Patel Nandinee Jatinkumar

Cloud computing

Module -4

1-Resource Monitoring Techniques

Ans:- Cloud resource management involves monitoring, allocating, and controlling computing resources in a cloud environment. Some resource monitoring techniques include:

Prioritizing metrics

Focus on metrics and events that are most important to your business and align with your goals.

Consolidating data

Use a single platform to gather data from multiple sources, such as servers, databases, networks, and applications.

Setting automatic triggers

Set thresholds for efficiency and automate actions when activity goes above or below them.

Monitoring user experience

Assess user interaction metrics to optimize performance and satisfaction.

Monitoring costs

Regularly review cloud spending to identify inefficiencies and optimize costs.

Monitoring resource usage

Track metrics such as CPU use, memory usage, network latency, and disk I/O.

Monitoring error rates

Monitor the frequency of errors to identify issues with application code or infrastructure.

Monitoring uptime and availability

Ensure cloud services meet uptime requirements.

Training team members

Train team members on best monitoring practices and ensure they understand the monitoring tool.

Regularly reviewing strategy

Regularly review your monitoring strategy to identify areas for improvement.

2-How to access compute (windows and Linux) from internet? describe tools and its security

- Ans:- Linux is known for its roughness and versatility, which powers a large portion of the internet and enterprise systems. However, its open-source nature also makes it more susceptible in case of security vulnerabilities. Hence, there's the need for effective security measures that cannot be overstated.

Popular Security Tools for Linux:

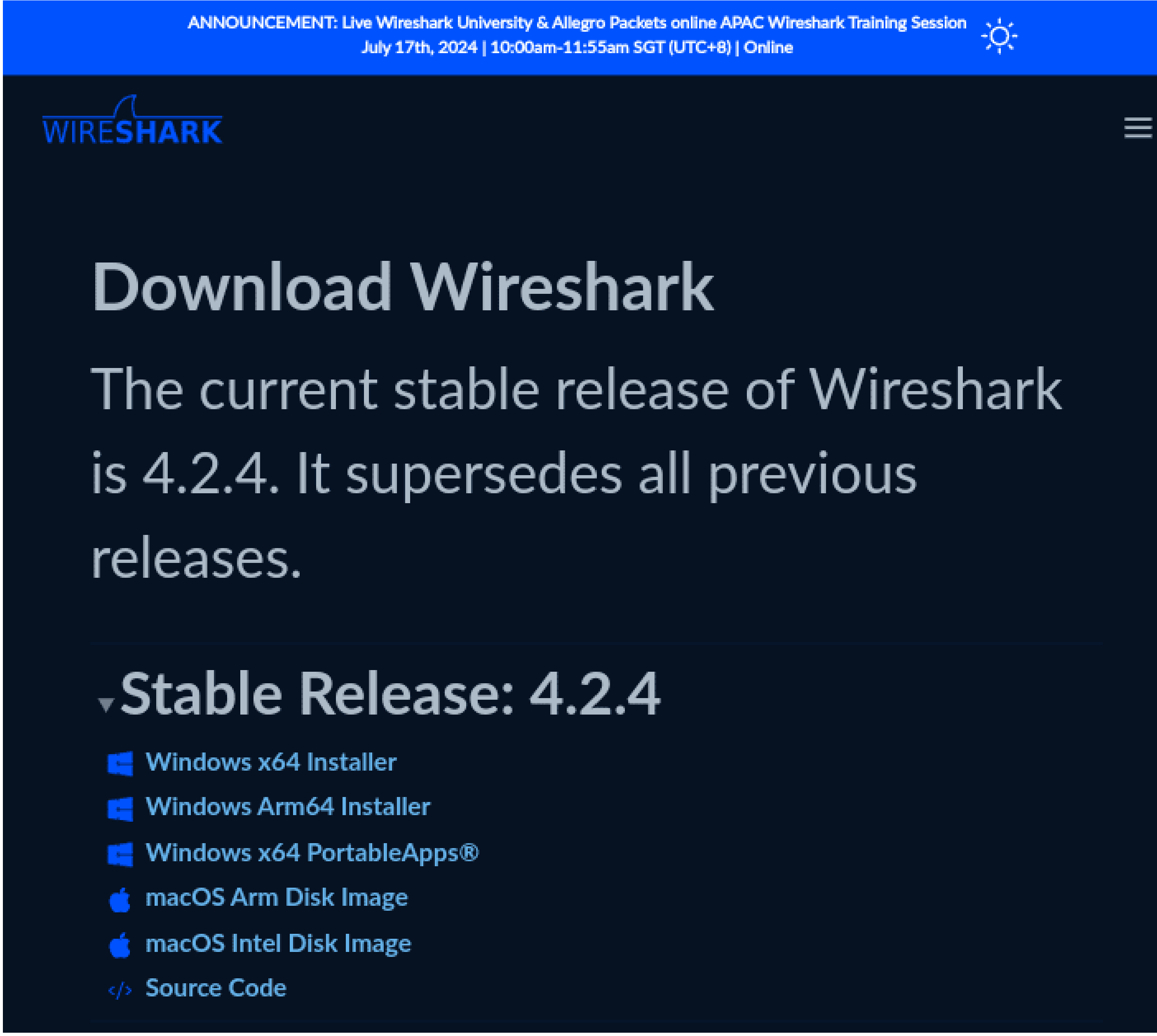
1. Nmap (Network Mapper)

Beyond just discovering hosts and services on a network, The Nmap offers a large amount of features. It can simply conduct port scanning, detect the operating systems, map the network topology, and even it perform vulnerability assessment as well. Its flexibility and extensive options make it a more stable tool for network administrators, security professionals, and ethical hackers.

Nmap

2. Wireshark

Commonly known as a packet analyzer, The Wireshark is an versatile tool that goes out of the box for network troubleshooting. It mostly allows users to capture and interactively browse the traffic running on a computer network statistics at a real-time. In addition, Wireshark also supports hundreds of the protocols, making it indispensable for the protocol development, network security analysis, and educational purposes as well.



ANNOUNCEMENT: Live Wireshark University & Allegro Packets online APAC Wireshark Training Session
July 17th, 2024 | 10:00am-11:55am SGT (UTC+8) | Online

WIRESHARK

Download Wireshark

The current stable release of Wireshark is 4.2.4. It supersedes all previous releases.

▾Stable Release: 4.2.4

- Windows x64 Installer
- Windows Arm64 Installer
- Windows x64 PortableApps®
- macOS Arm Disk Image
- macOS Intel Disk Image
- Source Code

Wireshark

3. Snort

This venerable intrusion detection system **(IDS)** is mostly famous for its speed and great accuracy in detecting and preventing the network intrusions. It's real-time traffic analysis capabilities, will coupled with editable rule sets, enable it to identify the suspicious activities and the potential threats effectively. The snort's open-source nature and it's active community will make it a great weapon in the arsenal of network defenders

4. ClamAV

As a malware threats continue to evolve with time, ClamAV still remains a steadfast protector of Linux systems. Its robust antivirus engine is adept at detecting as well as removing different forms of malware, including viruses, trojans, and ransomware in it. With the regular updates to its signature database, ClamAV make sure that Linux users stay protected against emerging threats

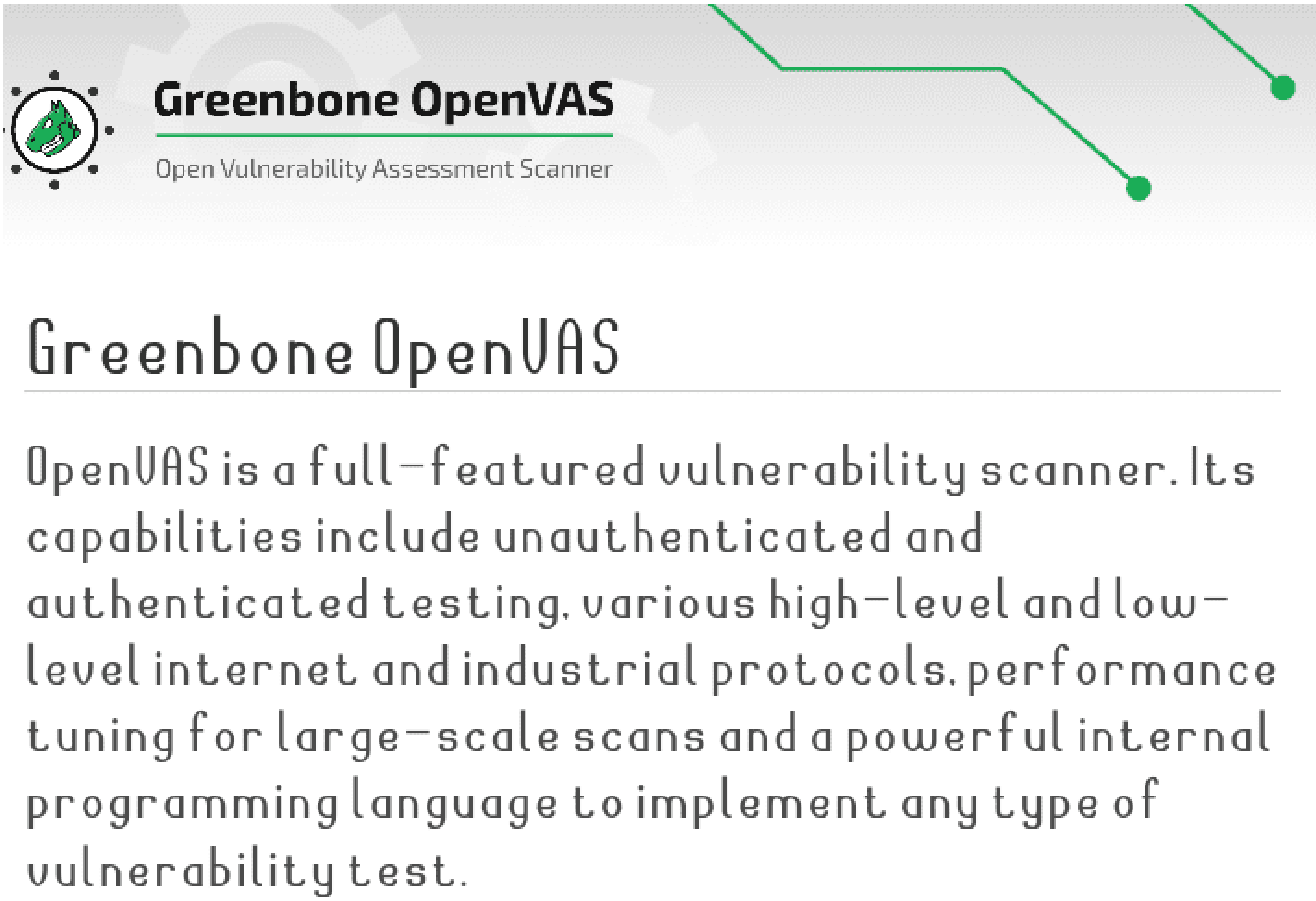
ClamAV® is an open-source antivirus engine for detecting trojans, viruses, malware & other malicious threats.

The latest stable release is version 1.3.1.

ClamAV

OpenVAS (Open Vulnerability Assessment System)

In today's cybersecurity market, identifying and finding solutions of vulnerabilities is at the top. OpenVAS excels in this regard by simply scanning networks for the security issues and misconfigurations included in it. Its comprehensive vulnerability database, paired with automated scanning and reporting capabilities, which will empowers organizations to proactively reduce risks and bolster their defenses.



Greenbone OpenVAS
Open Vulnerability Assessment Scanner

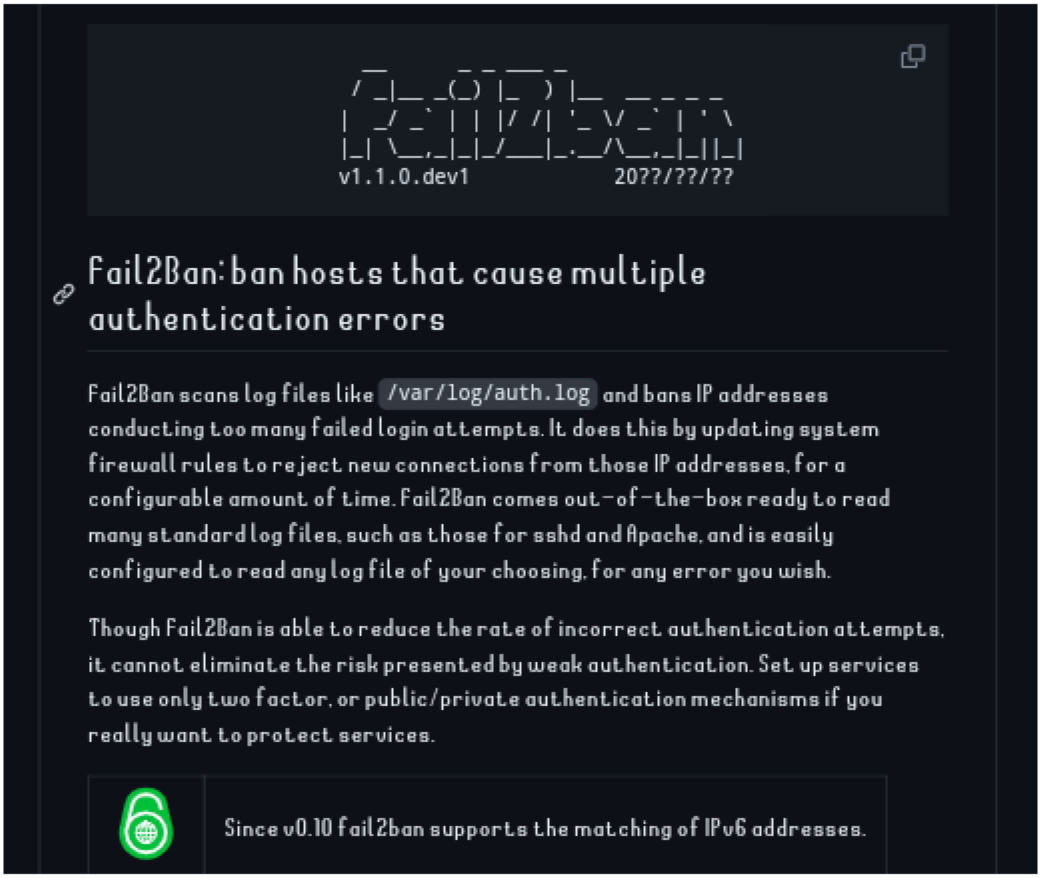
Greenbone OpenVAS

OpenVAS is a full-featured vulnerability scanner. Its capabilities include unauthenticated and authenticated testing, various high-level and low-level internet and industrial protocols, performance tuning for large-scale scans and a powerful internal programming language to implement any type of vulnerability test.

OpenVAS

6. Fail2ban

It act as a vigilant sentry, Fail2ban basically monitors system logs for targeting signs of malicious activity and quickly takes action by banning IPs exhibiting suspicious behavior. By dynamically updating the firewall rules, Fail2ban effectively reduces brute-force attacks, SSH intrusions, and other most common threats, enhancing the security posture of Linux systems effectively



```
   __      _ _ ___ _
  / _|__ _(_) |_  ) |__  __ _ _ _
 |  _/ _` | | |/ /| '_ \/ _` | ' \
 |_| \__,_|_|_/___|_.__/\__,_|_||_|
 v1.1.0.dev1            20??/??/??
```

Fail2Ban: ban hosts that cause multiple authentication errors

Fail2Ban scans log files like `/var/log/auth.log` and bans IP addresses conducting too many failed login attempts. It does this by updating system firewall rules to reject new connections from those IP addresses, for a configurable amount of time. Fail2Ban comes out-of-the-box ready to read many standard log files, such as those for sshd and Apache, and is easily configured to read any log file of your choosing, for any error you wish.

Though Fail2Ban is able to reduce the rate of incorrect authentication attempts, it cannot eliminate the risk presented by weak authentication. Set up services to use only two factor, or public/private authentication mechanisms if you really want to protect services.

Since v0.10 fail2ban supports the matching of IPv6 addresses.

3-Encryption Technologies and Methods

Ans:- Asymmetric encryption

Also known as public-key cryptography, this method uses two keys: a public key to encrypt and a private key to decrypt. It provides better security by verifying the data source and preventing the author from disputing its authorship.

Symmetric encryption

In this method, the sender and the intended recipient share a secret key. The encryption key converts the plaintext into ciphertext, and the recipient uses the same key to decrypt the file.

4-Describe network security in cloud, compute security and storage security

Ans:- Cloud network security, cloud computing security, and cloud storage security are all related to protecting data, applications, and infrastructure in the cloud:

Cloud network security

Protects cloud networks from unauthorized access, modification, misuse, or exposure of data. It uses hardware, software, controls, processes, and policies to assess access requests, authorize users, and neutralize malware. Cloud network security also includes network segmentation, namespaces, overlay networks, traffic filtering, and encryption for containers. Firewalls are a fundamental component of cloud network security.

Cloud computing security

Protects cloud-based data, applications, and infrastructure from cyberattacks and cyberthreats. It uses a combination of controls, policies, and technologies.

Cloud storage security

Protects data from unauthorized access and attacks. It focuses on malware, DDoS attacks, hacking, data breaches, data leaks, and disaster recovery. Cloud storage security uses physical security, technology tools, access management and controls, and organizational policies

Module - 5

1-How to configure, develop and maintain Security and Privacy in cloud?

Ans:- Encryption

Use encryption by default to protect data in transit and at rest. This can reduce the potential attack surface and prevent unauthorized access.

Multi-factor authentication (MFA)

Use MFA for staff logins to enhance security. MFA uses methods like biometrics or hardware tokens to verify login attempts.

Least privilege

Limit access rights to the bare minimum required for a user or process to perform their task. This minimizes the chances of a data breach.

Security posture visibility

Use tools to monitor and log cloud security configuration and network-based monitoring. This ensures security, privacy, and adherence to organizational and regulatory requirements.

Evaluate cloud service providers

Look for a cloud provider that has a good reputation, follows industry standards and regulations, and offers strong encryption and authentication mechanisms.

Incident response

Implement an incident response plan to remediate a breach, avoid operational disruptions, and recover lost data.

Training

Integrate cloud security into onboarding and ongoing training. Create cloud security plans for all staff levels and ensure everyone understands their role in security.

Zero Trust security model

Use zero trust solutions to verify each access request with continuous authentication and authorization checks.

2-What is Portability in cloud?

Ans:- cloud computing, portability is the ability to move applications, data, and workloads between cloud environments with minimal issues. This can include moving between public and private clouds, or between different public cloud providers.

Portability can be achieved by using open source tools to build applications and workloads that can run on any cloud. This can result in several advantages, including:

Flexibility

A cloud-agnostic approach can provide flexibility throughout the development process.

Prevents vendor lock-in

The ability to move workloads and hire developers with transferable skills across cloud providers.

Portability is different from interoperability, which is the ability of two cloud systems to exchange messages and information.

3-What is Reliability and high Availability in cloud?

Ans:- Reliability and high availability are important aspects of cloud computing that ensure users can access their data and applications without interruption:

Reliability

The probability that a cloud system will perform its intended function without failure. Reliability is measured by the frequency of component failures. It’s important for businesses to ensure their applications are reliable before deploying them to the cloud.

High availability

The probability that a cloud service is operational and reachable at a given time. High availability is achieved through redundancies, load balancing, failover mechanisms, and data replication. It’s essential for businesses to maintain customer confidence and avoid revenue losses.

Here are some ways to achieve high availability:

Active/Active

Two or more clusters in an HA cloud system are always running the same service. A cloud load balancer splits traffic between the clusters to maintain performance.

Active/Passive

Some clusters in an HA cloud system are available, while others are not. The passive cluster takes over if the active cluster fails.

4-Describe Mobility Cloud Computing

Ans:- Mobility in cloud computing refers to the ability to move data and workloads between different environments, such as the cloud, data centers, mobile devices, and the network edge:

Data mobility

The ability to move data between different environments to keep it safe and accessible. This can help improve employee productivity, reduce costs, and speed up application development.

Workload mobility

The ability to move computing workloads between different environments, such as from an on-premises data center to the cloud. This can help with load balancing and geographic redundancy.

Cloud mobility

The ability to balance resources and costs between public and private cloud services. This can help with flexibility and adapting to changes in the market, technology, or business.

Cloud mobility can also refer to a Platform as a Service (PaaS) offering that provides mobile apps and other extensions for traditional business applications. These apps can include analytic apps and custom applications.

5-Describe AWS, Azure, Google cloud Platforms

Ans:- Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) are all popular cloud providers with unique strengths:

AWS

Known for its global reach and scalability, AWS offers a wide range of solutions, including:

Infrastructure, including storage, networking, servers, and mobile development

Cybersecurity solutions

Auto-scaling features, like Elastic Load Balancing and Auto Scaling Groups

Compute services, like Elastic Compute Cloud (EC2)

Azure

Known for its integration and security, Azure offers:

Scalable and efficient software solutions

Seamless integration with Microsoft products

Auto-scaling capabilities, like Virtual Machine Scale Sets and Load Balancer

Security features, like firewall and DDoS protection

GCP

Known for its data management and machine learning capabilities, GCP offers:

High-end big data analytics solutions

Easy interaction with other vendor products

Auto-scaling features, like Managed Instance Groups and Load Balancing

Security options, like Identity and Access Management (IAM), Key Management Service (KMS), and Security Command Center (SCC)

Compute services, like Google Compute Engine (GCE)

When choosing a cloud provider, you can consider things like:

Performance: How well the provider meets your performance needs

Cost: How cost-effective the provider is

Integration: How well the provider integrates with other products

Security: How well the provider protects your data .

6-Accessing AWS, Azure and Google cloud Platforms (any one portal)

Ans:- There are several ways to access AWS, Azure, and Google Cloud Platform (GCP) from a single portal, including:

Workload Identity Federation

This feature allows you to access Google Cloud resources from an external workload. To configure Workload Identity Federation, you can:

Prepare your external identity provider

Define an attribute mapping and condition

Create the workload identity pool and provider

Authenticate a workload

Multicloud networks

You can implement multicloud networks by:

Logging into each cloud's IAAS console

Configuring the VPCs, VNETs, or VPCs with non-overlapping subnets

Configuring networking services for each cloud provider

Installing an instance-based virtual router in each cloud provider's VPC or VNET

Megaport

You can use Megaport to set up multicloud connectivity between AWS, Azure, and GCP. To do this, you can:

Provision a Virtual Cross Connect (VXC) from a Megaport Point of Presence (PoP) into your data center location

Connect your multiple CSPs using the Megaport Network

Spin up a Megaport Cloud Router (MCR) to connect to and between clouds .

7- Create compute, create network, create storage on AWS , Azure and GCP

Ans:- Step-by-Step Guide to Creating a GCP VM Instance

Sign in to the Google Cloud Console.

Navigate to Compute Engine.

Create an Instance: Click on the “Create Instance” button.

Configure Instance: Set the instance name, region, and zone.

Choose Machine Type: Select a machine type. ...

Boot Disk: ...

Firewall Rules: ...

Create:

8-Compare Cloud pricing of resources and services on all platform Amazon Web Services

(AWS):

Ans:- When comparing the pricing of cloud resources and services across different platforms, you can consider factors like:

Instance types

AWS is generally cheaper for general purpose and memory optimized instances, while Google Cloud is cheaper for compute optimized instances.

Discounts

AWS offers Reserved Instances (RIs) and Savings Plans, while Google Cloud offers Committed Use Discounts (CUDs) and Sustained Use Discounts (SUDs).

Commitment period

AWS offers a one- or three-year commitment for Savings Plans, while Google Cloud offers a one- or three-year commitment for CUDs.

Instance conversion

Google Cloud allows you to convert instance types during the commitment period, while AWS only offers this in a special tier with a reduced discount.

Payment options

AWS offers more flexible payment options than Azure, including reduced discounts for partial upfront payment and month-by-month payment.

Here are some examples of cloud pricing for different resources and services:

Storage

Amazon S3, Google Cloud Platform, and Azure all charge around $0.023 per GB/month for storage.

Servers

A t3.xlarge server with 4CPU/16GB capacity on AWS costs $267 per month, while a D4sV4 Linux server with the same capacity on Azure costs $351 per month.

Minimum instance

A minimum instance with 2 virtual CPUs and 8 GB of RAM on AWS costs around $69 per month, while the same on Google GCP costs around $52 per month.