pm - 9:00pm	Activity	
9:00pm - 9:45pm	Learners attempt assignments	
9:45pm - 10:00pm	Wrap Up	

Recap

- Servers
  - Both Hardware & Software
  - Types
    - Web
    - Application
    - Database
    - Proxy
    - Mail
    - Print
    - File

Recap

- Virtualization
  - Types
    - Full virtualization
    - Para-virtualization
    - Hardware-assisted virtualization
    - OS-level virtualization
    - Hypervisor virtualization
  - Containerization on top of OS-level virtualization
    - Docker

Self Study Check-In

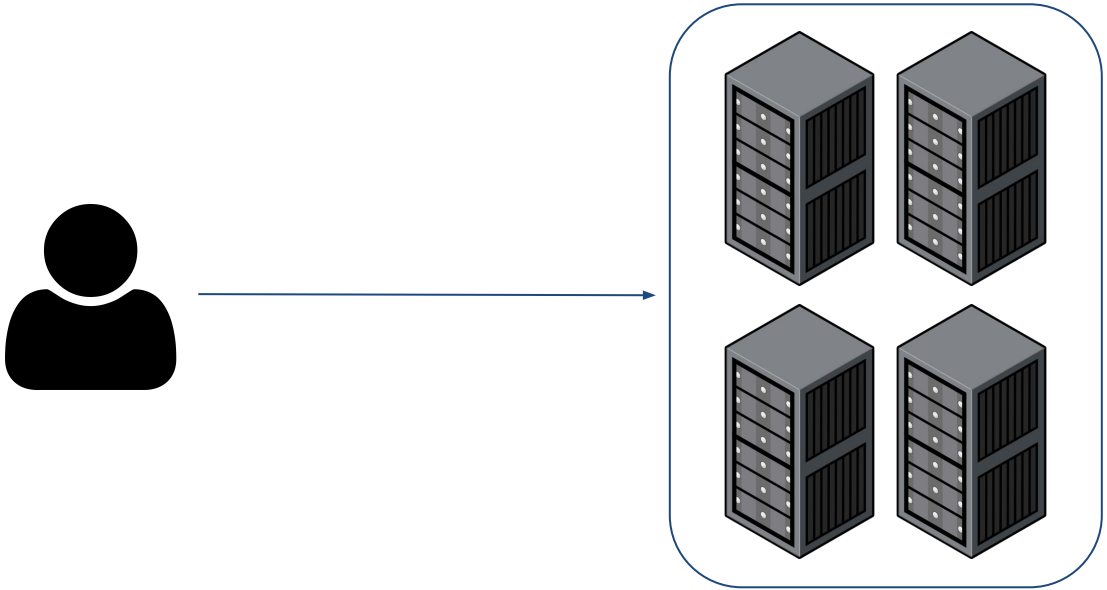
Server Clustering

What is Server Clustering?

When **several servers collaborate on a single system** to give users improved availability, this is referred to as **server clustering**.

By allowing a different server to take over in the event of an **outage**, these clusters are utilized to **minimize downtime and outages**.

What is Server Clustering?



Application / Service Failure

Any **disruptions** that result from **serious mistakes with software or services** that are essential to the server's or data center's functioning are referred to as application/service failure events.

It can be **challenging** for server administrators **to identify and fix possible problems** before they result in an outage due to the complicated and dense nature of server monitoring data.

System/ Hardware Failures

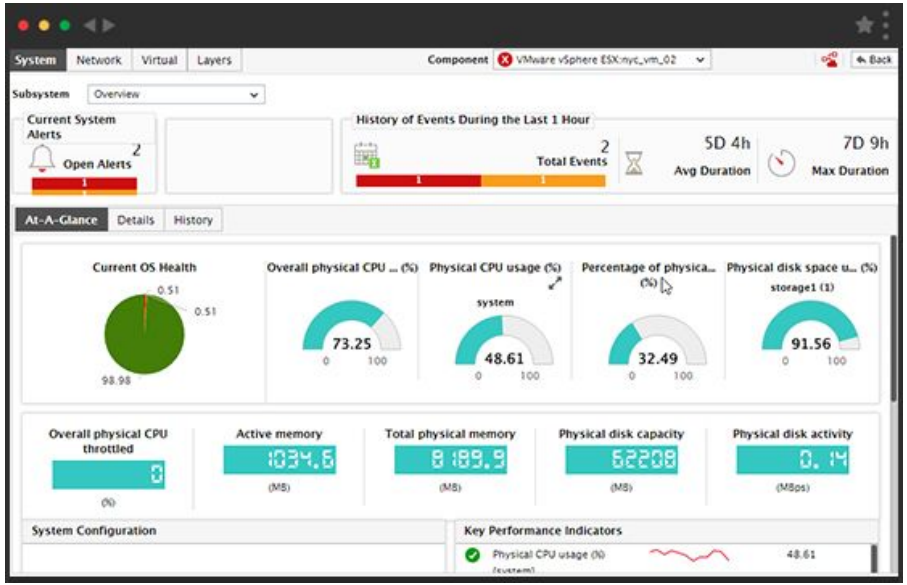
Failures with the actual hardware that the server is running on are the cause of this kind of outage.

Overheating, inadequate optimization, or just the component reaching the end of its useful life are all potential causes of this failure.

Due to their significance in ensuring the server's **continued operation**, **processors, physical memory, and hard disks** are among the components most prone to failure.

What Can We Do?

- Extensive Logging & Monitoring



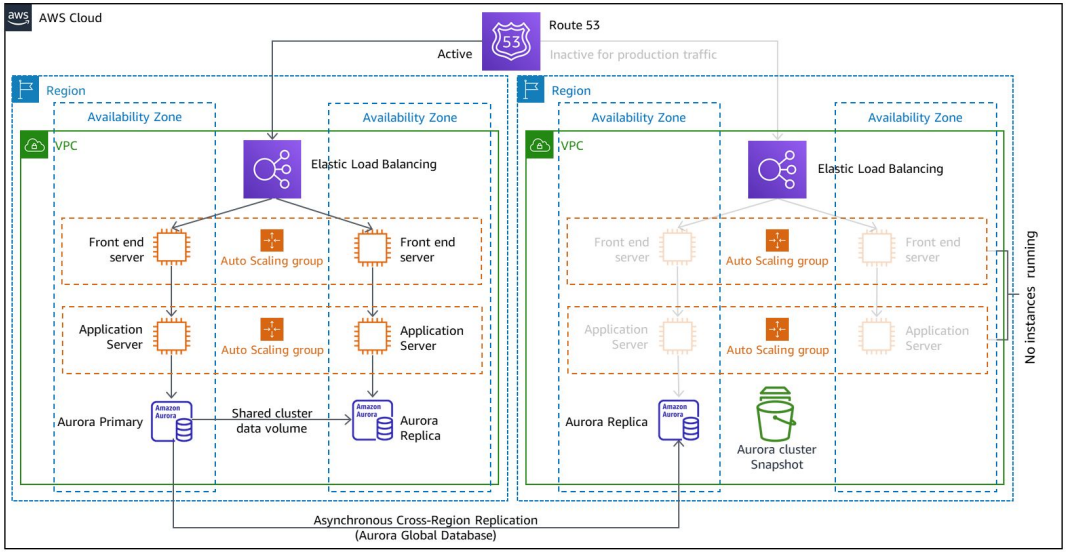
Site Failures

Site failures are typically brought on by **incidents** that take place **outside** of a data center.

Redundancy solutions are essential for data centers situated in disaster-prone areas.

What Can We Do?

- Plan for Redundancy/ Disaster Recovery (Next lesson 😁)



Summary

Even while problems that can cause these three different kinds of failures can be found and fixed, **redundancy techniques like server clustering** are the only way to guarantee almost **perfect reliability.**

Types Of Clustering Server

Types Of Clustering Servers

There are various types of Clustering Servers, but we will look at **three different types of server clusters**.

The three varieties are discussed in more detail below and comprise a:

1. High-Availability Servers
2. Load-Balancing Servers
3. High-Performance Servers

High-Availability Servers

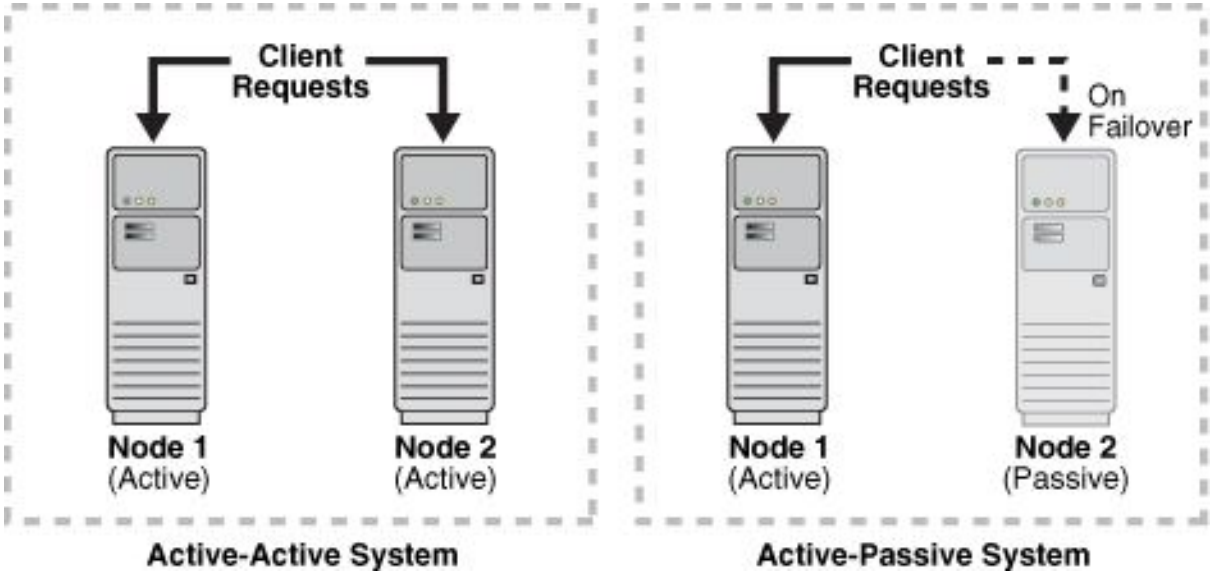
High availability clusters let you **avoid single points of failure** since they are built on redundant hardware and software.

They are critical for load balancing, system backups, and failover.

They are **composed of multiple hosts** that can take over if a server shuts down. This guarantees **minimal downtime** if a server overloads or fails.

High-Availability Servers

HA clusters have two architecture types: **Active-Active** and **Active-Passive**.



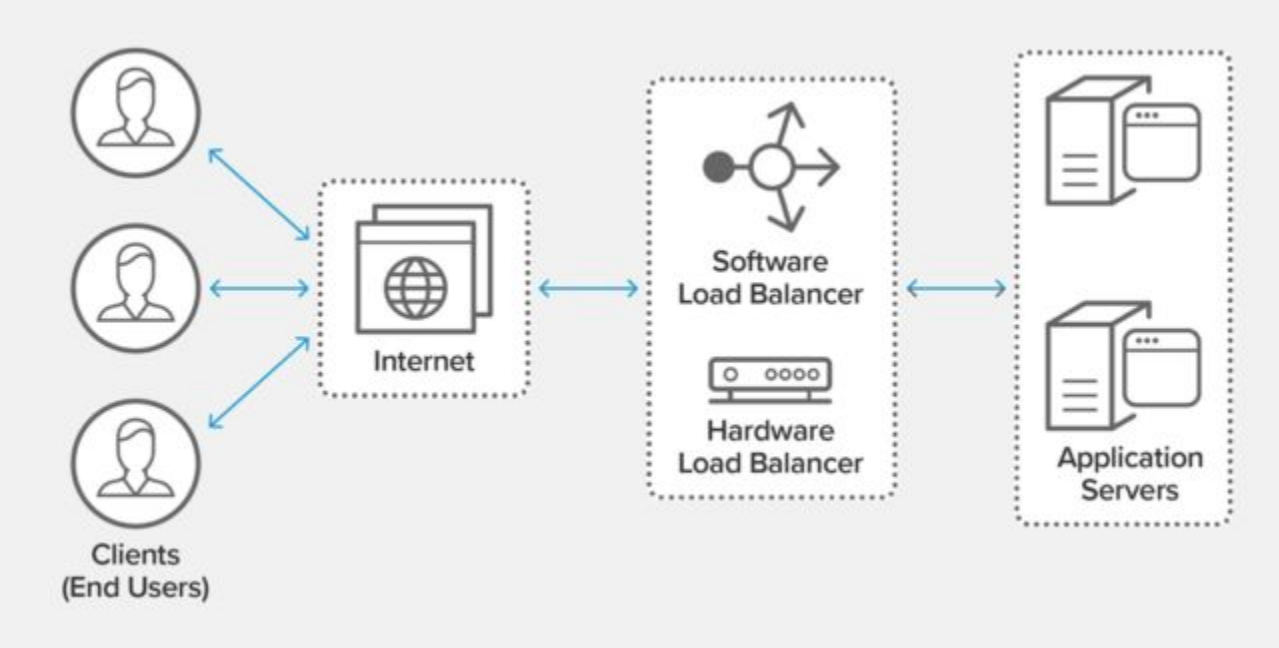
Load Balancing Server

Load balancing refers to **efficiently distributing incoming network traffic** across a **group of backend servers**, also known as a server farm or server pool.

Modern high-traffic websites must **serve hundreds of thousands** of **concurrent requests** from users or clients and return the response in a **fast and reliable manner**.

To cost-effectively scale to meet these high volumes, modern computing best practice generally requires **adding more servers.**

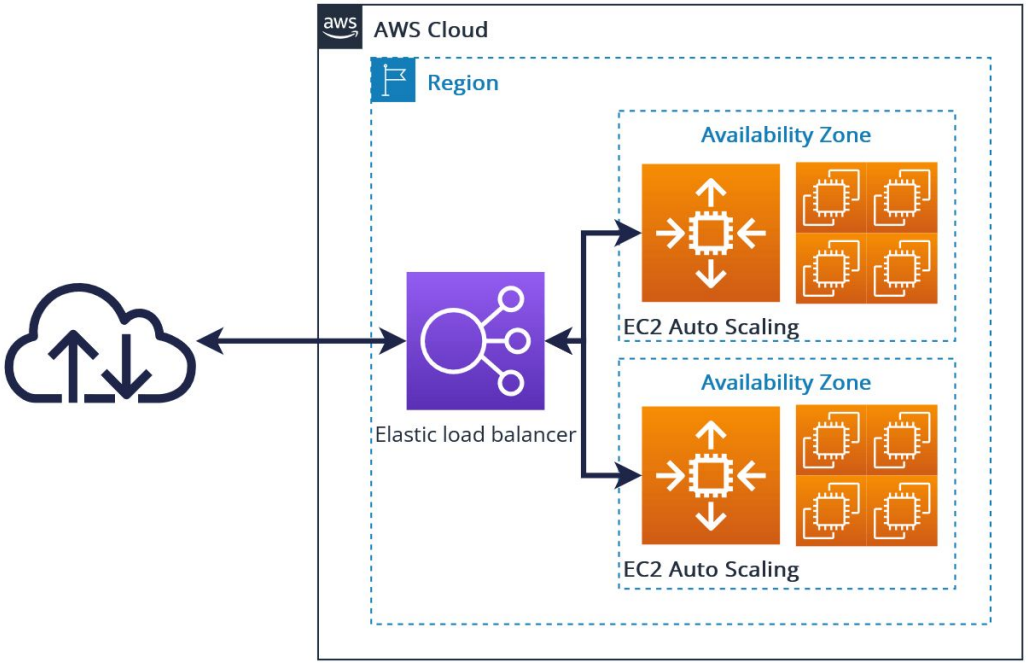
Load Balancer



Load Balancer Functions

- Distributes client requests or network load **efficiently across multiple servers**
- Ensures **high availability** and **reliability** by sending requests only to servers that are online
- Provides the **flexibility** to add or remove servers as demand dictates

AWS Load Balancer



Benefits Of Load Balancer

- Reduced downtime
- Scalable
- Redundancy
- Flexibility
- Efficiency

High Performance Servers

High-performance clusters, also known as **supercomputers**, offer **higher performance, capacity, and reliability**. They are most often used by businesses with resource-intensive workloads.

A high-performance cluster is **made up of many computers** connected to the **same network**.

You benefit from both **high-performance clusters** and data storage clusters and get seamless performance and high-speed data transfers.

High Performance Servers

These clusters are widely used with Internet of Things (IoT) and artificial intelligence (AI) technology.

They process **large amounts of data in real time** to power projects such as **live streaming, storm prediction, and patient diagnosis.**

For this reason, high-performance cluster applications are often used in research, media, and finance.

High Performance Servers

Time to Ponder…

1. What are the differences between the below terms:
    a. Availability
    b. Reliability
    c. Resiliency
    d. Durability

Availability

Understood as **system uptime**, i.e., the percentage of time the storage system is available and operational, allowing data to be accessed.

“Is my application available for use?”

Reliability

The ability of a workload to **perform its intended function correctly** and **consistently** when it's expected to.

“Is my application running correctly?”

Resiliency

The ability for a system to **recover from a failure** induced by load, attacks, and failures.

“Can my application run if there is a failure?”

Durability

Ability to **perform its responsibilities over time**, even when unexpected events may occur.

“Can I retrieve my data even when there is a failure?”

Break Time

Blacklisting & Whitelisting

Blacklisting

Blacklist

A border control authority, as an illustration in the real world, might keep a **blacklist of known or suspected terrorists.**

A store owner might keep track of **shoplifters on a blacklist**.

A **blacklist of malware**, including viruses, spyware, Trojan horses, worms, and other forms of malware, is common in the area of network security.

A **blacklist of individuals**, **IP addresses, programs, emails, domains, processes, or organizations** is another option.

Blacklisting can be used for almost every part of your network.

Blacklist

Organizations can use lists made by third parties, such as network security service providers, as well as their own blacklists to **delist applications.**

The **classic method of access control is blacklisting**, which has long been employed by spam filters, intrusion detection systems, anti-virus tools, and other security software applications.

Blacklist

The blacklist approach is **threat-centric**,

and the **default is to allow access.**

Any entity not on the blacklist is **granted access**, but anything that's known or expected to be a threat is blocked.

Pros of Blacklist

Simplicity

It works based on a simple principle — just identify the known and suspected threats, deny them access and let everything else go.

Pros of Blacklist

Low Maintenance

In many cases, your security software or security service provider will handle compiling the list with little need for input from the user.

Cons of Blacklist

Hard To Keep Updating

A blacklist can never be comprehensive, though, since new threats emerge constantly.

Every day, the AV-TEST Institute, which researches IT security, registers **more than 350,000 new malicious programs and potentially unwanted applications**.

Cons of Blacklist

Hard To Keep Track

Easy for security software providers to miss threats simply because there are so many.

While blacklisting is effective against known threats, it's **useless** against **new, unknown threats like zero-day attacks**.

Cons of Blacklist

Complexity of Threats

Hackers also sometimes design malware specifically to evade detection by tools that use a blacklist system.

They may be able to **modify the malware** so the blacklist tool does not recognize it as a blacklisted item.

Whitelisting

Whitelisting

Whitelisting tackles the same challenges as blacklisting but uses the **opposite approach**.

Instead of creating a list of threats, you **create a list of permitted entities** and block everything else.

It's **based on trust,** and the **default is to deny anything new** unless it's proven to be acceptable.

This results in a much stricter approach to access control.

Whitelisting

Whitelisting

The whitelisting strategy, for example, is used when a **firewall only permits specific IP addresses to enter a network**.

The Apple app store is another illustration that most people have encountered. The business only allows consumers to use programs that Apple has authorized and added to the app store.

Whitelisting

You must take into account all of the jobs that users must carry out and the tools they'll require to do so in order to develop a whitelist for the network level.

In addition to more specific information like **application dependencies, software libraries, plugins, extensions, and configuration files**, this network-level whitelist may also contain **network infrastructure, sites, locations, applications, users, contractors, services, and ports**.

A **user-level whitelist** could contain **files**, **applications**, and **email addresses**.

Whitelist Summary

Whitelisting involves only **allowing access for approved entities**.

The **default is to block access.**

Whitelisting is **trust-centric.**

Blacklist Summary

The blacklist approach is **threat-centric**,

and the **default is to allow access.**

Any entity not on the blacklist is **granted access**, but anything that's known or expected to be a threat is blocked.

Group Activity

Prepare **presentation** with your own **group** about which method that will you use to handle these case

Case:

- eCommerce Website
- Financial Institution
- Government
- Personal Static Website
- Email Application
- Company Portal

Group Activity

Methods to Consider:

- Clustering
- Load Balancing
- Whitelisting
- Blacklisting

You may combine more than 1 method and give details what and why you do it.

What’s Next?