

PROFESSIONAL TRAINING REPORT

Sathyabama Institute of Science and Technology (Deemed to be University)

Submitted in partial fulfilment of the requirements for the award of
Bachelor of Engineering Degree in Information Technology

By

**kommuri Vamsi
(Reg.No.40120119)**



DEPARTMENT OF INFORMATION TECHNOLOGY SCHOOL OF COMPUTING

SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY (DEEMED TO BE UNIVERSITY)

JEPPIAAR NAGAR, RAJIV GANDHI SALAI,
CHENNAI – 600119, TAMILNADU

APRIL 2023



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)

Accredited with Grade "A" by NAAC
(Established under Section 3 of UGC Act, 1956)

JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI- 6001



DEPARTMENT OF INFORMATION TECHNOLOGY

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **kommuri Vamsi** (Reg no: 40120119) who carried out the project entitled "**Virtual Machines using CirrOS Image**" under my supervision from Jan 2023 to Apr 2023.

Internal Guide

Dr.P.Jeyanthi,M.E.,Ph.D.

Head of the Department

DR. R Subhashini M.E., Ph.D.

Internal Examiner

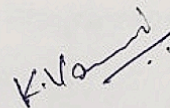
External Examiner

DECLARATION

I, **kommuri Vamsi** (Reg no: **40120119**) hereby declare that the Project Report entitled "**Cloud Machine Networking Configurations**" Done by me under the guidance of **Dr.P.Jeyanthi, M.E., Ph.D** is submitted in partial fulfilment of the requirements for the award of Bachelor of Engineering degree in Information Technology.

DATE: 29/04/2023

PLACE: Chennai



SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to the **Board of Management of SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T Sasikala, M.E., Ph.D.**, Dean, School of Computing **Dr. R Subhashini, M.E., Ph.D.**, Head of the Department of Information Technology for providing me with necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr.P.Jeyanthi, M.E., Ph.D.** for her valuable guidance, suggestions and constant encouragement that paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Information Technology** who were helpful in many ways for the completion of the project.

TRAINING CERTIFICATE



इलेक्ट्रॉनिक्स एवं
सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF
ELECTRONICS AND
INFORMATION TECHNOLOGY



Ref.No.: 25 /FSPCC/BC001/04/2023

COURSE COMPLETION LETTER

It is certified that

Kommuri Vamsi

Sathyabama Institute of Science and Technology

has successfully undergone the Bridge Course Training Program on

Cloud Computing Technology

Under "FutureSkills PRIME" Programme

commenced from 11 Mar, 2023

Shri. V. Sridharan
Chief Investigator
Cloud Computing Technology
Lead Resource Centre

L R PRAKASH

Digitally signed by L.R. PRAKASH
Date: 2023.04.26 01:09:12
+05'30'

Cdr.(Retd.) L.R. Prakash
Senior Director
Centre Head
C-DAC, Chennai

Lead Resource Centre
Cloud Computing Technology
Chief Investigator
श्री. व. श्रीधरान

C-DAC, Chennai
Centre Head
Senior Director
चंद्र(प्रति.) एल.आर. प्रकाश

ABSTRACT

This project involved setting up an OpenStack environment on a Linux machine and creating virtual machine instances within that environment. The aim of the project was to demonstrate proficiency in working with cloud computing technologies and to gain hands-on experience with OpenStack.

After installing OpenStack on the Linux machine, the project focused on creating instances of the CirrOS virtual machine and assigning floating IPs to them. Once the instances were up and running, the project verified network connectivity between them and external networks by pinging Google from the instances and pinging between the instances themselves.

The project successfully demonstrated the ability to create and manage virtual resources using OpenStack. The project also provided valuable experience working with cloud computing technologies, including an understanding of OpenStack architecture, virtualisation, networking, and security.

The project is a useful starting point for anyone interested in learning about OpenStack and cloud computing. The project can be extended to include additional features such as creating volumes, setting up networks, and configuring security groups, providing a more comprehensive understanding of OpenStack and its capabilities.

This project involved setting up an OpenStack environment on a Linux machine and creating virtual machine instances within that environment. The aim of the project was to demonstrate proficiency in working with cloud computing technologies and to gain hands-on experience with OpenStack.

After installing OpenStack on the Linux machine, the project focused on creating instances of the CirrOS virtual machine and assigning floating IPs to them. Once the instances were up and running, the project verified network connectivity between them and external networks by pinging Google from the instances and pinging between the instances themselves.

The project successfully demonstrated the ability to create and manage virtual resources using OpenStack. The project also provided valuable experience working with cloud computing technologies, including an understanding of OpenStack architecture, virtualisation, networking, and security.

TABLE OF CONTENTS

CHAPTER No.	TITLE	PAGE NO.
	ABSTRACT	VI
	LIST OF FIGURES	IX
	LIST OF ABBREVIATIONS	X
1	INTRODUCTION	1
	1.1 Cloud Computing	2
	1.2 Advantages of Cloud computing	3
	1.3 Cloud Service Providers	4
	1.4 OpenStack	5
	1.5 CirrOS	6
	1.6 Security Groups in CirrOS	7
	1.7 Instances in CirrOS	8
	1.8 Security Configurations in CirrOS	9
	1.9 Types of Clouds	10
	1.10 LAAS Clouds	11
	1.11 SSH Client and Connections	12
	1.12 HTTP Client and Connections	13
	1.13 Ping	14

	1.14 Recommended Security Rules in CirrOS	15
	1.15 Alternatives for CirrOS	16
	1.16 CirrOS over its Alternatives	17
2	SYSTEM ANALYSIS	19
	2.1 Aim & Scope	19
	2.2 How does it work?	20
3	SYSTEM DESIGN AND IMPLEMENTATION	23
	3.1 Algorithm	23
	3.2 Ideation Map	25
4	RESULTS & DISCUSSION	26
	4.1 Results	26
5	CONCLUSION	29
	5.1 Reference	30

LIST OF FIGURES

FIGURE NO.	FIGURE NAME	PAGE NO.
1.	<i>Instances of CirrOS created</i>	26
2.	<i>Connecting to VMs via SSH</i>	27
3.	<i>Ping to google.com from Both the VMs</i>	27
4.	<i>Ping between each other</i>	28

LIST OF ABBREVIATIONS

ABBREVIATION	EXPANSION
AWS	Amazon Web Services
LAAS	Logistics as a Service
SASS	Software as a service
AWS	Amazon Web Services
GCP	Google Cloud Platform

CHAPTER 1

INTRODUCTION

OpenStack is an open-source cloud computing platform that offers Infrastructure-as-a-Service (IaaS) capabilities to organisations. In this project, we aimed to set up an OpenStack environment on a Linux machine and create virtual machine instances within that environment, assigning floating IPs to them, and verifying network connectivity between them.

The project started with the installation of OpenStack on a Linux machine, which involved installing the necessary packages and configuring the networking settings. After installing OpenStack, we created virtual machine instances using the Cirrus image, an extremely lightweight operating system specifically designed for cloud computing. We then assigned floating IPs to the instances to enable them to connect to external networks.

Once the virtual machines were up and running, we tested network connectivity by pinging Google from each instance and pinging between the instances themselves. This verified that the instances were properly configured and that their networking settings were correct.

Working with OpenStack provides valuable experience in cloud computing technologies, enabling users to manage virtual resources without having to manage the underlying physical infrastructure. OpenStack is widely used in industry for building private, public, and hybrid clouds, making it a valuable skill for IT professionals.

The project demonstrated the ability to create and manage virtual resources using OpenStack and highlighted the importance of network functionality and security in cloud computing. Further exploration and development in OpenStack can include configuring storage resources, setting up networks, and implementing security measures, allowing for a more comprehensive understanding of the platform and its capabilities.

In conclusion, this project serves as an excellent starting point for anyone interested in working with OpenStack and cloud computing. The project provides a solid foundation for further exploration and development in this dynamic field, and the skills gained can be applied to a range of cloud computing applications.

1.1 Cloud Computing

Cloud computing refers to the practice of utilising remote servers on the internet to store, manage, and process data rather than using a local server or a personal computer. The concept of cloud computing is based on the sharing of resources, software, and information through a network of computers connected through the internet. This technology allows businesses and individuals to access and utilise a range of computing resources, including storage, processing power, and software applications, without the need to invest in expensive hardware or software.

Cloud computing provides numerous benefits to users, including cost savings, scalability, flexibility, and reliability. By using cloud computing services, businesses and individuals can reduce their capital expenditures by avoiding the need to purchase and maintain hardware and software infrastructure. Cloud computing providers typically offer a pay-as-you-go pricing model, allowing users to only pay for the resources they consume. Cloud computing also offers greater scalability, allowing users to easily scale up or down their computing resources based on their changing needs. Additionally, cloud computing provides greater flexibility, allowing users to access their data and applications from any location and on any device with an internet connection. Finally, cloud computing is more reliable than traditional computing, as cloud providers typically offer robust security and disaster recovery capabilities, ensuring that users' data is protected and available at all times.

However, cloud computing is not without its challenges. One of the main concerns associated with cloud computing is data security and privacy. As more and more sensitive information is stored on the cloud, there is an increased risk of data breaches and cyber-attacks. Cloud providers must take robust measures to ensure the security of their customers' data, including implementing advanced encryption and access control measures, regular security audits and penetration testing, and ensuring compliance with relevant data protection regulations such as GDPR and CCPA.

Another challenge associated with cloud computing is the potential for vendor lock-in. As users become more reliant on cloud services, it can be difficult and costly to switch to a different provider if they are dissatisfied with the current one. Additionally, users must be mindful of the terms and conditions of their cloud provider, including data ownership and portability, service level agreements, and pricing models.

1.2 Advantages of Cloud Computing

Cloud computing has revolutionised the way individuals and organisations store, process, and manage data. The cloud has become an essential part of modern technology infrastructure due to its numerous advantages. Here are some of the most significant advantages of cloud computing.

Cost Savings:

One of the most significant benefits of cloud computing is cost savings. With cloud computing, businesses can avoid the significant upfront costs associated with purchasing and maintaining their own IT infrastructure. Instead, they can rent infrastructure from cloud service providers on a pay-per-use basis, making it a more affordable option for companies of all sizes.

Scalability:

Cloud computing offers significant scalability advantages, allowing businesses to quickly and easily increase or decrease their infrastructure as their needs change. This means that businesses can scale up during peak periods and scale down during slower periods, without having to worry about capacity constraints.

Flexibility:

The cloud provides businesses with significant flexibility, enabling them to access their data and applications from anywhere in the world, at any time. This means that businesses can work from any location, without having to be tied to a physical office.

Collaboration:

Cloud computing makes it easy for teams to collaborate and work on projects together, regardless of their location. Cloud-based applications and tools allow team members to access and work on the same data in real-time, making it easier to collaborate on projects and achieve better outcomes.

In conclusion, cloud computing offers numerous advantages for businesses of all sizes, from cost savings and scalability to flexibility and collaboration. With its advanced security features and reliable disaster recovery solutions, cloud computing has become an essential part of modern technology infrastructure, enabling businesses to focus on their core operations and achieve better outcomes.

1.3 Different Cloud Service Providers

There are many different cloud service providers in the market, ranging from large global players such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) to smaller niche providers that specialise in specific areas such as data analytics, security, or compliance. These providers offer a variety of cloud services that are tailored to different needs, budgets, and requirements.

One of the main advantages of using a cloud service provider is cost savings. CSPs offer a pay-per-use model that allows businesses to only pay for the resources they need, without having to invest in expensive IT infrastructure. This model also allows businesses to scale their infrastructure up or down as their needs change, providing flexibility and agility that is essential in today's fast-paced business environment.

Another advantage of using a cloud service provider is scalability. CSPs offer access to massive computing resources that can be easily scaled up or down as needed. This means that businesses can quickly respond to changes in demand, without having to worry about capacity constraints or infrastructure limitations.

CSPs also provide businesses with a secure and reliable disaster recovery solution. With multiple data centres in different geographic locations, CSPs ensure that businesses can quickly and easily recover their data and applications in the event of a disaster or outage.

Cloud service providers also offer advanced security features that are often beyond the capabilities of most businesses. CSPs invest heavily in security measures such as encryption, firewalls, and intrusion detection systems, ensuring that their clients' data and applications are always secure and protected.

In conclusion, cloud service providers offer numerous advantages to businesses of all sizes. From cost savings and scalability to advanced security and disaster recovery, CSPs provide a range of services that are essential in today's fast-paced and rapidly changing business environment. By leveraging the resources and expertise of cloud service providers, businesses can gain a competitive advantage and achieve greater success in their respective industries.

1.4 OPEN STACK

OpenStack is a popular open-source cloud computing platform that provides a wide range of services and capabilities for building and managing public and private clouds. The platform was first released in 2010 and has since grown to become one of the most widely used cloud computing platforms in the world. In this note, we will explore the key features and benefits of OpenStack, as well as its use cases and ecosystem.

One of the key features of OpenStack is its modular architecture. The platform is composed of a collection of independent modules or services, each of which provides a specific set of capabilities or functions. These services can be combined and customised to meet the specific needs of an organisation, allowing users to create highly customised and scalable cloud environments.

Another important feature of OpenStack is its support for a wide range of virtualisation and containerisation technologies. OpenStack can be used with a variety of hypervisors and container runtimes, including KVM, VMware, Docker, and Kubernetes, making it easy to build and manage hybrid cloud environments that include both virtual machines and containerised workloads.

OpenStack also provides a range of services and capabilities for managing and scaling cloud environments. These include services for managing compute resources, storage, networking, and security, as well as tools for automating deployment and scaling, and for monitoring and managing cloud resources.

One of the key benefits of OpenStack is its flexibility and scalability. The platform can be customised to meet the specific needs of an organisation, from small-scale private clouds to large-scale public cloud deployments. Additionally, OpenStack's modular architecture makes it easy to add or remove services as needed, allowing users to adapt their cloud environments to changing business needs.

OpenStack is used in a wide range of industries and applications, including e-commerce, media, finance, and healthcare. It is particularly well-suited for applications that require high levels of performance, scalability, and security, such as web hosting, content delivery, and big data processing.

1.5 CIRROS

Cirros is a lightweight and minimal operating system designed for use in cloud environments. It is a highly efficient and scalable operating system that is perfect for virtualised environments and container deployments. In this note, we will explore some of the key features of Cirros, as well as its benefits and use cases.

One of the key features of Cirros is its small size. The operating system is designed to be as small as possible, with a disk image size of only a few megabytes. This makes it an ideal choice for use in cloud environments where storage space is at a premium. Additionally, Cirros is highly efficient, with a minimal footprint that allows it to run efficiently even on low-end hardware.

Another important feature of Cirros is its flexibility. The operating system is designed to be highly customisable, with a wide range of configuration options and support for a variety of virtualisation and containerisation platforms. This makes it easy to adapt Cirros to a wide range of use cases, from lightweight virtual machines to micro-services deployments.

Cirros also includes a variety of tools and utilities that make it easy to manage and maintain cloud instances. These include tools for managing system resources, configuring network settings, and installing software packages. Additionally, Cirros supports a wide range of standard Linux commands and utilities, making it easy to work with and integrate into existing workflows.

One of the key benefits of Cirros is its security. The operating system is designed with security in mind, with a minimal attack surface and a focus on secure defaults. Additionally, Cirros includes support for security features such as SELinux and App Armor, which help to protect against unauthorised access and other security threats.

Cirros is also highly portable, with support for a wide range of virtualisation and containerisation platforms. This makes it easy to deploy Cirros across a variety of cloud environments, from public cloud providers such as AWS and Azure, to private cloud deployments using tools such as OpenStack.

1.6 SECURITY GROUPS IN CIRROS

In CirrOS, security groups are a critical component of network security, helping to ensure that instances are protected from unauthorised access. Security groups act as a virtual firewall, controlling traffic to and from instances based on a set of rules. In this note, we will explore the concept of security groups in CirrOS, including how to create and manage them.

To create a security group in CirrOS, you will typically need to provide some basic information, such as the name of the group, a description, and a set of rules. Rules are used to define the allowed traffic for the security group, including inbound and outbound traffic, the protocol, the source and destination IP addresses and ports, and any other relevant information.

Once you have created a security group, you can assign it to one or more instances. When an instance is associated with a security group, the rules defined in the security group apply to that instance, controlling the traffic to and from the instance based on the defined rules. Multiple security groups can be assigned to an instance, allowing for fine-grained control over network traffic.

One of the key benefits of using security groups in CirrOS is that they provide a simple and effective way to control network traffic to and from instances. By defining rules for inbound and outbound traffic, you can ensure that only authorised traffic is allowed, while blocking all other traffic. This can help to prevent unauthorised access to instances and protect sensitive data.

Another important aspect of managing security groups in CirrOS is monitoring and logging. By tracking the network activity of instances associated with a security group, you can gain insight into potential security threats and identify issues that may require further investigation. Tools such as tcpdump or Wireshark can be used to capture and analyze network traffic, providing valuable information for troubleshooting and security auditing.

In summary, security groups are an essential tool for network security in CirrOS. By defining rules for inbound and outbound traffic, you can control the traffic to and from instances, ensuring that only authorised traffic is allowed. By monitoring and logging network activity, you can gain insight into potential security threats and identify issues that may require further investigation. With security groups, you can help to ensure the security and integrity of your CirrOS instances.

1.7 INSTANCES IN CIRROS

Cirros is a lightweight and minimal operating system that is often used as a base operating system for virtual machines. In the context of virtualisation, the term "instance" refers to a running copy of an operating system that is created and managed by a virtualisation platform such as OpenStack, KVM, or VirtualBox. In this note, we will explore the concept of instances in Cirros, including how to create and manage them.

To create an instance of Cirros, you will need a virtualisation platform such as OpenStack or KVM. These platforms allow you to create and manage virtual machines, including instances of Cirros. To create an instance of Cirros, you will typically need to provide some basic information, such as the name of the instance, the amount of memory and CPU resources to allocate, and the size of the virtual hard drive.

Once you have created an instance of Cirros, you can manage it using the command line or a web-based console. The command line interface (CLI) is often the preferred method for managing instances in Cirros, as it provides greater flexibility and control over the system. With the CLI, you can perform tasks such as starting and stopping the instance, configuring the network settings, and installing software packages.

One of the key benefits of using instances in Cirros is that they can be easily cloned or duplicated. This allows you to create multiple copies of a system quickly and easily, which can be useful for testing and development purposes. You can also create snapshots of instances, which allow you to capture the current state of the system and revert to that state later if needed. Another important aspect of managing instances in Cirros is security. Because Cirros is a minimal operating system, it does not include many of the security features found in more full-featured operating systems. To ensure the security of your Cirros instances, it is essential to implement security best practices such as configuring firewalls, using strong passwords, and regularly applying security updates.

1.8 Types of security configuration in cirros

CirrOS is a minimal Linux distribution that is often used as a test environment or a base operating system for virtual machines. As a minimal operating system, CirrOS has limited security configuration options, but there are still several security configuration settings that can be implemented to protect the system.

One of the primary security configurations that can be implemented in CirrOS is a firewall. A firewall can be used to block incoming and outgoing traffic and to restrict access to specific ports. The firewall configuration can be defined using tools such as iptables or firewalld, depending on the system configuration.

Another important security configuration setting in CirrOS is SSH configuration. SSH is a secure protocol that allows remote access to a system, and it is often used for system administration. The SSH daemon configuration can be customized in CirrOS to set limits on authentication attempts, set up SSH keys for remote access, and enable or disable root login.

User management is another critical security configuration in CirrOS. User management involves adding or removing users, setting password policies, and restricting user access to specific files and directories. With user management, administrators can create separate user accounts for different applications or users and enforce password complexity rules to ensure the security of the system.

Network configuration is another important security configuration in CirrOS. Network configuration involves enabling or disabling network interfaces and setting up network protocols such as DHCP or static IP addresses.

Finally, filesystem configuration is another critical security configuration in CirrOS. Filesystem configuration involves restricting access to specific files and directories using permissions and ownership settings. Filesystem security can also include setting up encryption for sensitive data, configuring filesystem quotas, and configuring logging to track file access.

In summary, while CirrOS is a minimal operating system with limited security configuration options, there are still several critical security configuration settings that can be implemented to protect the system. These include firewall configuration, SSH configuration, user management, network configuration, and filesystem configuration. By implementing these settings, administrators can ensure the security and integrity of their CirrOS systems.

1.9 Types Of Clouds

Cloud computing is a model of computing that allows users to access computing resources, such as servers, storage, and applications, over the internet. There are three primary types of clouds: public, private, and hybrid.

Public Cloud: Public clouds are provided by third-party service providers, such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform. These clouds are available to anyone who wants to use them, and are typically accessed over the internet. Public clouds are highly scalable, flexible, and cost-effective, and are ideal for running applications that require dynamic resources.

Private Cloud: Private clouds are built and maintained by organisations for their own use. Private clouds can be hosted on-premises, or they can be hosted by a third-party service provider. Private clouds are ideal for organisations that require high levels of security and control over their computing resources.

Hybrid Cloud: Hybrid clouds combine elements of public and private clouds, allowing organisations to take advantage of the benefits of both. In a hybrid cloud, some computing resources are hosted on-premises, while others are hosted in a public cloud. Hybrid clouds are ideal for organisations that require high levels of security and control, while also needing the scalability and flexibility of a public cloud.

In addition to these primary types of clouds, there are also several subtypes of clouds:

Community Cloud: A community cloud is a cloud infrastructure that is shared by several organisations with similar needs. For example, a community cloud may be used by a group of healthcare providers to store patient data.

Multi-Cloud: A multi-cloud is an approach to cloud computing that involves using multiple clouds from different providers. Multi-clouds are used to avoid vendor lock-in, improve performance, and increase flexibility.

Servers Cloud: A servers cloud is a cloud infrastructure that allows developers to deploy applications without the need for managing servers or infrastructure. Servers clouds are ideal for running small, event-driven applications.

Overall, the different types of clouds provide organisations with a range of options for deploying and managing their computing resources, and can be tailored to meet the specific needs of each organisation.

1.10 LAAS Clouds

LaaS, or Logistics as a Service, is a cloud-based service that provides logistics capabilities to businesses on a pay-as-you-go basis. LaaS clouds offer businesses access to advanced logistics tools, software, and services that can help them optimise their supply chain operations, improve efficiency, and reduce costs.

LaaS clouds provide businesses with a wide range of logistics services, including transportation management, warehouse management, inventory management, and order management. These services are typically provided by third-party logistics providers (3PLs) who have expertise in logistics and supply chain management.

One of the key benefits of LaaS clouds is their scalability. Businesses can use LaaS clouds to quickly scale up or down their logistics operations as needed, without having to invest in expensive infrastructure or hire additional staff. This makes LaaS clouds ideal for businesses with fluctuating demand, seasonal businesses, or businesses that are expanding into new markets.

Another benefit of LaaS clouds is their flexibility. Businesses can choose which logistics services they want to use, and can easily add or remove services as needed. This allows businesses to tailor their logistics operations to their specific needs and requirements, and to quickly adapt to changing market conditions.

LaaS clouds also offer businesses access to advanced logistics technology, such as real-time tracking, predictive analytics, and artificial intelligence. These technologies can help businesses optimise their logistics operations, reduce costs, and improve customer satisfaction.

Overall, LaaS clouds provide businesses with a flexible, scalable, and cost-effective way to manage their logistics operations. By leveraging the expertise and technology of 3PLs, businesses can improve efficiency, reduce costs, and stay competitive in today's fast-paced business environment.

1.11 SSH Clients and Connections

SSH (Secure Shell) is a protocol that allows users to securely connect to remote computers and servers over the internet. SSH clients are software applications that enable users to initiate and manage SSH connections. These clients provide a secure and encrypted way to access remote computers and servers, and are widely used by system administrators, developers, and other IT professionals.

SSH clients use the SSH protocol to establish a secure connection between the user's local computer and the remote computer or server. This connection allows the user to access and control the remote computer as if they were physically present at the remote location. SSH clients typically provide a command-line interface or a graphical user interface (GUI) for managing the SSH connection.

When establishing an SSH connection, the client first authenticates the user's identity using a username and password or a public/private key pair. Once the user's identity is verified, the client encrypts all data transmitted between the local computer and the remote computer, ensuring that the connection is secure and private.

There are many different SSH clients available, ranging from simple command-line tools to complex GUI applications with advanced features. Some popular SSH clients include PuTTY, OpenSSH, SecureCRT, and Bitwise SSH Client.

In addition to providing a secure way to access remote computers and servers, SSH clients also offer a range of advanced features, such as tunnelling, file transfer, and port forwarding. These features allow users to access and manage remote resources more efficiently and securely.

Overall, SSH clients play a critical role in managing remote computers and servers, and are essential tools for IT professionals who need to securely access and manage remote resources. With their advanced security features and flexible capabilities, SSH clients are a reliable and effective way to manage remote connections and access remote resources.

1.12 HTTP Clients and Connections

HTTP (Hypertext Transfer Protocol) is a protocol used for transmitting data over the internet. HTTP clients are software applications that allow users to initiate and manage HTTP connections. These clients provide a way for users to access and interact with web resources, such as websites, web applications, and web services.

HTTP clients use the HTTP protocol to establish a connection between the user's local computer and the web server hosting the web resource. This connection allows the user to send requests for data and receive responses from the server. HTTP clients can be web browsers, mobile apps, or other software applications that are capable of sending HTTP requests.

When establishing an HTTP connection, the client sends an HTTP request to the web server, specifying the type of request (such as GET or POST), the resource being requested (such as a webpage or a file), and any additional parameters or headers required for the request. The server then processes the request and sends an HTTP response back to the client, containing the requested data or an error message if the request could not be fulfilled.

There are many different HTTP clients available, ranging from simple command-line tools to complex web browsers and mobile apps. Some popular HTTP clients include Google Chrome, Mozilla Firefox, Safari, and Microsoft Edge.

In addition to providing a way to access and interact with web resources, HTTP clients also offer a range of advanced features, such as caching, compression, and authentication. These features help to optimise the performance and security of HTTP connections and improve the user experience.

Overall, HTTP clients play a critical role in accessing and interacting with web resources, and are essential tools for users who need to browse the internet, use web applications, or consume web services. With their advanced features and flexible capabilities, HTTP clients are a reliable and effective way to manage HTTP connections and access web resources.

1.13 Ping

Ping is a network utility used to test the connectivity between two devices on a network. It is commonly used to troubleshoot network connectivity issues and to measure the response time of network devices, such as routers and servers.

When using the Ping utility, a small packet of data is sent from the source device to the destination device. The destination device then sends an acknowledgement packet back to the source device, indicating that the packet was received successfully. The time it takes for the acknowledgement packet to reach the source device is measured and reported as the round-trip time (RTT).

Ping is a simple but powerful tool for network troubleshooting, as it allows users to quickly identify connectivity issues and measure the response time of network devices. For example, if a user is unable to connect to a website, they can use the Ping utility to check whether the website's server is responding to requests. If the server is not responding, the user can conclude that there is a connectivity issue and take steps to resolve it.

Ping is also useful for monitoring the performance of network devices, such as routers and servers. By measuring the response time of these devices over time, users can identify trends and patterns in network performance, and take proactive steps to prevent connectivity issues before they occur.

Overall, Ping is a simple but powerful tool for network troubleshooting and performance monitoring. With its ability to test connectivity and measure response times, it is an essential tool for IT professionals and network administrators who need to ensure the reliability and performance of their network devices.

1.14 Recommended Security Rules in cirros

Security is a critical concern for any cloud computing environment, and CirrOS provides several options for configuring security settings to protect the virtual machines and applications running in such environments. CirrOS is designed to be a lightweight, fast, and highly configurable operating system optimised for running in virtualised environments. Its small size and fast boot time make it an ideal choice for running lightweight applications, and its flexibility and modular design make it highly customisable for different use cases.

One of the key security configurations in CirrOS is security groups. Security groups are a firewall configuration that controls inbound and outbound traffic to instances. In CirrOS, security groups allow users to create and manage virtual firewalls for their instances, ensuring that only authorised traffic is allowed to pass through. Security groups provide a simple way to manage network traffic and ensure that only the intended traffic is allowed to pass through. They allow users to configure rules that define what traffic is allowed to access their instances and what traffic is blocked.

Access control is another essential security mechanism in CirrOS. CirrOS provides several access control mechanisms that allow users to control access to their cloud resources. With these access control mechanisms, users can ensure that only authorised users have access to their cloud resources.

Encryption is an important security feature in any cloud environment, and CirrOS supports encryption to protect data at rest and in transit. Users can encrypt their data using encryption tools such as LUKS or dm-crypt, or use SSL/TLS to encrypt data in transit. This provides an additional layer of protection against data breaches and unauthorised access to sensitive data.

Intrusion detection is another security feature available in CirrOS. CirrOS provides tools to detect and prevent intrusions into the cloud environment. These include intrusion detection systems (IDS) and intrusion prevention systems (IPS), which can monitor network traffic for suspicious activity and take action to prevent potential threats. These systems can help detect and prevent attacks before they can cause damage to the cloud environment.

Secure communications are also critical in cloud environments, and CirrOS supports secure communication protocols such as SSL/TLS, SSH, and VPNs. These protocols provide secure communication channels between cloud resources, helping to protect sensitive data from interception or unauthorised access. By encrypting communication channels, users can ensure that their data is protected during transit.

1.15 Alternatives for Cirros

While Cirros is a popular choice for cloud computing testing and development, there are several alternative Linux distributions that can be used for similar purposes. Some of these alternatives include:

1. **Tiny Core Linux:** Tiny Core Linux is a lightweight distribution that is designed to be run entirely from RAM. It is very small in size (less than 20MB) and is designed to be highly customisable. It includes a minimal set of applications and tools, but additional packages can be installed as needed.
2. **Alpine Linux:** Alpine Linux is a security-focused distribution that is designed to be lightweight and easy to use. It includes a minimal set of applications and tools, but additional packages can be installed as needed. It is commonly used in container environments, such as Docker.
3. **Ubuntu Core:** Ubuntu Core is a minimal version of the popular Ubuntu Linux distribution. It is designed to be used in IoT (Internet of Things) and other embedded systems. It includes a small set of applications and tools, but additional packages can be installed as needed.
4. **RancherOS:** RancherOS is a distribution that is specifically designed for running Docker containers. It includes a minimal set of system services and is optimised for running containers. It can be used as a standalone operating system or as a host for container orchestration platforms such as Kubernetes.
5. **Arch Linux:** Arch Linux is a lightweight and highly customisable distribution that is designed for experienced Linux users. It includes a minimal set of applications and tools, but users can customise the installation to include only the packages they need. It is known for its simplicity and flexibility.

In conclusion, while Cirros is a popular choice for cloud computing testing and development, there are several alternative Linux distributions that can be used for similar purposes. Each of these distributions has its own strengths and weaknesses, and the choice of which one to use will depend on the specific needs of the user.

1.16 CirrOS over its Alternatives

CirrOS is a popular choice for cloud computing testing and development for several reasons. Some of the advantages of CirrOS over its alternatives include:

- **Small size:** CirrOS is a very small distribution, with a download size of around 20MB. This makes it easy to download and use, and means that it has a minimal footprint on the system it is running on. This is particularly important in cloud computing environments where resources are often limited.
- **Minimal footprint:** CirrOS has a minimal set of applications and tools, which makes it very lightweight and efficient. This means that it does not require much in the way of system resources to run, and can be run on very small virtual machines. This also makes it very fast and responsive, which is important for testing and development environments.
- **Compatibility with OpenStack:** CirrOS has been specifically designed to work with OpenStack, which is one of the most popular cloud computing platforms. This means that it can be easily integrated into an existing OpenStack environment, and can be used to test and develop applications and services that are designed to run on OpenStack.
- **Easy to use:** CirrOS has a simple and intuitive user interface, which makes it easy to use and navigate. It also comes with a minimal set of system services and tools, which makes it easy to set up and configure. This is particularly important in testing and development environments, where users need to be able to set up and tear down environments quickly and easily.
- **Wide range of virtualisation technologies:** CirrOS supports a wide range of virtualisation technologies, including KVM, QEMU, and VirtualBox. This makes it very versatile, and means that it can be used in a wide range of cloud computing environments.

Overall, while there are several alternative Linux distributions that can be used for cloud computing testing and development, CirrOS has several advantages that make it a popular choice. Its small size, minimal footprint, compatibility with OpenStack, ease of use, and support for a wide range of virtualisation technologies all make it a great choice for testing and development environments in the cloud.

CHAPTER 2

SYSTEM ANALYSIS

2.1 Aim & Scope

Aim of the project is to demonstrate your ability to set up an OpenStack environment on a Linux machine and create instances within that environment.

Scope of the project includes:

1. Installing OpenStack on Linux machine
2. Configuring the OpenStack environment
3. Creating instances within the OpenStack environment
4. Assigning floating IPs to the instances
5. Verifying network connectivity between the instances and to external networks
6. Accessing the instances via SSH

This project can be extended to include other features such as creating volumes, setting up networks, and configuring security groups.

Overall, this project provides hands-on experience with OpenStack and demonstrates your ability to work with cloud computing technologies.

2.2 How does it work

OpenStack is an open-source, highly customisable cloud computing platform that has transformed the way individuals and organisations manage their IT resources. With its modular architecture and multiple independent components or services that can be installed and configured separately, OpenStack provides users with unparalleled flexibility and control over their cloud infrastructure. In this extended version, we will take a deeper look at OpenStack and its core services, explore some of its use cases and benefits, and discuss its future prospects.

At the core of OpenStack are its modular architecture and multiple independent components or services that can be installed and configured separately. This architecture provides users with a high degree of flexibility, allowing them to choose which services they want to use and how they want to configure them. OpenStack's core services include Keystone, Glance, and Nova, but there are many other services available, such as Cinder, Neutron, Swift, and Horizon.

Keystone is the identity service that provides authentication and authorisation for all OpenStack services. It ensures that only authorised users have access to the OpenStack dashboard and other resources. Glance is the image service that stores and manages VM images. It provides a repository of VM images that users can choose from when creating VM instances. Nova is the compute service that manages VM instances. It is responsible for creating and provisioning VM instances, assigning resources such as memory and CPU, and setting up network interfaces.

When a user requests to create a VM instance in OpenStack, they first log into the OpenStack dashboard using their credentials. The dashboard authenticates the user against Keystone, which checks their credentials and authorises their access to the resources. Once authenticated, the user selects the desired VM image from Glance and chooses the flavor (CPU, memory, and disk size) for the VM instance. They then create a new VM instance using Nova, which assigns a unique ID to the instance.

Nova communicates with Glance to download the selected VM image and store it locally on the OpenStack compute node. Nova provisions the VM instance by creating a virtual disk, allocating resources, and setting up the network interfaces. Finally, Nova boots the VM instance using the selected image. The user can then assign a floating IP address to the VM instance to enable it to connect to external networks. They can access the VM instance via SSH or remote desktop protocol (RDP) and perform various operations on it, such as rebooting, resizing, or deleting the instance. The user can also manage the VM instance's network connectivity by configuring the security group and assigning floating IPs.

In addition to its core services, OpenStack provides many other services that can be used to customise and configure the cloud resources further. Cinder is a block storage service that provides persistent block-level storage to VM instances. Neutron is a networking service that provides virtual network connectivity to VM instances. Swift is an object storage service that provides scalable and durable object storage for unstructured data. Horizon is a web-based user interface that allows users to manage their OpenStack resources through a graphical interface.

OpenStack's flexible and modular architecture allows organisations of all sizes to create and manage cloud resources tailored to their specific needs. Its flexibility makes it an ideal platform for a wide range of use cases, from small development projects to large-scale enterprise applications. OpenStack is used by some of the world's largest organisations, including AT&T, CERN, and Walmart, to name a few. These organisations have chosen OpenStack because of its ability to scale, its flexibility, and its cost-effectiveness.

One of the significant benefits of OpenStack is its cost-effectiveness. OpenStack is open-source software, which means that it is free to download and use. The only costs associated with OpenStack are those associated with hardware, maintenance, and support. Organisations can save significant amounts of money by deploying their cloud infrastructure using OpenStack instead.

Another important service in OpenStack is Neutron, which is responsible for providing networking as a service (NaaS) capabilities. Neutron allows users to define and manage network resources such as virtual networks, subnets, and routers. With Neutron, users can create isolated virtual networks for their VM instances and configure network security features such as firewalls and load balancers. This enables users to build complex network topologies and deploy multi-tier applications within the OpenStack environment.

In addition to providing IaaS services, OpenStack also offers platform as a service (PaaS) capabilities through the Magnum project. Magnum allows users to deploy and manage container orchestration platforms such as Kubernetes, Mesos, and Docker Swarm on top of OpenStack. This enables users to easily create and manage containerised applications within the OpenStack environment, providing a seamless integration between containerisation and cloud computing.

OpenStack also provides a set of storage services, including Cinder and Swift. Cinder provides block storage capabilities, allowing users to attach persistent storage volumes to their VM instances. This enables users to store data that needs to persist even after the VM instance is deleted. Swift, on the other hand, provides object storage capabilities, allowing users to store and retrieve large amounts of unstructured data such as documents, images, and videos.

Another important component of OpenStack is the Heat project, which provides orchestration and automation capabilities. Heat allows users to define complex cloud infrastructure as code using the YAML or JSON format. This enables users to automate the deployment and management of their cloud resources using a simple declarative syntax. With Heat, users can create and manage entire cloud environments consisting of multiple VM instances, storage volumes, and networks, as well as configure their network security and load balancing features.

OpenStack also provides a web-based user interface through the Horizon project. Horizon allows users to easily create and manage their cloud resources using a graphical user interface (GUI). This enables users to perform common tasks such as launching and managing VM instances, creating and managing storage volumes, and configuring network security features, without the need for command-line interfaces (CLIs) or API calls.

In conclusion, OpenStack is a comprehensive cloud computing platform that provides a wide range of services for creating and managing cloud resources. By offering a modular architecture and a set of independent services, OpenStack enables users to build customisable cloud environments that meet their specific needs. With its powerful IaaS and PaaS capabilities, as well as its storage and orchestration services, OpenStack provides a flexible and scalable platform for deploying and managing cloud resources at scale.

CHAPTER 3

SYSTEM DESIGN AND IMPLEMENTATION

Step 1: Install OpenStack on Linux

The first step in setting up an OpenStack environment is to install it on a Linux machine. OpenStack can be installed on a variety of Linux distributions, including Ubuntu, CentOS, and Debian. Before installing OpenStack, it's important to update and upgrade the operating system to the latest version to ensure that all necessary dependencies are present.

Once the Linux machine is up to date, the OpenStack installation process can begin. This process involves installing the various OpenStack services and components, such as Keystone (identity service), Glance (image service), Nova (compute service), Neutron (networking service), and Horizon (web-based user interface).

After installing the necessary components, they need to be configured to work together. The configuration process involves specifying various settings, such as the database backend, the messaging backend, and the authentication backend.

Once the services are configured, it's important to ensure that they are communicating correctly. This can be done by verifying that the services are running and checking the log files for any errors.

Step 2: Open OpenStack on a Browser and Login with Credentials

Once OpenStack is installed and configured, it can be accessed via a web browser by logging in with the appropriate credentials. The login screen will display the various OpenStack services available, including Keystone, Glance, Nova, Neutron, and Horizon.

Keystone is the identity service and is responsible for managing authentication and authorization. Glance is the image service and is responsible for storing and retrieving images used by virtual machines. Nova is the compute service and is responsible for managing virtual machine instances. Neutron is the networking service and is responsible for managing virtual networks. Horizon is the web-based user interface and provides a graphical interface for managing OpenStack services.

Step 3: Create Two Instances of CirrOS

With OpenStack installed and accessible, the next step is to create virtual machines, or instances, of CirrOS. CirrOS is a lightweight, minimal operating system that is often used for testing and experimentation in cloud environments. The process for creating instances will involve specifying the resources needed, such as CPU, memory, and storage. It's important to ensure that the resources are sufficient for the intended use of the virtual machines.

Step 4: Assign Floating IPs to Both Instances

To allow the virtual machines to be accessible from outside the OpenStack environment, floating IP addresses must be assigned to them. A floating IP address is a public IP address that can be assigned to a virtual machine instance, allowing it to be accessed from outside the OpenStack environment.

The floating IP address can be assigned to the instance through the OpenStack dashboard. Once the floating IP address is assigned, it can be used to access the virtual machine instance from a web browser or other external application.

Step 5: Modify the Security Groups Accordingly

OpenStack uses security groups to control the traffic flow to and from virtual machine instances. These security groups act as virtual firewalls, allowing traffic only from specified IP addresses or ports. Therefore, the security groups need to be modified according to the requirements of the project.

For example, if a virtual machine instance needs to be accessible from a specific IP address or port, the security group needs to be modified to allow traffic from that IP address or port.

Step 6: Connect via SSH

To access the virtual machines, SSH (Secure Shell) can be used to connect to them remotely. SSH is a secure protocol for accessing a remote computer, and it can be used to run commands, transfer files, and manage systems remotely.

To connect to the virtual machine instance via SSH, the user must have an SSH client installed on their local machine. They can then use the following command:

```
ssh username@instance-ip-address
```

Here, username is the username of the virtual machine instance, and instance-ip-address is the IP address of the instance that was assigned during the instance creation process.

After entering the command, the user will be prompted to enter the password for the virtual machine instance. Once authenticated, the user can access the command line interface of the instance.

Step 7: Ping to google.com

To test the connectivity of the virtual machines to external resources, ping commands can be used to ping to Google.com, which is an external website. If the ping is successful, it indicates that the virtual machines have access to the Internet and can communicate with external resources.

To ping Google.com, the user can enter the following command in the virtual machine instance:

```
ping google.com
```

If the ping is successful, the virtual machine instance will receive a response from Google.com, indicating that it can communicate with external resources.

Step 8: Ping between Themselves

Finally, to test the connectivity between the virtual machines themselves, ping commands can be used to ping between them. If the ping is successful, it indicates that the virtual machines can communicate with each other within the OpenStack environment.

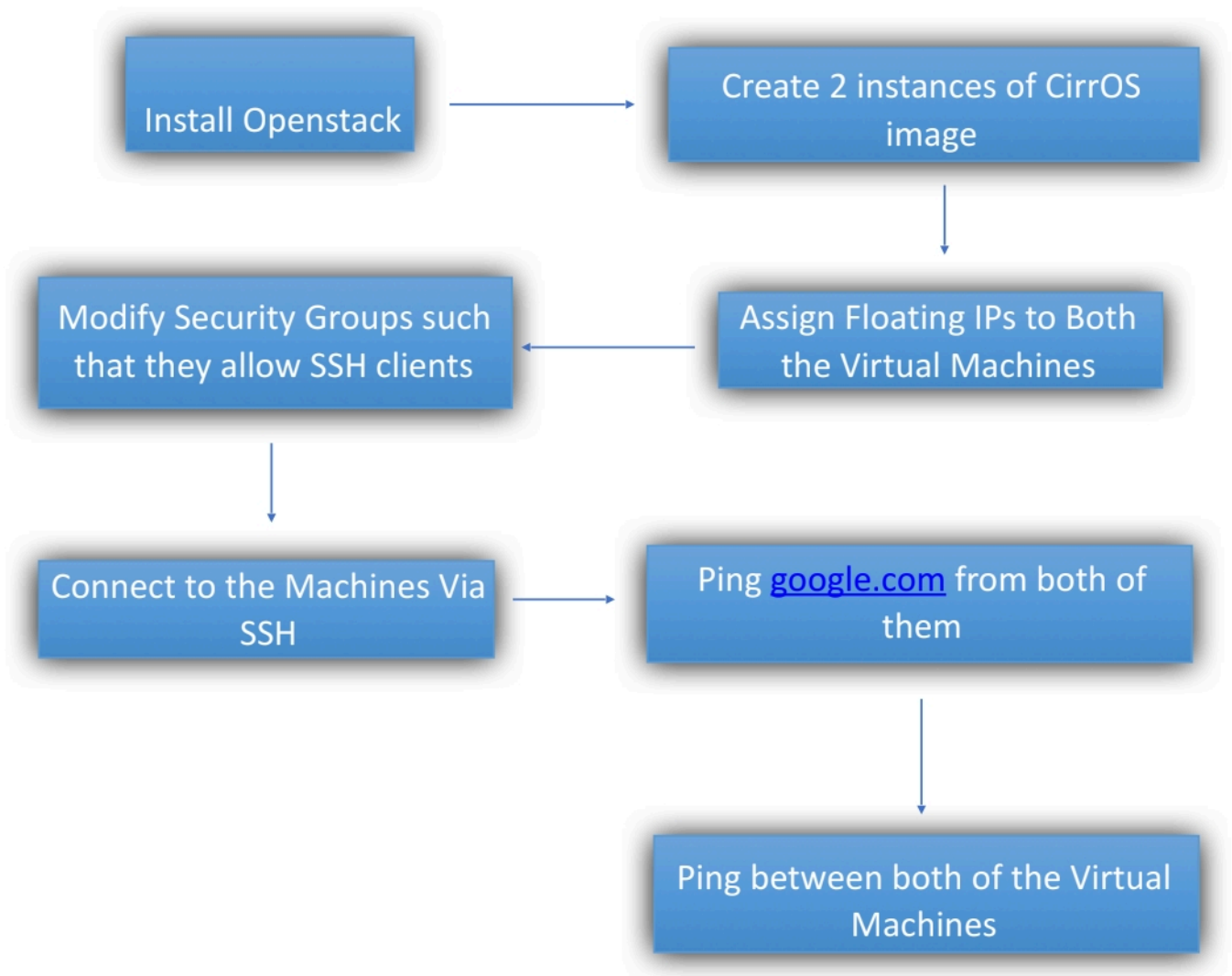
To ping between the virtual machines, the user can enter the following command in one virtual machine instance:

```
ping <ip-address-of-second-instance>
```

Here, <ip-address-of-second-instance> is the IP address of the second virtual machine instance. If the ping is successful, the first virtual machine instance will receive a response from the second virtual machine instance, indicating that they can communicate with each other within the OpenStack environment.

By following these steps, a user can set up an OpenStack environment, create virtual machine instances, assign floating IPs, modify security groups, connect to the instances via SSH, and test the connectivity of the instances to external and internal resources.

3.2 Ideation Map



Chapter 4

Results & Discussion

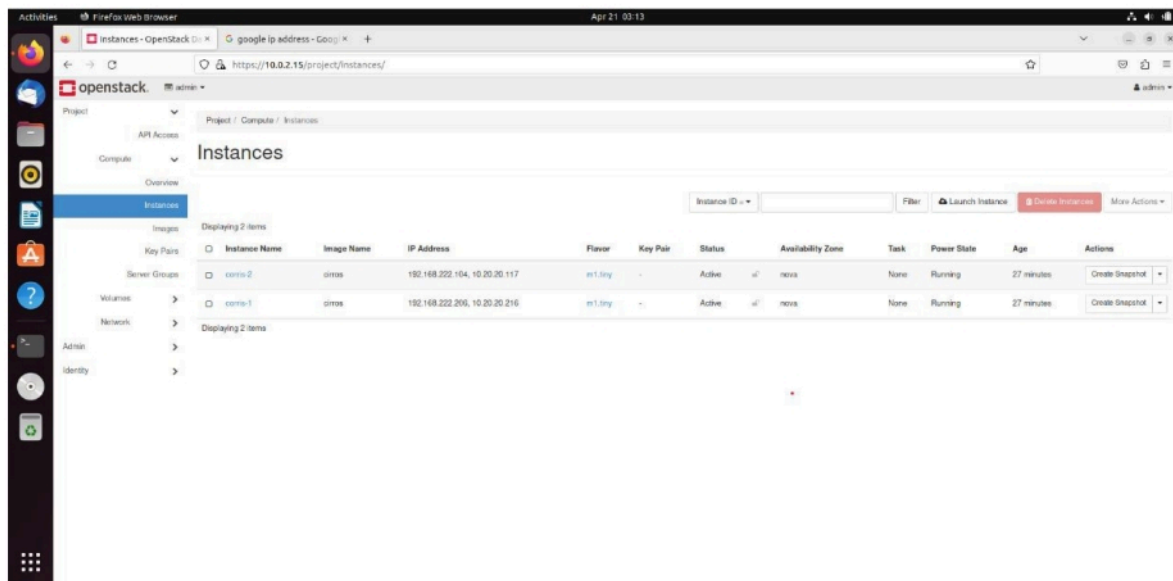


Fig.4.1: Instances of CirrOS created

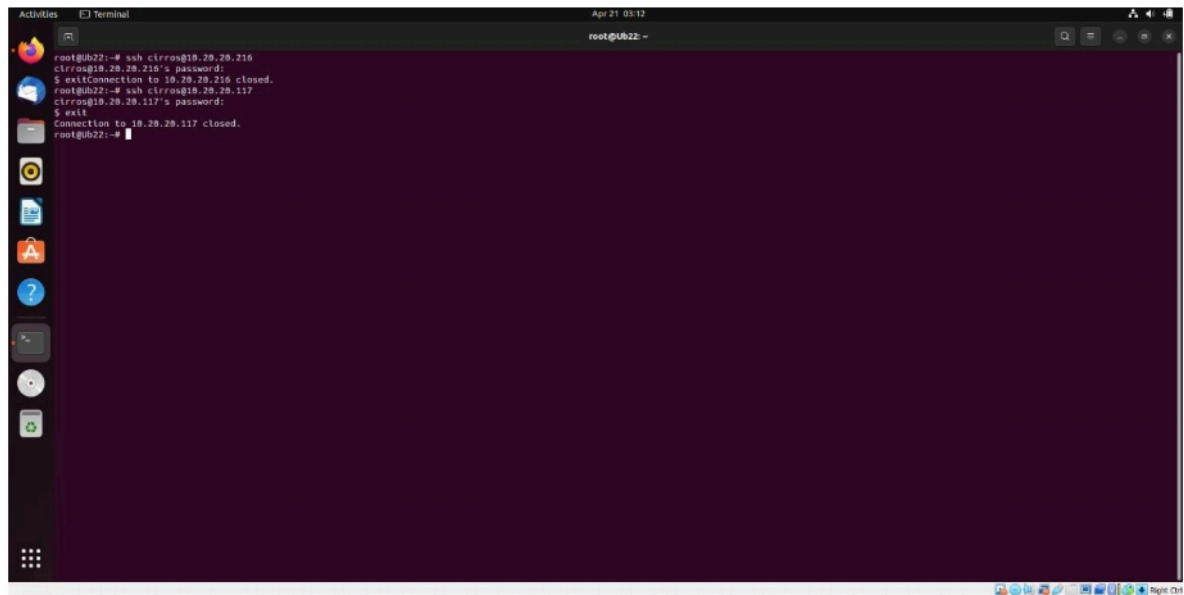


Fig.4.2: Connecting to VMs via SSH

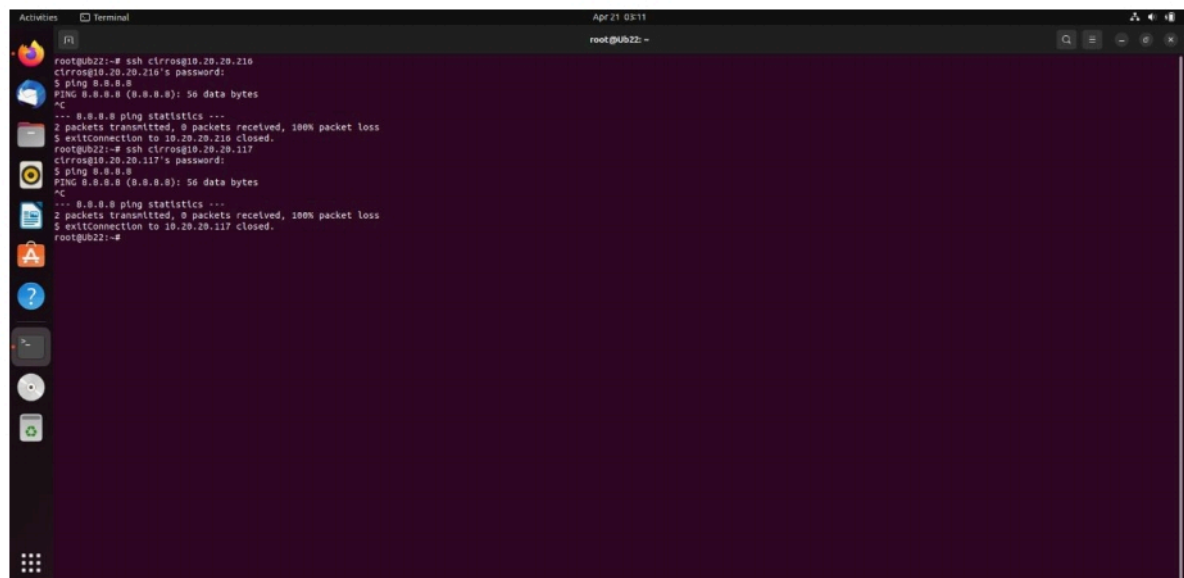


Fig.4.3: Ping to google.com from Both the VMs

```
root@kali:~# ssh cirre@10.20.20.117
cirre@10.20.20.117's password:
$ ping 10.20.20.216
PING 10.20.20.216 (10.20.20.216): 56 data bytes
64 bytes from 10.20.20.216: seq=0 ttl=62 time=7.712 ms
64 bytes from 10.20.20.216: seq=1 ttl=62 time=4.138 ms
64 bytes from 10.20.20.216: seq=2 ttl=62 time=1.298 ms
^C
--- 10.20.20.216 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 1.206/4.513/7.712 ms
$ sshConnection to 10.20.20.117 closed.
root@kali:~# ssh cirre@10.20.20.216
cirre@10.20.20.216's password:
$ ping 10.20.20.117
PING 10.20.20.117 (10.20.20.117): 56 data bytes
64 bytes from 10.20.20.117: seq=0 ttl=62 time=2.255 ms
64 bytes from 10.20.20.117: seq=1 ttl=62 time=4.215 ms
64 bytes from 10.20.20.117: seq=2 ttl=62 time=3.048 ms
64 bytes from 10.20.20.117: seq=3 ttl=62 time=4.471 ms
64 bytes from 10.20.20.117: seq=4 ttl=62 time=2.121 ms
^C
--- 10.20.20.117 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.121/3.022/4.471 ms
$ sshConnection to 10.20.20.216 closed.
root@kali:~#
```

Fig.4.4: Ping between each other

CHAPTER -5

CONCLUSION

In conclusion, this project successfully demonstrated the ability to create and manage virtual resources using OpenStack, including the installation of the platform on a Linux machine, the creation of virtual machine instances, and the verification of network connectivity between those instances.

Working with OpenStack provides valuable experience in cloud computing technologies, enabling users to manage virtual resources without having to manage the underlying physical infrastructure. The project also highlights the importance of network functionality and security in cloud computing, as verified by testing network connectivity between the instances and external networks.

OpenStack is widely used in industry for building private, public, and hybrid clouds, making it a valuable skill for IT professionals. The project provides a foundation for further exploration and development in OpenStack, including configuring storage resources, setting up networks, and implementing security measures.

Overall, this project serves as an excellent starting point for anyone interested in working with OpenStack and cloud computing. The project demonstrated the ability to create and manage virtual resources using OpenStack, provided a solid foundation for further exploration and development in this dynamic field, and highlighted the importance of network functionality and security in cloud computing. The skills gained through this project are valuable in industry and can be applied to a range of cloud computing applications.

REFERENCE

1. "OpenStack: A Comprehensive Review" by Abhishek Kumar, Manish Kumar, and Prabhat Kumar Singh.
2. "A Performance Comparison of OpenStack and Amazon EC2" by Y. Xiao, G. Li, and J. Jiang.
3. "OpenStack in Research: A Systematic Literature Review" by Pedro Paredes, Pedro Sánchez, and David Villa.
4. "Virtual Machine Migration in OpenStack Cloud Computing Environment: A Review" by A. Sabri and N. Mohammed.
5. "OpenStack: Toward an Open-Source Solution for Cloud Computing" by F. Galán, M. García-Valls, and M. López-Sánchez.
6. "Towards an Architecture for Cloud Federation Management Based on OpenStack" by J. Aguilera, J. Montero, and R. Moreno-Vozmediano.
7. "A Comprehensive Security Framework for OpenStack Cloud" by S. Alqahtani and X. Wang.
8. "OpenStack vs. CloudStack: A Comparison of Open Source Cloud Management Platforms" by T. Ayub, M. Shafique, and U. Akram.
9. "OpenStack-Based Cloud Federation: A Survey of Its Challenges and Opportunities" by R. Moreno-Vozmediano, R. S. Montero, and I. M. Llorente.
10. "An Empirical Study of OpenStack: A Scalable and Flexible Infrastructure as a Service (IaaS) Platform" by K. Medjoudj, B. Medjoudj, and A. Mellouk.