**Student Assessment Submission and Declaration**

When submitting evidence for assessment, each student must sign a declaration confirming that the work is their own.

|  |  |  |  |
| --- | --- | --- | --- |
| Student name:Shahed Montaser | | Assessor name: Rama Al-Share | |
| Issue date (5-4-2023): | Submission date (5-6-2023): | | Submitted on: |
| In case of resubmission | | | |
| Issue date (1St Submission): | Submission date (1St Submission): | | Submitted on: |
| Programme: Higher National Diploma in computing | | | |
|  | | | |
| Assignment number and title:1. **Investigating Cloud Technologies** | | | |

Q1.

Three distinct cloud network architecture deployment strategies are described below for businesses to consider.

=>Built-in networking tools: The first approach is to merely make use of the networking tools that come built into the CSP as a standard component of the IaaS service. Using the Amazon Virtual Private Cloud service, for instance, gives you control over the fundamentals, like assigning private IP addresses of your choice, segmenting the virtual network into different subnets, and setting and enforcing security policies for each subnet. The route table, internet gateways, and supplementary network services like Dynamic Host Configuration Protocol and DNS are also within your control. The IaaS cloud must be configured and managed separately from any other private or public clouds if you use the built-in networking tools.

The following are some benefits and limitations of cloud-based networking tools:

Advantages:

-Scalability: The networking tools integrated into the cloud can be adjusted up or down in accordance with the needs of the organization. This implies that organizations don't need to worry about their networking equipment' capability adapting to variations in traffic or usage.

-Cost-effectiveness: Using networking solutions that are already incorporated into the cloud may be less expensive than setting up and maintaining an on-premises networking infrastructure. Businesses can avoid the up-front expenditures of purchasing and maintaining gear and software by using cloud networking tools.

-Accessibility: Networking tools integrated into the cloud are reachable from any location with an internet connection. This makes it possible for companies to control their networking infrastructure whenever and from wherever they are, which can be especially helpful for remote workers.

-Security: Many networking solutions that are integrated into the cloud also include built-in security protections that can help shield enterprises from online dangers. Firewalls, intrusion detection, and data encryption are some examples of these characteristics.

Constraints:

-Control: Businesses may have less control over their networking infrastructure using cloud-integrated networking technologies than they would with an on-premises architecture. The network may become more challenging to adapt to specific needs as a result.

-Latency: The built-in networking capabilities of the cloud rely on the internet, which might cause delays in communication. Businesses that need real-time communication or high-performance networking may find this to be particularly difficult.

-Reliability: Problems like network congestion or outages may have an impact on how reliable cloud networking products are. Some businesses may be concerned that they will need to rely on their cloud provider to guarantee uptime and dependability.

-Complexity: Setting up and managing cloud-integrated networking tools can be challenging, especially for companies without a dedicated IT staff. Because of this, it could be challenging to utilize the networking technologies' capabilities to their maximum potential.

=>Virtual networking appliances: A second approach is to manage networking tasks using virtual networking appliances from a networking vendor rather than the built-in tools provided by the cloud provider. On well-known IaaS markets, organizations like Cisco, Arista, Juniper, and SonicWall sell various variations of their virtualized routers, firewalls, and software-defined WAN appliances.

To more closely resemble network configurations already developed in their private data centers, businesses considering a hybrid cloud may wish to investigate if they can integrate one or more virtual appliances from a third party into the IaaS. Both initial configuration and ongoing management and maintenance will become much simpler as a result.

Before choosing to employ them, enterprises should take into account the advantages and limitations that cloud virtual networking equipment provide. Some of the more significant ones are listed below:

Advantages:

-Flexibility: Businesses may simply scale up or down virtual networking equipment to match their networking needs without investing in pricey hardware. This may be especially helpful for businesses that are expanding or experiencing demand shifts.

-Cost-effective: Since they don't require any capital investments and companies just pay for what they actually use, cloud virtual networking equipment are frequently less expensive than their hardware equivalents.

-Security: To provide effective defense against online threats, virtual networking appliances are equipped with a variety of built-in security capabilities, including firewalls, intrusion detection systems, and data encryption.

-Remote management: Because virtual networking equipment are remotely manageable, enterprises have the freedom to modify their network infrastructure from any location in the globe.

Constraints:

-Performance: Virtual networking equipment may have problems with performance, especially when a lot of bandwidth is needed. Network congestion and slower data transmission rates may follow from this.

-Network complexity: Virtual networking appliances can be more difficult to set up and administer than traditional networking gear, and they need enterprises to have a solid grasp of networking fundamentals.

-Dependence on the cloud provider: Companies that significantly rely on virtual networking equipment must have faith in their cloud provider to guarantee that they have access to the resources and assistance they need when they need it.

Virtual networking devices depend on internet access, which might cause latency or communication delays. Businesses that need real-time communication or high-performance networking may find this to be particularly difficult.

=>Multi-cloud management platform: Finally, while companies wishing to develop a multi-cloud environment may attempt using third-party network appliances in several CSPs, using a multi-cloud management platform is an additional alternative to streamline the management of different clouds from a configuration and policy viewpoint.

These multi-cloud administration tools are specifically designed to produce a software layer that covers any underlying configuration management discrepancies between private and public clouds. Despite being far more complicated than the other two, this method presents a compelling alternative for those looking to spread a sizable network across numerous public cloud providers.

Before choosing to utilize them, organizations should take into account the advantages and limitations that cloud multi-cloud management solutions provide. The following are a few of the more crucial ones:

Advantages:

-Centralized administration: Organizations may manage their cloud infrastructure from a single location with the help of multi-cloud management tools. Deploying, tracking, and managing resources across several clouds is made simpler as a result.

-Cost-effective: By locating unused resources and choosing the most affordable cloud provider, multi-cloud management tools help organizations to optimize their cloud utilization and lower expenses.

-Flexibility: Businesses may pick the best cloud provider for their individual needs using multi-cloud management solutions, allowing them to take advantage of the special features and capabilities of each cloud provider.

-Security: Organizations may implement security standards across all cloud providers using multi-cloud management tools. This makes sure companies are complying with regulations and reducing cybersecurity threats.

Constraints:

-Complexity: Setting up and managing multi-cloud management systems may be challenging, necessitating that enterprises have a solid grasp of networking and cloud architecture concepts.

-Multi-cloud management solutions are dependent on third-party software, which increases the risk of dependability and security. To reduce these risks, businesses must make sure they are utilizing reliable software vendors.

-Internet connectivity, on which multi-cloud management tools depend, might cause latency or communication delays. Businesses that need real-time communication or high-performance networking may find this to be particularly difficult.

-Vendor lock-in: Due to the potential for vendor lock-in, multi-cloud management systems, organizations may find it more challenging to transfer cloud providers in the future. This may reduce flexibility and raise overall expenses.

Three network standards that this company may implement are:

1-The Transmission Control Protocol/Internet Protocol (TCP/IP) is a family of widely used network protocols that serves as the backbone of the Internet and other private networks. TCP is in charge of making sure data is delivered reliably, whereas IP is in charge of addressing and routing. This business probably uses TCP/IP to provide device-to-device connectivity and data-to-data networking.

There are two primary protocols in TCP/IP:

-TCP: Transmission Control Protocol TCP offers data packet transmission that is dependable, well-organized, and error-checked. In addition to ensuring that data packets are received between two devices in the right sequence and without mistakes, it also creates a link between them. TCP is frequently used for applications like web surfing, email, file transfer, and remote access that need dependable data transport.

-Internet Protocol (IP): IP handles addressing and packet routing across networks. It offers logical addressing to identify devices on a network and specifies the IP address format. By handling packet forwarding, fragmentation, and reassembly, IP enables linked data transmission across devices.

By dividing data into packets, transporting them via networks, and reassembling them at the destination, TCP/IP facilitates communication between devices. It is widely utilized in several networked applications and serves as the foundation for internet communication.

2- DNS: The Domain Name System is a hierarchical naming structure that associates IP addresses with domain names, such as www.example.com or 203.0.113.0. The majority of networks utilize DNS, which is crucial for the Internet's operation and allows devices to discover and interact with one another using domain names rather than IP addresses.

These features are made available via DNS:

-Name Resolution: DNS converts domain names to IP addresses, enabling users to connect to networked services, visit websites, and send emails using simple names rather than obscure IP addresses.

-Hierarchical framework: Top-level domains (TLDs) such as.com,.org, and country-specific domains are used by DNS to arrange domain names in a hierarchical framework. This hierarchical structure allows for effective domain name administration and delegation.

-Caching and Redundancy: DNS uses caching techniques to save answers to requests, minimizing the need for additional lookups. Additionally, it makes use of an international dispersed network of DNS servers to ensure redundancy and fault tolerance.

DNS is essential to internet communication because it enables the conversion of domain names into IP addresses and lets users access online resources with names that are easy to remember.

3- UDP (User Datagram Protocol): This Internet Protocol (IP) suite network protocol works at the transport layer. It is a connectionless protocol, which implies that data is transmitted without first creating a special connection between the sender and recipient.

UDP is frequently employed in cloud networking for applications that place a higher priority on speed and low latency than on data delivery assurances.

Data is divided into individual packets known as datagrams and sent to the destination independently using UDP. It doesn't offer mechanisms for flow control, error correction, or packet retransmission. Since speed and responsiveness are so important in real-time applications, such as audio and video streaming, online gaming, and other applications, UDP is frequently utilized in these contexts.

On top of IP, UDP is a lightweight, connectionless transport protocol. UDP does not provide packet sequencing or reliable delivery like TCP does. Applications that value economy and speed above dependability frequently employ it. UDP has a few properties, such as:

-Connectionless: Before transferring data, UDP does not create a connection. Without checking to see if they were received or were sent in the right sequence, it only delivers datagrams, or packets of data, to the receiver.

-Unreliable: UDP lacks methods for error checking or retransmission. A lost or damaged UDP packet is not retransmitted, and the recipient is not made aware of the loss.

-Low Overhead: Because UDP lacks the mechanisms for dependable data delivery and sequencing, it has less overhead than TCP. Because of this, UDP is quicker and more suited for uses like real-time streaming, video conferencing, online gaming, and DNS lookups.

When speed and low latency are essential and some data loss or out-of-order packets can be accepted, UDP is preferred.

Q2.

Employees may more easily operate from any location at any time thanks to cloud communication, which offers remote access to apps and services. This is accomplished by using a distributed architecture, in which resources are housed in data centers and accessible online. Cloud communication relies on network elements that are virtualized, such as virtual computers or containers, which may be swiftly added or deleted to meet changing demands. Cloud providers provide security measures like encryption and firewalls to secure data in transit. Network communication between various virtualized components might occur through private or public IP addresses.

The company's usage of the cloud to distribute e-learning platforms and bespoke applications to outside customers is an example of cloud communication. As a result, the business can provide its consumers with highly scalable and accessible services without having to maintain physical equipment on-premises, and it can also add more security measures to safeguard critical user data. Another illustration is the use of a cloud-based video conferencing platform to hold online training sessions. Participants can join virtual classes and webinars using web browsers, and features like screen sharing, interactive whiteboards, and chat are used to promote efficient online learning.

Cloud computing technology is used to ease communication and information exchange between several parties. This is referred to as cloud communication. In this instance, the business is distributing e-learning platforms and custom apps to its external clients through the cloud. This indicates that the business makes use of cloud infrastructure supplied by a cloud service provider rather than hosting these services on actual servers situated on their premises.

The business benefits in a number of ways by delivering e-learning platforms and apps over the cloud. Scalability is a significant benefit. The organization can simply scale its resources up or down in response to demand thanks to the cloud. The business may instantly deploy extra cloud resources if there is an unexpected spike in the number of people accessing the e-learning platforms in order to handle the increased strain. Similar to this, resources might be reduced during times of low demand to maximize cost effectiveness.

Accessibility is another advantage. The business may provide clients with simple access to its e-learning platforms and apps from any location with an internet connection by employing the cloud. Users do not need to install and maintain specialist software on their own devices in order to use these services because they may access them using web browsers.

Cloud communication also enhances security. To safeguard the sensitive user data kept in the cloud, the business might put in place strong security measures. To guarantee the integrity and confidentiality of the stored data, cloud service providers often offer a variety of security features and technologies, including encryption, access restrictions, and frequent data backups.

The example also suggests using a cloud-based video conferencing tool for online training sessions in addition to e-learning platforms. This eliminates the requirement for installing particular video conferencing software and enables users to join online courses and seminars using web browsers. The cloud-based platform has tools like screen sharing, interactive whiteboards, and chat that improve online learning and encourage productive teamwork amongst users.

Q3.

There are several networking standards that enable cloud computing, but the following four prevalent ones and how they help businesses are listed:

- BGP is a typical internet routing system used in cloud networking, or border gateway protocol. It makes it possible for autonomous systems (AS) to communicate routing data and choose the best routes for data flow. In multi-cloud and hybrid cloud architectures, where various cloud providers and on-premises networks must connect and exchange routes, BGP is crucial.

BGP is an external gateway protocol that is used on the internet to exchange routing and reachability data between autonomous systems (AS). It provides routing decisions and communication between routers in various autonomous systems. Among the crucial facets of BGP are:

.BGP functions at the level of autonomous systems, where an autonomous system is a network or a group of networks that fall under a single administrative domain. BGP enables traffic optimization by allowing autonomous systems to share routing data.

.Path Vector Protocol: BGP exchanges routing information and makes routing choices using the path vector algorithm. To choose the best route for routing, it takes into account variables including network policies, path characteristics, and total path cost.

.Scalability and Policy Control: The internet's size and complexity are easily handled by BGP. It gives network managers fine-grained control over routing policies, enabling them to govern how traffic moves between autonomous systems in accordance with criteria like network performance, cost, and policy agreements.

Internet service providers (ISPs) and big networks frequently utilize BGP to create routing links and communicate routing information between independent systems.

-Data that is transferred over the internet is encrypted using the security protocols SSL/TLS. Because they offer a safe means for devices to connect with cloud servers and storage devices, SSL/TLS are crucial for cloud computing. This is crucial for preventing unwanted access to sensitive data, such as passwords and financial information.

A cryptographic protocol called SSL/TLS offers safe internet connection. It guarantees the privacy, authenticity, and integrity of data sent between a client and a server. SSL/TLS's salient characteristics include:

.Encryption: To safeguard the data in transit, SSL/TLS employs encryption methods. It encrypts the data transferred between the client and server so that anybody who intercepts the transmission cannot decipher it.

.Certificate-based Authentication: To verify the identity of the server, SSL/TLS uses digital certificates. To demonstrate its identity to the client, the server hands out a certificate that has been digitally signed by a reliable certificate authority (CA). By doing so, it is made sure that the client is speaking with the intended server and not a phony one.

. Secure Handshake: SSL/TLS establishes a secure connection between the client and server via a secure handshake procedure. Negotiating encryption protocols, transferring cryptographic keys, and confirming the server's identity are all part of the handshake.

Numerous internet protocols, including HTTPS (secure web surfing), FTPS (secure file transfer), SMTPS (secure email), and others, are protected by SSL/TLS.

-Open Shortest Path First (OSPF): OSPF is an inner gateway protocol (IGP) that is often used in business networks and may be utilized in some cloud networking configurations. Larger networks benefit from OSPF since it uses the network topology to compute the shortest path and assign fees to find the best route. In cloud networking, OSPF can be applied to a particular cloud area or to the network architecture of a single cloud provider.

An inside gateway routing protocol called OSPF is frequently used in autonomous systems to choose the most efficient routes for IP packet routing. It offers dynamic routing capabilities and is based on the link-state algorithm. Key characteristics of OSPF include:

.Link-State Routing: OSPF routers communicate link-state data, which contains information on the topology of the network, link prices, and available routes. In order for routers to determine the quickest way to destinations, this data is needed to create a thorough map of the network.

.Dynamic Routing Updates: OSPF routers only exchange updates when the network topology changes. This lowers network overhead and makes it possible for routing table upgrades to be done quickly.

.Scalability: In big networks, OSPF is made to scale well. Hierarchical routing is supported, which streamlines routing tables' complexity and boosts overall network performance by grouping routers into distinct zones.

Internet service providers (ISPs) and business networks frequently implement efficient routing within autonomous systems using OSPF.

-Interior Gateway Routing technology (IGRP): EIGRP has mostly supplanted IGRP, another Cisco-exclusive routing technology. Similar to RIP, IGRP is not widely utilized in cloud networking nowadays, however it could be used in certain Cisco-based cloud networking situations or older configurations.

The inner gateway routing protocol known as IGRP was created by Cisco Systems. The most effective routes for routing within an autonomous system were found using it. Even though IGRP is no longer frequently used, it can nonetheless provide light on how routing protocols have changed over time. The following are some of the essential characteristics of IGRP:

.Routers communicate routing updates providing details about network reachability and related costs using the distance vector routing protocol known as IGRP. Based on the vector metric, which takes into account elements like bandwidth, latency, dependability, and load, routers choose the optimum way.

.Loop-Free Routing: IGRP has features like split horizon and route poisoning to stop routing loops. These methods make sure that packets effectively reach their destination and do not repeatedly loop between routers.

.Limited Scalability: When compared to more recent routing technologies, IGRP is not as scalable. It is not appropriate for large-scale installations and only supports smaller networks.

Advanced routing protocols like OSPF and EIGRP (Enhanced Interior Gateway Routing Protocol), which provide better scalability and functionality, have mostly supplanted IGRP.

Q4

Comparing cloud networks to traditional networks, there are various benefits:

-First of all, cloud networks give organizations a highly adaptable and scalable architecture that enables them to swiftly add or remove resources as needed. Utilizing virtualized resources, such as virtual machines and containers, which are simple to copy, duplicate, and delete, allows for this scalability.

- Additionally, cloud networks provide higher availability and accessibility. Employees may work remotely or interact with coworkers in different places more easily thanks to cloud networks, which make resources accessible from anyplace with an internet connection. Due to the use of load balancing and redundancy measures, cloud networks often offer higher uptime and availability than traditional networks.

- Third, compared to conventional networks, cloud networks frequently provide more security. To secure the data of their clients, cloud providers frequently put in place strong security measures including encryption, firewalls, and intrusion detection systems. Due to the usage of backup and replication strategies, cloud networks can also offer enhanced disaster recovery and business continuity capabilities.

Cloud networks do, however, have significant disadvantages that must be taken into account. The possibility of data breaches and cyberattacks is one possible drawback of cloud networks. Data transmission and storage on the internet might leave it open to theft and interception. Furthermore, compared to traditional networks, cloud networks can be more complicated and challenging to administer, necessitating specific expertise and abilities.

Summary: Scalability, accessibility, availability, and security are just a few benefits that cloud networks have over traditional networks. They do, however, carry some hazards and complexity that must be properly controlled.

Q5.

On cloud infrastructure, remote operating systems can be installed via virtual machines (VMs) or containers. The procedure usually entails installing the operating system on the cloud server as a virtual instance.

A virtual machine that replicates the hardware and software environment of a real system is created using a hypervisor in the case of a VM. Following the installation of the operating system, the VM may be used to access the cloud infrastructure remotely. For more complicated operating systems that consume a lot of resources, VMs are frequently employed.

Contrarily, containers offer a compact replacement for virtual machines. Although they separate them from other programs running on the same system, they execute apps on the host operating system. since of this, containers are more effective than virtual machines (VMs) since they may run on a single host.

In both situations, the operating system may be accessed remotely using a number of tools, such as remote desktop protocol (RDP) or secure shell (SSH), once it has been installed on the cloud infrastructure. As with a physical machine, this enables users to access and manage the operating system remotely.

-Remote Desktop Protocol (RDP): RDP is a Microsoft-developed proprietary protocol that enables users to connect to and operate a Windows-based computer or server from a distance. With RDP, a user may create a remote session and view the distant machine's graphical user interface (GUI). This entails that the user may operate software, manage files, and interact with the remote desktop environment just as if they were physically in front of the computer. RDP makes it simple to complete activities that call for a GUI interface by offering a fluid and interactive remote access experience.

-SSH: SSH is a network protocol that enables secure remote access to a server or machine. Both Windows and Unix-like operating systems are supported, and it is frequently used in cloud contexts. When connecting to a remote system using SSH, a user can access its command-line interface (CLI) and create a safe, encrypted connection. The user may run commands, manage files, set up settings, and carry out administrative actions on the remote system through the SSH connection. SSH is a well-liked option for secure remote access because of its excellent security features, such as encryption, authentication, and data integrity.

Although both RDP and SSH offer remote access capabilities, they are different in the kind of access they grant. Users may interact with the remote workstation as if they were physically present thanks to RDP, which focuses on offering a remote graphical desktop experience. While SSH offers a text-based interface for managing and controlling the remote system, it places an emphasis on secure command-line access.

----------

Depending on the service and device being utilized, remote clients and consumers can access cloud services in a variety of ways.

Here are some instances of cloud services and how they are deployed:

-SaaS (software as a service):

Service illustration: Salesforce CRM deployment With SaaS, the software program is centrally hosted in the cloud and distributed to consumers through the internet. Users don't need to install or maintain the software on their own devices in order to use the program through a web browser.

-IaaS (Infrastructure as a Service):

Typical service Deployment of Amazon Web Services (AWS): IaaS offers virtualized computer resources including networking, storage, and virtual machines. Using management consoles or APIs, users may remotely access and manage these resources. They are in charge of the operating system, programs, and configurations, while the cloud service provider is in charge of the supporting infrastructure.

-PaaS, or platform as a service:

A platform for the development, deployment, and management of apps is offered by PaaS services, such as Heroku Deployment. Without worrying about the underlying infrastructure, developers may build, test, and deploy their apps on the platform via remote access. Scalability, security, and infrastructure management are handled by PaaS providers.

-DAS (Desktop as a Service):

As an illustration, consider VMware Horizon Cloud Deployment. Users that utilize DaaS can access cloud-hosted virtual desktops from a distance. Using remote display protocols, users may access their virtual desktop environment from a variety of devices, such as laptops, tablets, or thin clients. The virtual desktop infrastructure, including the hardware, operating system, and apps, is managed by the cloud provider.

-Storage as a service:

Typical service Users are able to store and retrieve their files and data in the cloud thanks to Dropbox Deployment: Storage as a Service. Using client programs or online interfaces, users may remotely upload, download, and exchange data. The storage infrastructure, including redundancy, data replication, and availability, is managed by the cloud provider.

-DBaaS, or database as a service:

Service illustration: Amazon RDS deployment Managed database services are provided by DBaaS in the cloud. Users don't have to bother about infrastructure setup and administration because they can create, configure, and access databases remotely. The cloud service provider is in charge of duties including software patching, scaling, and backups.

Web-based interfaces, APIs, and mobile apps are a few examples of prevalent techniques. Any device with an internet connection may use web-based interfaces, which enables remote clients to manage data, modify settings, and keep tabs on system performance. APIs make it possible to construct specialized apps that make use of the features of cloud services or to integrate them specifically with other software systems. The functionalities of the service are accessible through mobile applications, which also offer push alerts and offline access.

Utilizing distant clients and consumers to access cloud services has several advantages, including flexibility, cost-effectiveness, and increased security. It is not necessary to install costly hardware and software on each client device thanks to remote clients, which let customers access cloud services from any location with an internet connection. Customers that utilize cloud services have the flexibility to rapidly and easily expand or reduce the amount of resources they use in accordance with their demands, without making a sizable upfront expenditure or committing to a lengthy period of time. As a result, less expensive hardware and infrastructure may be required and productivity may rise.

Furthermore, cloud service providers are accountable for maintaining and updating their services to ensure that customers always have access to the most recent features and security improvements. As a result, remote clients and customers can access the most recent technology and updates without the need for ongoing hardware upgrades.

Q6.

An operating system (OS) can be optimized in a number of ways to enhance functionality, effectiveness, and user experience. Here are a few instances:

-Memory and Process Management:

putting into practice excellent resource allocation and prioritization algorithms for processes.

increasing the use of virtual memory and other memory management techniques to better use RAM and reduce disk usage.

-Optimization of the file system:

using caching techniques to enhance file read/write operations and decrease disk I/O.

enhancing metadata management and file system architecture for quicker file access and search activities.

To maintain file system consistency and reduce data loss in the event of unplanned system failures, enable journaling or other mechanisms.

-Performance I/O:

I/O scheduling techniques can be used to streamline network and disk access, lowering latency and increasing throughput.

I/O operations can be parallelized and optimized by using methods like asynchronous I/O.

Buffering and caching techniques can be used to decrease disk access and enhance overall I/O performance.

-Power Control:

To minimize energy consumption and lengthen the battery life of mobile devices, power-saving technologies such CPU frequency scaling, sleep states, and idle task management are implemented.

adjusting power management settings depending on user preferences and system use trends.

-Improved security measures:

protecting user data and system integrity by putting security measures like access limits, authentication, and encryption in place.

deploying security updates and patches on a regular basis to fix vulnerabilities and maintain a safe OS environment.

-Optimization of the kernel:

adjusting kernel settings and parameters to improve system performance, stability, and resource use.

enhancing the kernel's efficiency by compiling it with unique hardware-specific optimizations.

-Optimization of the network stack:

enhancing socket management, network protocols, and buffers for effective network communication.

enabling methods like TCP/IP tweaking to raise throughput, cut latency, and improve network performance.

The performance of an operating system can be significantly impacted by remote operating system optimization. Here are some of the most common methods:

-Reduced Downtime: By enhancing system dependability and stability, remote operating system optimization may also assist decrease downtime. Advanced monitoring and management technologies, together with preventative upkeep and upgrades, can help with this.

-Improved Security: By adopting cutting-edge security protocols and procedures like encryption, firewalls, and intrusion detection systems, remote operating system optimization may also improve security. This can aid in defending against online dangers and data breaches.

-Improved Resource Utilization: Remote systems can make greater use of available resources by optimizing the operating system in the cloud. This might involve maximizing the use of RAM, the CPU, and disk I/O, which can lead to quicker reaction times and lower latency.

-Enhanced Scalability: Operating systems that run in the cloud may be scaled up or down fast and simply to accommodate changing workloads. This can ensure that even during times of high usage, distant clients and customers have constant service.

- Cost Savings: Remote operating system optimization in the cloud can potentially result in cost savings. Organizations may increase efficiency and lessen the need for expensive hardware updates and maintenance by optimizing resource use, expanding scalability, and decreasing downtime.

Overall, remote operating system optimization in the cloud may significantly boost performance by maximizing resource use, boosting scalability, minimizing downtime, strengthening security, and cutting expenses.

References:

My reliance was on the material and chapters that we took in the lectures, and I searched the following sites as well:

<https://study.com/academy/lesson/organizations-that-create-networking-standards.html>

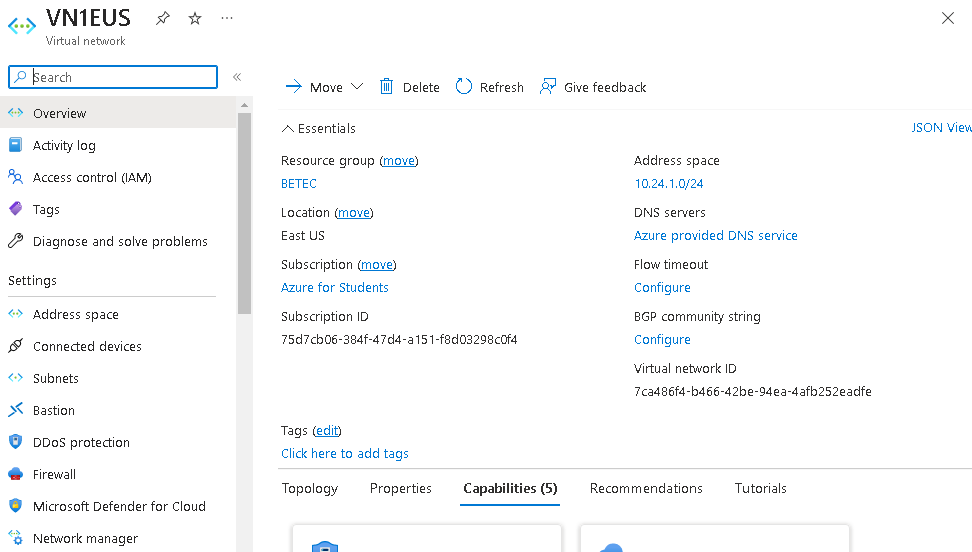
<https://www.techtarget.com/searchnetworking/tip/An-introduction-to-cloud-network-architecture>

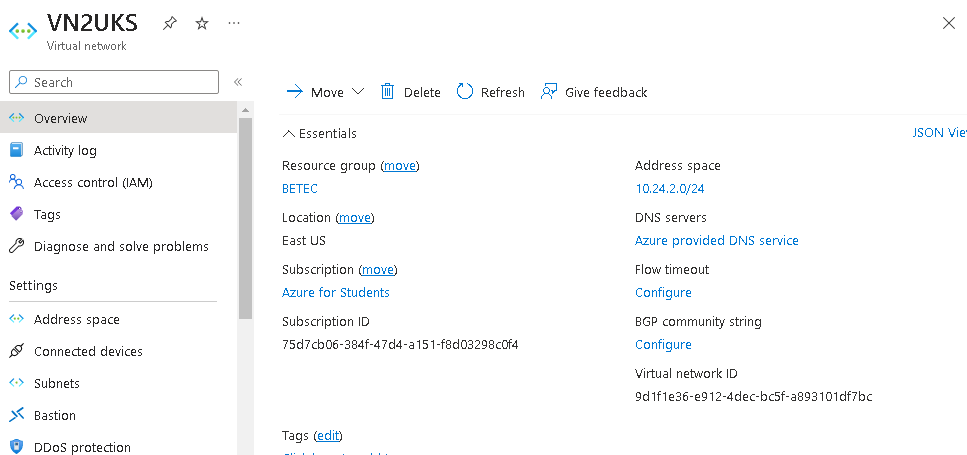
<https://link.springer.com/chapter/10.1007/978-981-19-3026-3_4>

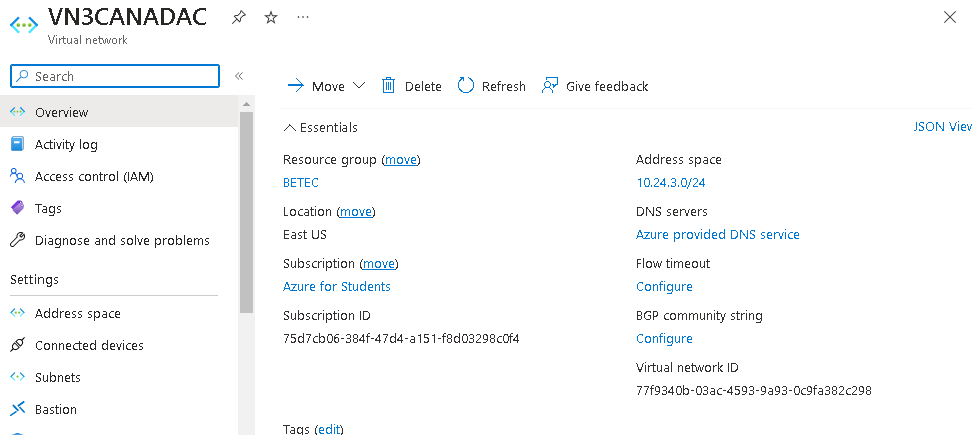
<https://www.zuj.edu.jo/wp-content/uploads/IT_Research/IT_20.pdf>

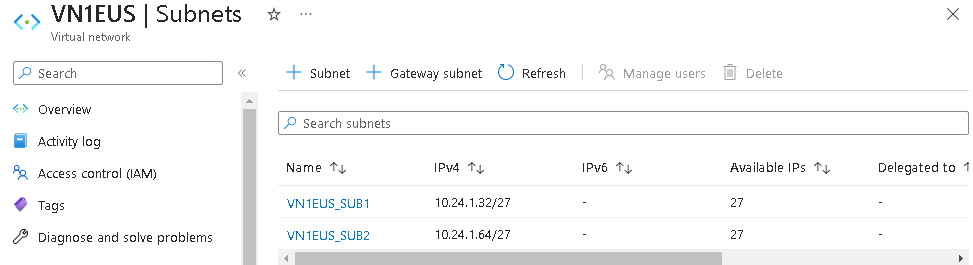
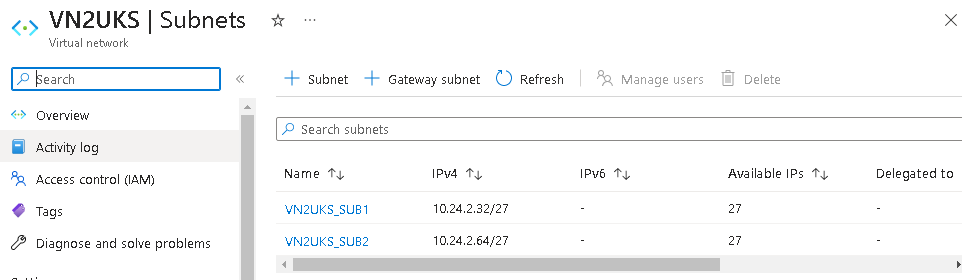
<https://www.tokioschool.com/en/news/operating-system-cloud-computing/>

TASK B:

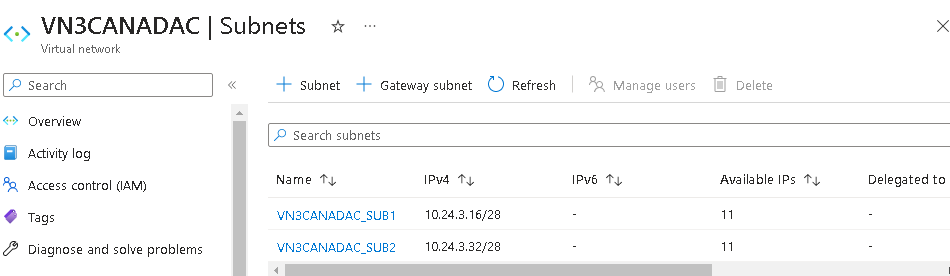
7.A-



****

**7.**B**-**

7.C-

****

7.D-

VNET1 (EAST US): 10.24.1.0/24

SUB1 (EAST US): 10.24.1.32/27

SUB2 (EAST US): 10.24.1.64/27

WASTED IPs: 32-(5+20) = 7.

VNET2 (UK SOUTH): 10.24.2.0/24

SUB1 (UK SOUTH): 10.24.2.32/27

SUB2 (UK SOUTH): 10.24.2.64/27

WASTED IPs: 32-(5+20) = 7.

VNET3 (CANADA CENRAL): 10.24.3.0/24

SUB1 (CANADA CENRAL): 10.24.3.16/28

SUB2 (CANADA CENRAL): 10.24.3.32/28

WASTED IPs: 16-(5+10) = 1.

\*AZURE TAKES 5 ADDRESSES FOR SPECIAL USES.

7.E-

The two distinct IP (Internet Protocol) address types used in computer networking to identify devices on a network are public IP and private IP. Here's a quick explanation of the differences between public IP and private IP:

Public IP:

A public IP address is accessible through the internet and is one of a kind in the whole world.

It is given to a device by a network administrator or Internet service provider (ISP).

To connect with devices on other networks, such the internet, public IP addresses are utilized.

Anywhere on the internet may immediately access devices with public IP addresses.

There is a finite supply of public IP addresses, and they are routable everywhere.

Private IP:

The internet cannot directly reach a private IP address since it is only used in private networks.

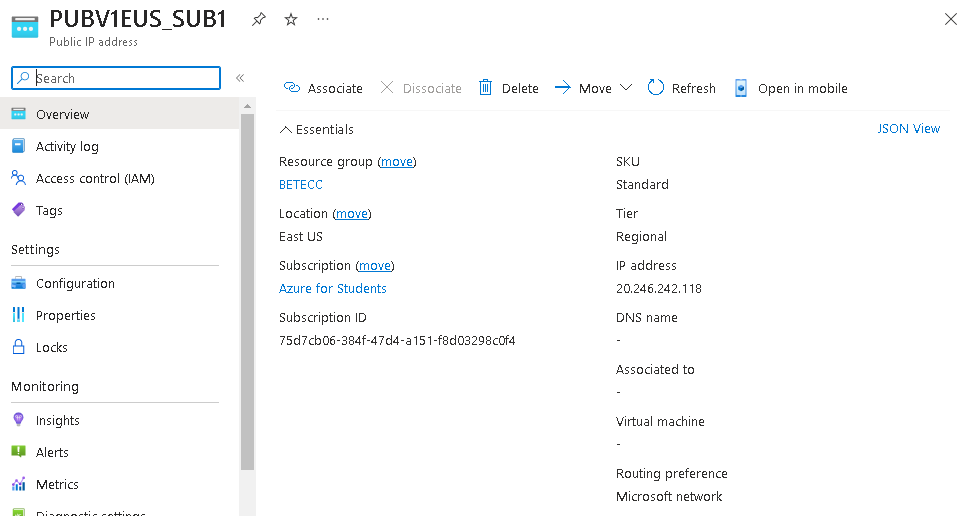
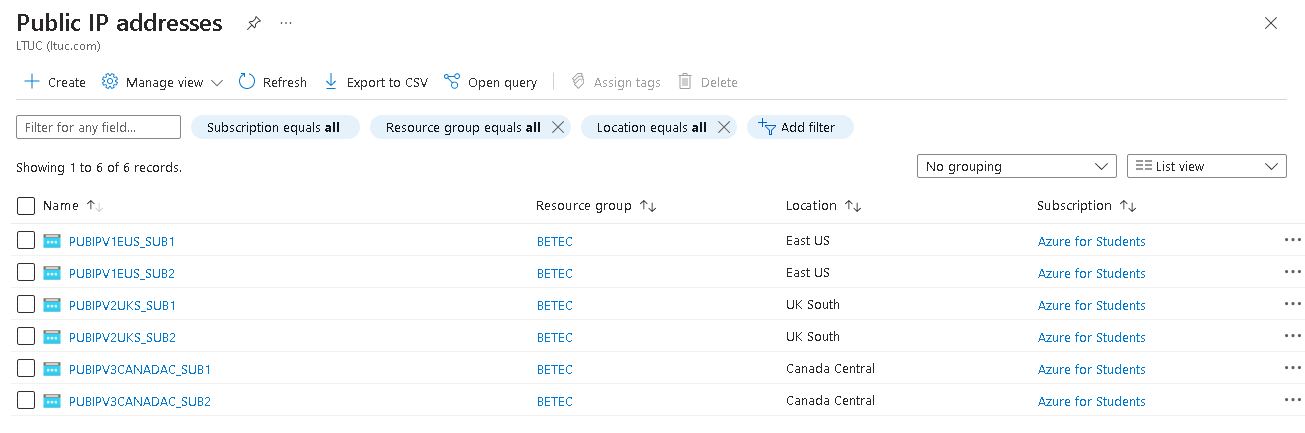
Using network address translation (NAT), a local network router assigns it to a device.

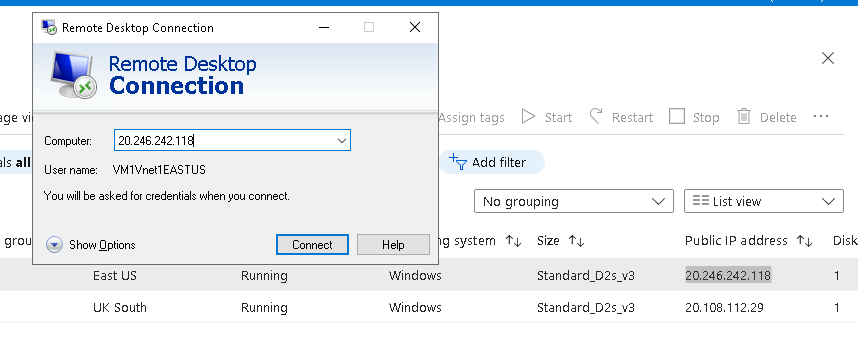
For internal communication within a local network, such as a network in a house or workplace, private IP addresses are utilized.

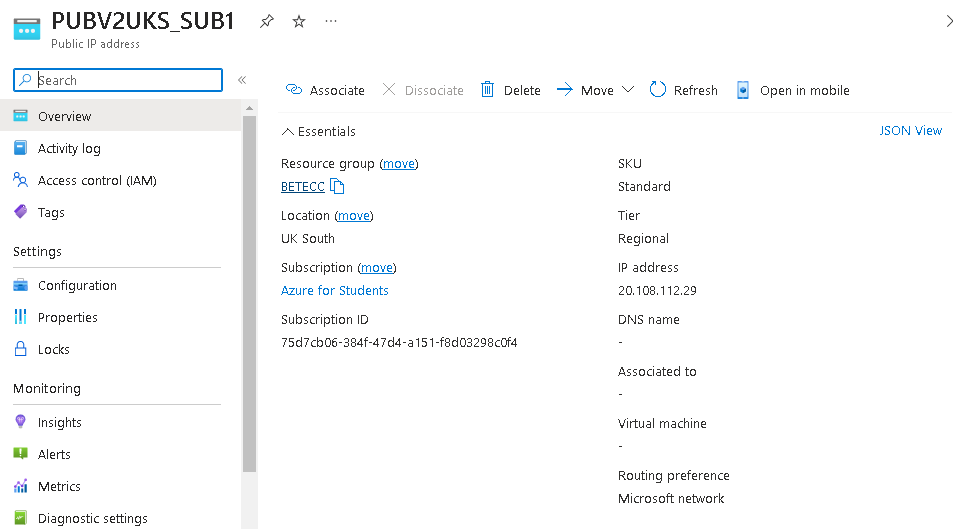
Without employing methods like port forwarding or VPN, devices with private IP addresses cannot be accessed from the internet directly.

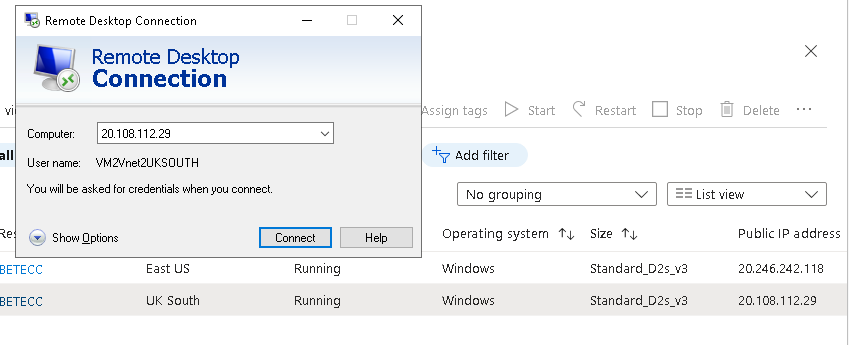
Private IP addresses can be reused in many private networks since they are not universally unique.

In conclusion, a public IP address is distinct and reachable from anywhere in the world, enabling devices to connect to external networks like the internet. A private IP address, on the other hand, is used for internal communication within a private network and is inaccessible from the internet.

8-







\*A system's speed and scalability can be impacted by the public IP address in a number of ways:

-Data routing and network performance: Data is routed across networks, including the internet, using the public IP address. Network performance may be impacted by routing's effectiveness and quality. Systems' ability to communicate with one another may suffer from delays or packet loss if the routing infrastructure is not optimal or faces congestion.

-Network Address Translation (NAT): In many cases, local networks utilize private IP addresses, but the router or gateway of the network is given a public IP address.

To translate between private and public IP addresses, NAT is used. Network traffic is burdened by the process of translating IP addresses, which can have an adverse effect on performance, especially when dealing with heavy loads or big volumes of data.

-System scalability and the availability of public IP addresses: Since public IP addresses are a scarce resource, it is important to ensure that there are enough of them available. Getting enough public IP addresses might be difficult when a company needs several of its devices or services to be available to the public. This restriction may make it difficult to grow the system, necessitating the use of workarounds like network address translation or the deployment of load balancers to split traffic across several private IP addresses.

It is essential to implement effective routing infrastructure, monitor network performance, use appropriate security precautions, and take into account strategies like load balancing and caching to distribute and handle traffic in order to maximize performance and scalability in systems using public IP addresses.

In Azure, the decision between Basic and Standard Public IPs relies on the capabilities you desire and your individual needs. Let's contrast the two possibilities:

\*Basic Public IP Address:

-Basic Public IPs often cost less than Standard Public IPs in terms of price.

-IPv4 Only: Only IPv4 addresses are supported by Basic Public IPs.

-Availability: basic SLA (Service Level Agreement) uptime guarantees are offered by Basic Public IPs, which implies they offer basic availability.

-services: Basic Public IPs include fundamental services including port forwarding, load balancing, and inbound and outbound network address translation (NAT).

\*Standard Public IP:

-Price: Generally speaking, Standard Public IPs are more expensive than Basic Public IPs.

-IPv6 Support: IPv4 and IPv6 addresses are supported by Standard Public IPs. Especially if you need IPv6 connectivity, this might be useful.

-Availability Zones: Resources in Azure Availability Zones can be paired with Standard Public IPs to increase availability and redundancy.

-DDoS Protection: To assist defend your resources from DDoS assaults, Standard Public IPs come with integrated DDoS (Distributed Denial of Service) protection.

-SLA: Standard Public IPs promise greater availability and uptime than Basic Public IPs since they have a higher SLA.

So I used standard IP addresses.

9.A- I decided to enhance with DNS.

For a number of reasons, DNS (Domain Name System) is utilized in cloud networking to improve cloud outcomes.

-Name Resolution: DNS offers a method for converting domain names that can be read by humans into IP addresses. Instead of needing to memorize and utilize the underlying IP addresses, cloud networking enables users and programs to access cloud resources using simple-to-remember domain names. This makes using cloud services easier and makes them more usable.

-DNS may be used to load balance across several cloud services or instances. Traffic can be divided across many servers or locations by establishing DNS with numerous IP addresses linked to a domain name. By ensuring that the traffic is evenly distributed over the available resources, this helps to share the workload and increases performance.

-High Availability and Failover: Multiple IP addresses for the same domain name, signifying redundant or backup resources, can be set in DNS. DNS can automatically transfer traffic to an alternate IP address if one server or area goes down. In the case of failures or outage, cloud services are still available because to high availability and failover made possible by this.

-Traffic Management and Routing: DNS may be utilized in cloud networking for sophisticated traffic management and routing. Traffic may be routed depending on elements like geographic location, network circumstances, or special regulations by setting DNS with various entries and rules. By directing users to the closest or quickest cloud resource depending on their location or other factors, this enables enterprises to maximize performance.

-Scalability and Flexibility: In cloud networking, DNS offers scalability and flexibility. DNS can be readily modified to reflect new resources or configurations as the cloud architecture grows or changes. By enabling the addition of additional resources to the network and their association with domain names, which guarantees smooth access and availability, DNS allows speedy and effective growth.

In conclusion, DNS improves cloud outcomes in cloud networking by streamlining resource access via name resolution, enabling load balancing and high availability, easing traffic management and routing, and offering scalability and flexibility. By maximizing resource usage and guaranteeing easy access to cloud services, it enhances performance, availability, and user experience in cloud settings.

In cloud networking, DNS (Domain Name System) can have a substantial influence on both performance and scalability:

Performance:

-Reduced Latency: By offering a quick and effective way to translate domain names into IP addresses, DNS lowers latency. When a user uses a domain name to make a request for a cloud resource, DNS rapidly converts that name to the matching IP address, enabling the client to make a connection. This shortens the distance customers must travel to get to the resources they want, improving performance and hastening response times.

- Using load balancing, numerous servers or instances are used to disperse incoming traffic. Requests from customers are distributed across various resources by setting DNS with several IP addresses linked to a domain name. By spreading out the load over many servers, load balancing helps to maximize resource use. The performance is improved by minimizing bottlenecks and guaranteeing effective handling of incoming requests when the load is equally distributed across several servers.

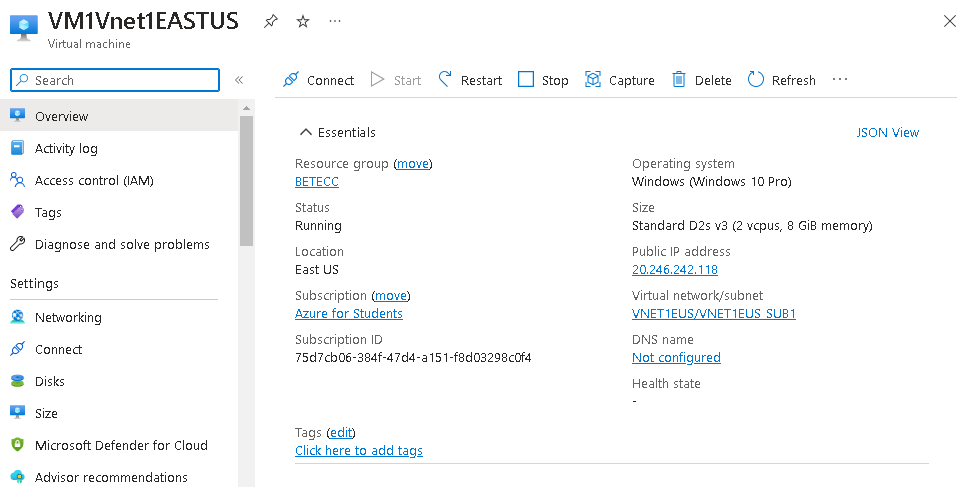
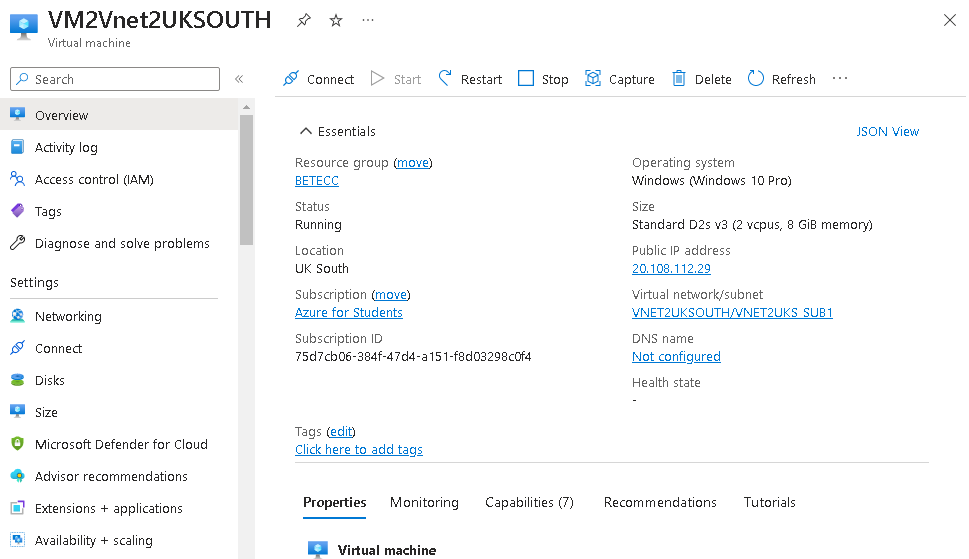
Scalability:

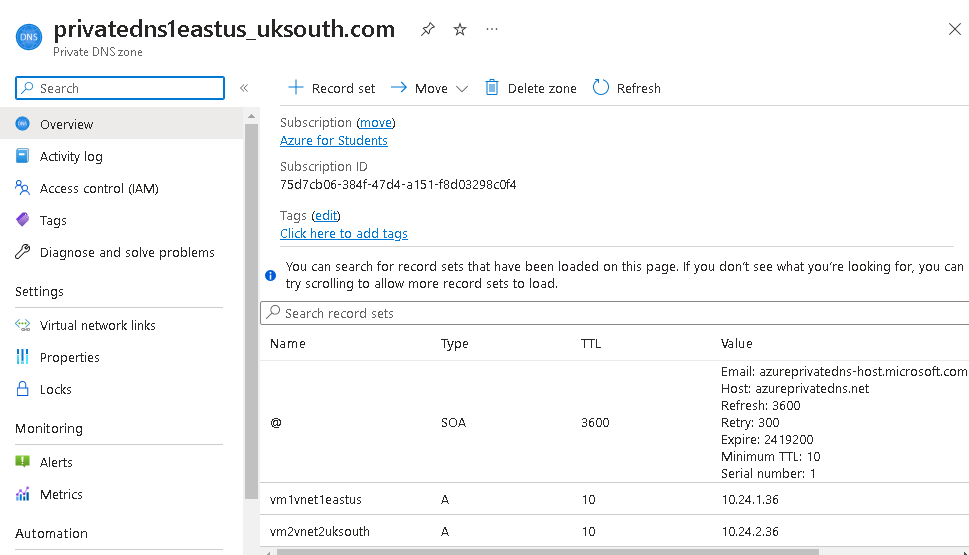
-Elastic Scaling: By enabling the dynamic addition or removal of resources, DNS is essential to elastic scaling. Additional resources can be provided and linked to DNS records as the demand for cloud services rises. This makes it possible for the system to scale up seamlessly to accommodate more traffic while maintaining performance standards. Scalability without service interruption is made possible through DNS, which makes it easier for traffic to be automatically distributed to newly additional resources.

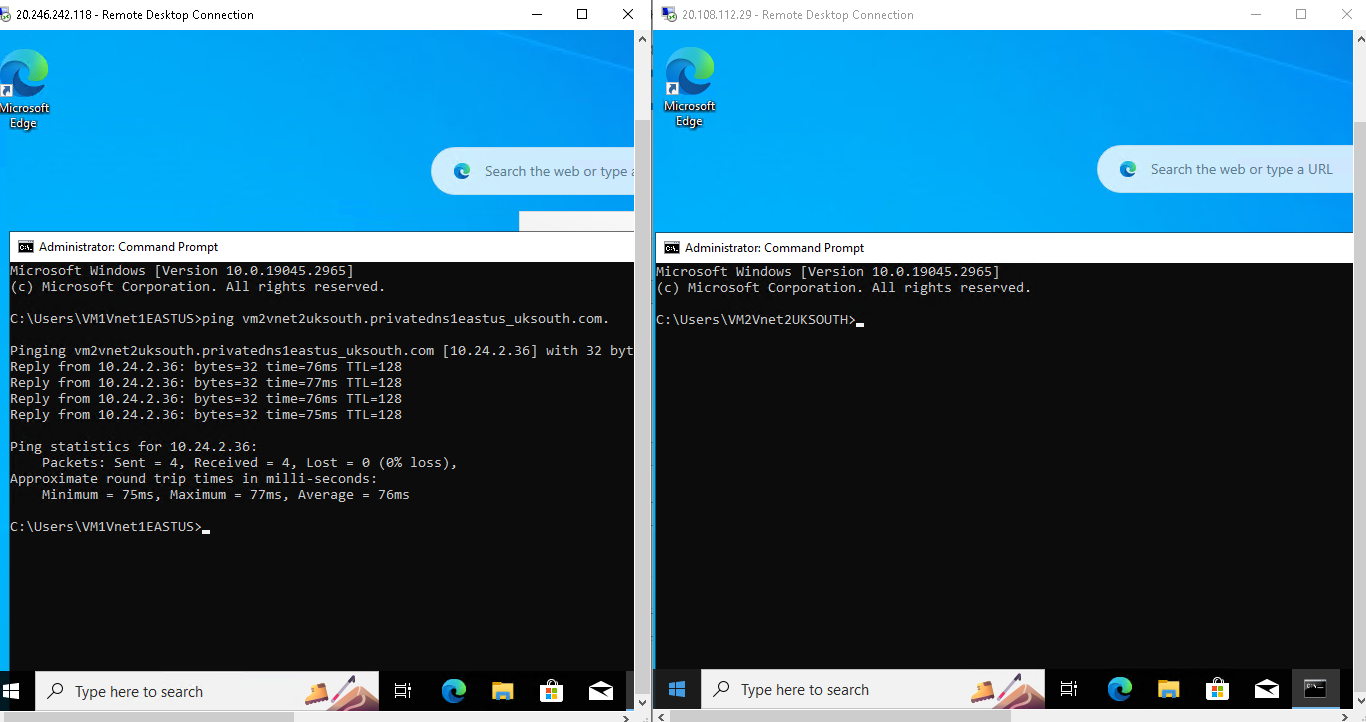
- High availability and fault tolerance are two further features that DNS enables. DNS may send traffic to backup resources in the event of problems or downtime by establishing DNS with several IP addresses for the same domain name, each pointing to separate servers or regions. DNS can automatically route traffic to the next available IP address in the event that one server or region goes down, maintaining service availability and scalability.

-Geographic Load Distribution: Depending on the user's location, DNS can distribute traffic regionally by routing them to the closest accessible server or area. By lowering network latency and streamlining data transmission times, this enhances performance. Cloud systems can efficiently manage global traffic and extend horizontally across several areas by utilizing DNS to point users to the nearest resources.

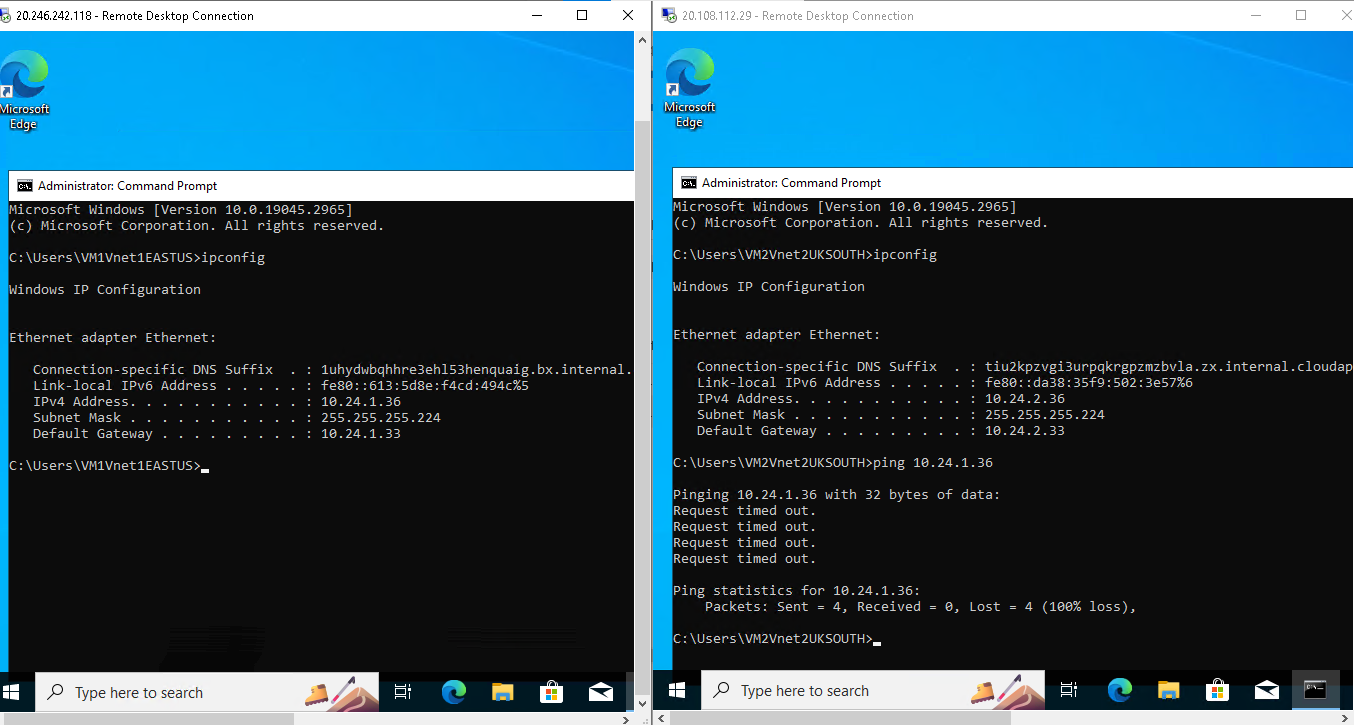
9.B-



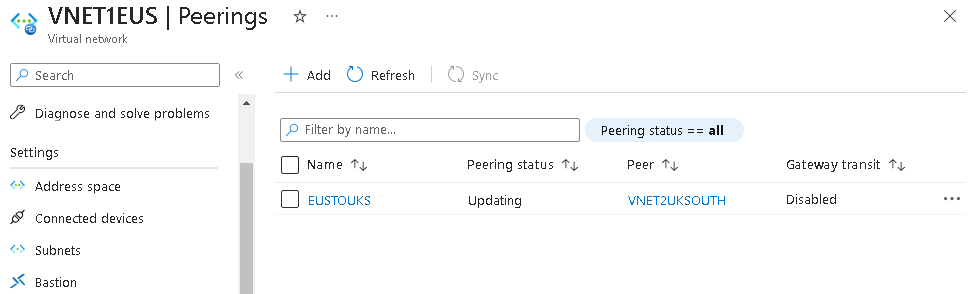




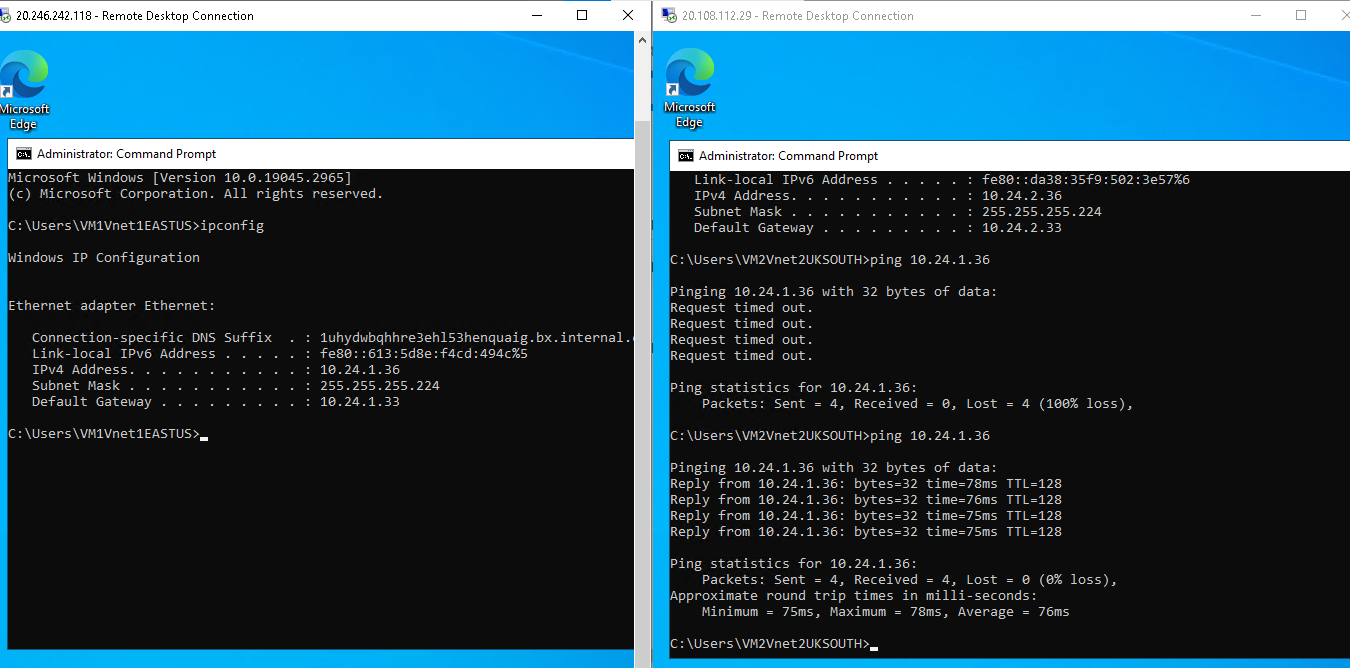
10-

BEFORE PEERING:

PEERING:



AFTER PEERING:



11.

The corporation will use three Virtual Networks (Vnets) installed in various regions—East US, UK South, and Canada Central—in the suggested cloud-based network solution. To meet the company's network needs, each Vnet will have unique subnets and IP addressing schemes. Scalability, security, and performance optimization are the main design considerations.

Virtual Networks (Vnets):

a) The company's activities in the eastern part of the United States will be served by the East US Vnet.

b) UK South Vnet: This Vnet will support the business' activities in the United Kingdom's south.

c) The Canada Central Vnet: This Vnet will assist the business' operations in Canada's central provinces.

Subnets:

a) East US and UK South:

Each Vnet will have two subnets, ensuring segregation and improved security.

Each subnet will accommodate 20 users.

Subnets will be named based on their purpose or department within the organization.

IP addresses will be assigned to each subnet to facilitate network communication.

b) Canada Central:

Each Vnet will have two subnets to maintain segregation and enhance security.

Each subnet will accommodate 10 users.

Subnets will be named according to their specific usage or department.

IP addresses will be assigned to each subnet for effective network communication.

Subnet IP Addresses and Waste IP Calculation:

The design will include the allocation of IP addresses for each subnet, ensuring efficient utilization and minimizing IP waste. The IP addresses will be calculated based on the required number of users in each subnet and the desired IP address scheme (IPv4).

Separation of Public and Private IP Addresses: The design will make a clear distinction between public and private IP addresses. Resources that must be accessed over the internet, such as externally facing servers or services, will be given public IP addresses. For internal communication within the cloud network, private IP addresses will be utilized, guaranteeing privacy and security.

Public IP Address: To communicate with users or networks outside the company, a public IP address will be generated. The unique needs of the organization will be used to justify the kind of public IP address (Standard or Basic). The range and subnet mask of the IP address will be used to define its class. We'll assess how the public IP address affects performance and scalability while taking things like latency, bandwidth, and availability into account.

Enhancement with Virtual Machines (VMs): The design will incorporate the development of virtual machines in the East US and UK South Vnets to improve cloud outcomes. Scalable and adaptable computational resources are offered by virtual machines for the use of applications and services. The business can assure availability, disperse burden, and boost performance by deploying VMs in several areas.

Peering will be used to provide communication between the VMs deployed in various Vnets. Peering and its Impact on Performance and Scalability. Peering improves network speed, lowers latency, and expands scalability by enabling private, direct connection across virtual networks. It will be examined how peering affects performance and scalability, taking into account things like data transfer rates, network latency, and overall network effectiveness.

Evaluation of Performance, Scalability, and Effectiveness

The infrastructure of the organization is improved in terms of security, performance, and resilience by the suggested cloud-based network design. The following elements can be used to assess how effective the design is:

Data privacy and network security are ensured by the division of subnets and the usage of private IP addresses. The architecture improves the overall security posture of the network by utilizing the security controls offered by the cloud provider, such as firewalls and access restrictions.

Scalability: Using virtual networks and subnets allows for a scalable design that can support the company's expanding user base and future development plans. Scalability without major interruptions is guaranteed by the cloud environment's simple addition and removal of resources.

Performance: The design includes methods for load balancing, caching, and speeding of data transfers, as well as approaches for network optimization. These actions boost user experience overall, enhance network performance, and decrease latency.

Performance Assessment:

Prior to the improvement, the company's network may have had performance concerns because to hardware limits, restricted scaling possibilities, and maybe problematic latency. However, the following performance enhancements can be anticipated following the implementation of the suggested cloud-based network design:

Scalability: As the company's user base and resource demands grow, smooth scaling is made possible by the cloud's capacity to dynamically provide resources. The business may expand resources as needed thanks to the cloud-based network design, assuring excellent performance even during moments of high consumption.

Network Performance: The use of load balancing, caching, and data acceleration techniques will greatly enhance network performance.

The user experience is improved through decreased latency, effective data transfers, and resource allocation that is optimized.

Availability and Resilience: In the cloud environment, availability and resilience are improved by the deployment of redundant infrastructure and fault-tolerant techniques. The utilization of numerous data centers and availability zones can be used to alleviate failures or disturbances in one area or subnet, maintaining uninterrupted network functioning.

Overall, the company's infrastructure is more secure, scalable, and effective thanks to the suggested cloud-based network design. The business may boost user experience, increase operational efficiency, and support future development and expansion by utilizing cloud technology and best practices.

THE MAIN REFERENCE IS OUR CHAPTERS.

OTHER REFERENCES:

<https://www.scaler.com/topics/computer-network/public-and-private-ip-address/>

<https://phoenixnap.com/kb/public-vs-private-ip-address>

<https://www.globaldots.com/resources/blog/the-advantages-of-using-cloud-based-dns-in-modern-business/>

<https://learn.microsoft.com/en-gb/azure/?product=popular>

<https://serverfault.com/questions/1090042/what-is-the-difference-between-basic-and-standard-public-ips-in-azure>

<https://www.cloudflare.com/en-gb/learning/dns/what-is-dns/>

**Plagiarism**

Plagiarism is a particular form of cheating. Plagiarism must be avoided at all costs and students who break the rules, however innocently, may be penalised. It is your responsibility to ensure that you understand correct referencing practices. As a university level student, you are expected to use appropriate references throughout and keep carefully detailed notes of all your sources of materials for material you have used in your work, including any material downloaded from the Internet. Please consult the relevant unit lecturer or your course tutor if you need any further advice.

**Student Declaration**

|  |
| --- |
| **Student declaration**  I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice.  Student signature:Shahed Montaser Date:13/5/2023 |