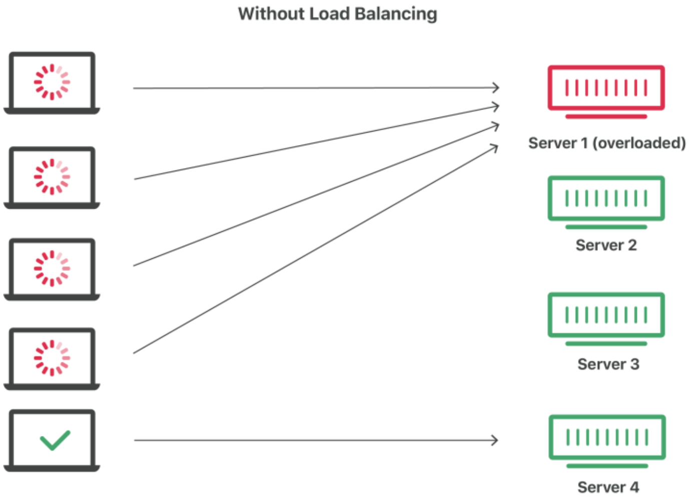
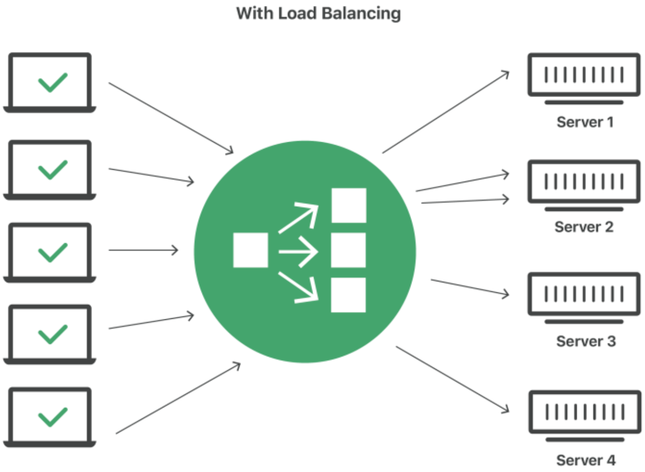
Interview questions

Networking:

1.What is Load balancer?

Load balancing is the practice of distributing computational workloads between two or more computers. On the Internet, load balancing is often employed to divide network traffic among several servers. This reduces the strain on each server and makes the servers more efficient, speeding up performance and reducing latency. Load balancing is essential for most Internet applications to function properly.



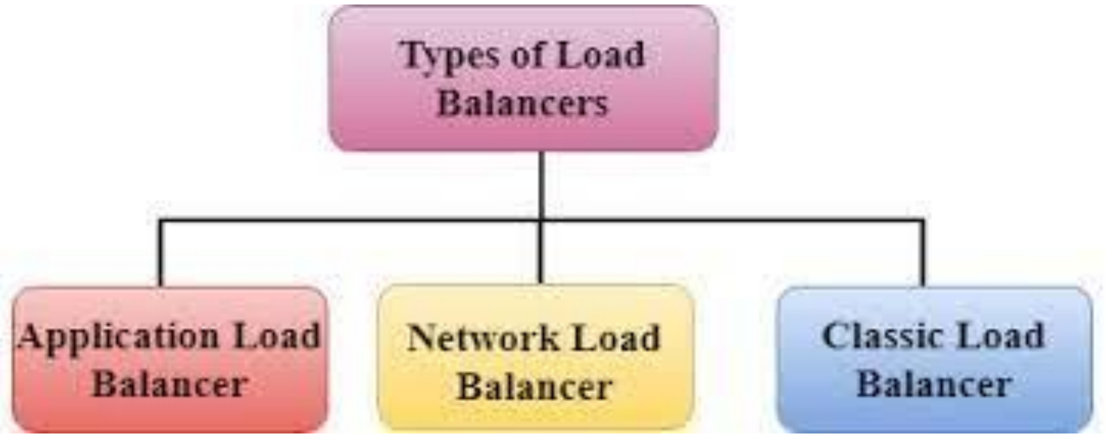


2. Types of Load balancer?

1.Application Load Balancer: The Application Load Balancer is a feature of Elastic Load Balancing that allows a developer to configure and route incoming end-user traffic to applications based in the AWS public cloud. In a cloud environment with multiple web services, load balancing is essential.

2.Network Load Balancer: The Network Load Balancing (NLB)feature distributes traffic across several servers by using the TCP/IP networking protocol. By combining two or more computers that are running applications into a single virtual cluster, NLB provides reliability and performance for web servers and other mission-critical servers.

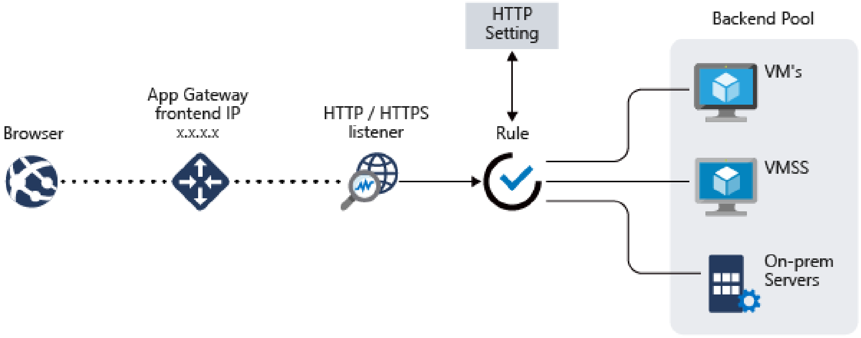
3.Classic Load Balancer: Classic Load Balancer provides basic load balancing across multiple Amazon EC2 instances and operates at both the request level and connection level. Classic Load Balancer is intended for applications that are built within the EC2-Classic network.



3.what is application gateway?

An application gateway is a program that serves as a firewall proxy. It runs between computers in a network to tighten security. It is responsible for filtering incoming traffic that contains network application data.

It provides an additional layer of protection against unwanted network traffic. It is also sometimes known as an “application-level gateway” or “application proxy.”



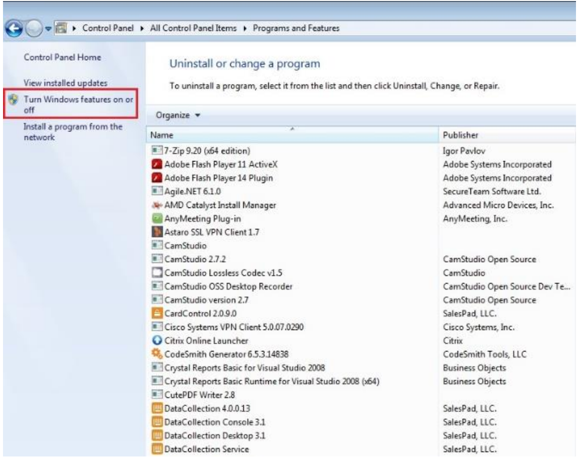
4.Difference between Load balancer and Gateways?

ALB	APL Gateway
1.No rate limiting, bursting capability	1. Can implement rate limiting, brusting for apl
2.Integrate with AWS WAF for protection	2. Integrate with AWS WAF for protection
3.possible to get a static IP address for Load balancer endpoint	3. Not possible to get a static IP address for GW endpoint
4. Accepts HTTP, HTTPS traffic	4. Accepts HTTPS traffic
5.Timeout limit 30 seconds	5. Timeout limit 4000 seconds
6.Integrates with almost all AWS services	6. Use EC2, Lambda, Ip address as backend
7. No health check available	7. Health check is available

5.How do you configure IIS Webserver in your windows server? Why is it important

To install Internet Information Services (IIS), follow the steps below:

1. Start > Control Panel > Programs and Features



Control Panel ▸ All Control Panel Items ▸ Programs and Features

Control Panel Home

View installed updates

Turn Windows features on or off

Install a program from the network

Uninstall or change a program

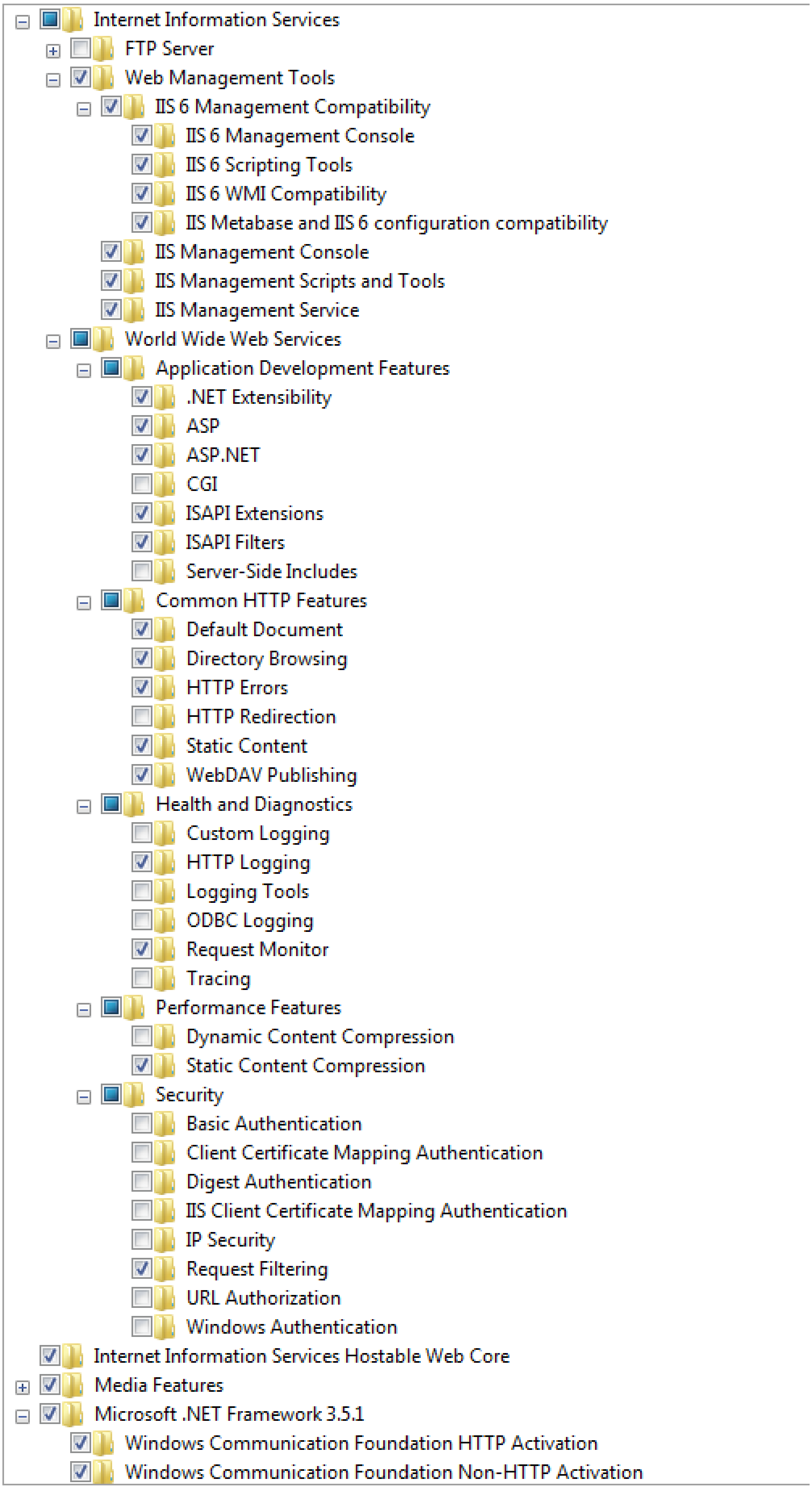
To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Organize ▾

Name	Publisher
7-Zip 9.20 (x64 edition)	Igor Pavlov
Adobe Flash Player 11 ActiveX	Adobe Systems Incorporated
Adobe Flash Player 14 Plugin	Adobe Systems Incorporated
Agile.NET 6.1.0	SecureTeam Software Ltd.
AMD Catalyst Install Manager	Advanced Micro Devices, Inc.
AnyMeeting Plug-in	AnyMeeting, Inc.
Astaro SSL VPN Client 1.7	
CamStudio	
CamStudio 2.7.2	CamStudio Open Source
CamStudio Lossless Codec v1.5	CamStudio
CamStudio OSS Desktop Recorder	CamStudio Open Source Dev Te...
CamStudio version 2.7	CamStudio Open Source
CardControl 2.0.9.0	SalesPad, LLC.
Cisco Systems VPN Client 5.0.07.0290	Cisco Systems, Inc.
Citrix Online Launcher	Citrix
CodeSmith Generator 6.5.3.14838	CodeSmith Tools, LLC
Crystal Reports Basic for Visual Studio 2008	Business Objects
Crystal Reports Basic Runtime for Visual Studio 2008 (x64)	Business Objects
CutePDF Writer 2.8	
DataCollection 4.0.0.13	SalesPad, LLC.
DataCollection Console 3.1	SalesPad, LLC.
DataCollection Desktop 3.1	SalesPad, LLC.
DataCollection Service	SalesPad, LLC.

2. Click Turn Windows features on or off. The Windows Features window will appear.

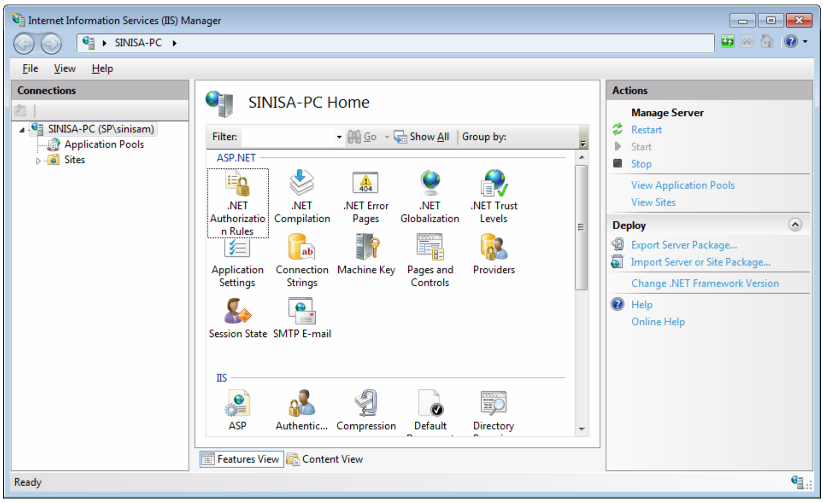
3. Make sure all features under Internet Information Services and Microsoft .NET Framework are select



- ⊟ ■ Internet Information Services
  - ⊞ □ FTP Server
  - ⊟ ☑ Web Management Tools
    - ⊟ ☑ IIS 6 Management Compatibility
      - ☑ IIS 6 Management Console
      - ☑ IIS 6 Scripting Tools
      - ☑ IIS 6 WMI Compatibility
      - ☑ IIS Metabase and IIS 6 configuration compatibility
    - ☑ IIS Management Console
    - ☑ IIS Management Scripts and Tools
    - ☑ IIS Management Service
  - ⊟ ■ World Wide Web Services
    - ⊟ ■ Application Development Features
      - ☑ .NET Extensibility
      - ☑ ASP
      - ☑ ASP.NET
      - □ CGI
      - ☑ ISAPI Extensions
      - ☑ ISAPI Filters
      - □ Server-Side Includes
    - ⊟ ■ Common HTTP Features
      - ☑ Default Document
      - ☑ Directory Browsing
      - ☑ HTTP Errors
      - □ HTTP Redirection
      - ☑ Static Content
      - ☑ WebDAV Publishing
    - ⊟ ■ Health and Diagnostics
      - □ Custom Logging
      - ☑ HTTP Logging
      - □ Logging Tools
      - □ ODBC Logging
      - ☑ Request Monitor
      - □ Tracing
    - ⊟ ■ Performance Features
      - □ Dynamic Content Compression
      - ☑ Static Content Compression
    - ⊟ ■ Security
      - □ Basic Authentication
      - □ Client Certificate Mapping Authentication
      - □ Digest Authentication
      - □ IIS Client Certificate Mapping Authentication
      - □ IP Security
      - ☑ Request Filtering
      - □ URL Authorization
      - □ Windows Authentication
- ☑ Internet Information Services Hostable Web Core
- ⊞ ☑ Media Features
- ⊟ ☑ Microsoft .NET Framework 3.5.1
  - ☑ Windows Communication Foundation HTTP Activation
  - ☑ Windows Communication Foundation Non-HTTP Activation

4.Click **OK** to install selected Windows components, including IIS.

5.To access IIS, click the Windows **Start** button. The Start menu/screen appears. Start typing internet information services manager in the search field and click the Internet Information Services (IIS) Manager once it appears.



6.What is public IP, private IP?

A **Public IP address** (*External*) is assigned to every device that connects to the Internet and each IP address is unique. Therefore, there cannot exist two devices with the same public IP address. This addressing scheme makes it possible for the devices to “find each other” online and exchange information. A user has no control over the IP address (public) that is assigned to the device. The public IP address is assigned to the device by the Internet Service Provider as soon as the device is connected to the Internet. This is known to be wrong.

A public IP address can be **static**, **dynamic** or **shared**.

Private IP address (*Internal*) is only used by devices communicating to each other on the same network. Devices with private IP addresses cannot connect to the Internet directly. Likewise, computers or other devices outside the local network cannot connect directly to a device with a private IP.

IP Address Terminology

Static means the IP address never changes as long as you stay with the same provider or same server.

Dynamic means the IP address can change from time-to-time.

Public means the IP address can be reached via the Internet from any computer in the world.

Private means the IP address can only be reached by other devices on the same network.

Shared means other people besides you use your IP address for their connection.

Dedicated means no one else uses your IP address for their connection.

Class identifies the range of your IP address and the default subnet mask. Examples of IP classes:

A class - 0 to 127 with default mask of 255.0.0.0

B class - 128 to 191 with default mask of 255.255.0.0

C class - 192 to 223 with default mask of 255.255.255.0

D class - 224 to 247 (not currently used)

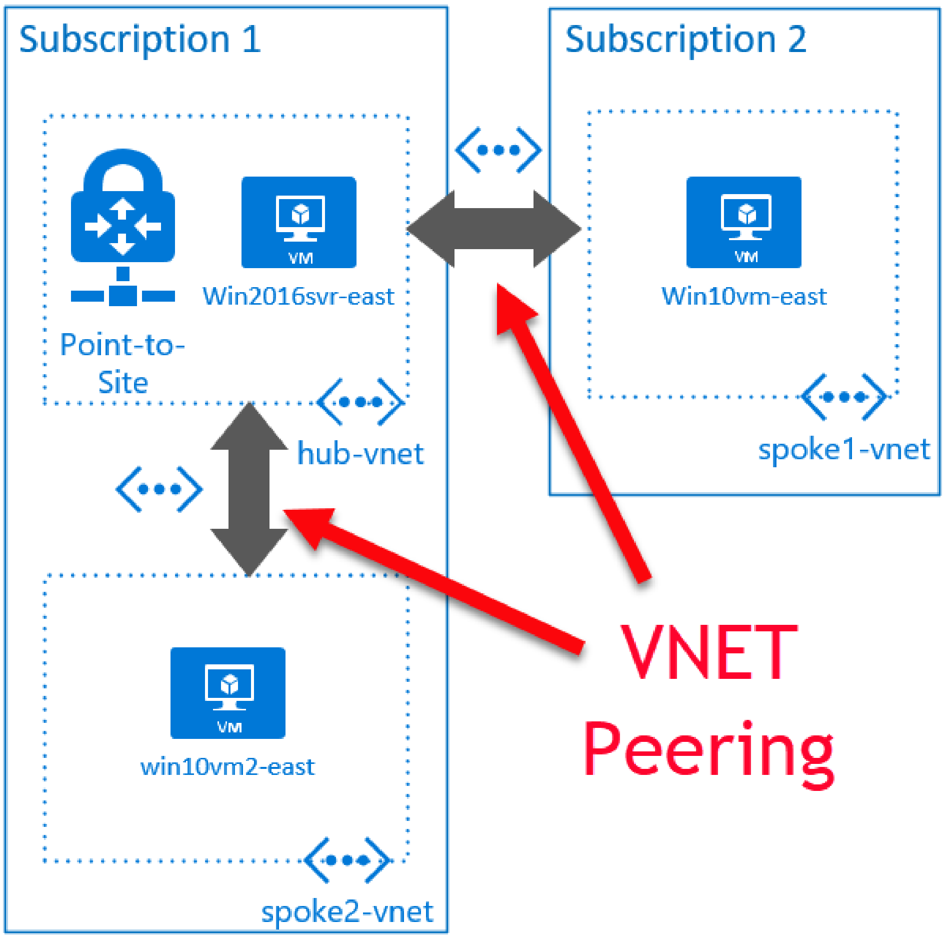
E class - 248 to 255 (not currently used)

7.What is vnet, subnet?

A **subnet** is a range of IP addresses in the **Vnet**. You can divide a **Vnet** into multiple **subnets** for organization and security. Each NIC in a VM is connected to one **subnet** in one **Vnet**. NICs connected to **subnets** (same or different) within a **Vnet** can communicate with each other without any extra configuration.

8.What is vnet peering?

Vnet peering is a mechanism that connects two virtual networks (VNets) in the same region through the Azure backbone network. Once **peered**, the two virtual networks appear as one for all connectivity purposes.



9.How to monitor your services in azure is (healthy or not)/is working properly or not?

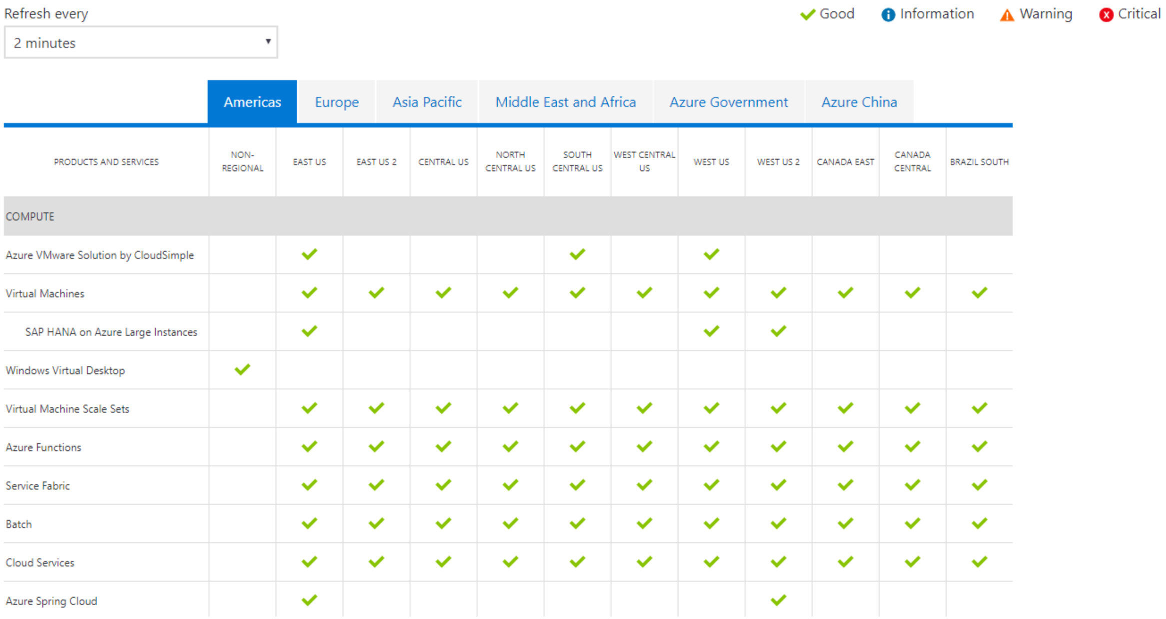
Microsoft Azure Service Health is your personalized dashboard in the Azure portal for receiving notifications, guidance, and technical support when Azure service issues, updates, or planned maintenance affect your Azure resources.

Azure health can be checked with variety of options available. But the native way is to monitor your resources using the Azure Service Health: Status page, Azure Service Health, Azure Resource Health. These are simple but effective solutions offered by Azure.

You can even use the Azure metrics to perform performance monitoring on your Azure resources. In this blog we will discuss on using Azure Service Health to monitor your Azure Status.

Azure Status

The Azure status page provides information about the health of Azure Services and regions. The Azure status page can help us understand the availability of resources in different regions. It is more useful for beginners who are looking for a region to host their Azure resources. Azure status page keeps the user informed on the service availability of each resource across various regions so the user can choose the right region for better performance and increased efficiency.



Refresh every: 2 minutes

✓ Good ⓘ Information ⚠ Warning ✖ Critical

Americas | Europe | Asia Pacific | Middle East and Africa | Azure Government | Azure China

PRODUCTS AND SERVICES	NON-REGIONAL	EAST US	EAST US 2	CENTRAL US	NORTH CENTRAL US	SOUTH CENTRAL US	WEST CENTRAL US	WEST US	WEST US 2	CANADA EAST	CANADA CENTRAL	BRAZIL SOUTH
COMPUTE												
Azure VMware Solution by CloudSimple		✓				✓		✓				
Virtual Machines		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SAP HANA on Azure Large Instances		✓						✓	✓			
Windows Virtual Desktop	✓											
Virtual Machine Scale Sets		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Functions		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Service Fabric		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Batch		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cloud Services		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Spring Cloud		✓							✓			

The Azure status page can be used by organizations to choose the best option to host their Azure resources across various regions as the hosting region plays an important role in the performance and availability of Azure resources.

10. What are the different types of disks we have when you create virtual machine?

That is, the files that **make** up an IDE **virtual disk** can be stored on either an IDE hard **disk** or a SCSI hard **disk**. So can the files that **make** up a SCSI **virtual disk**. **They** can also be stored on **other types** of fast-access storage media, such as DVD-ROM or CD-ROM **discs**.

Thin Provisioned Disks

Thin provisioning can be done on the virtual disk level (so per disk thin provisioning) or you at the storage array level.

It allows you to provision a disk without fully allocating all the necessary underlying physical storage. New storage blocks are allocated and zeroed on the fly, as the data is written by the guest.

When you provision a 100GB thin provisioned hard disk and you store 1GB of data on it, you will physically consume just the 1GB. This allows for overprovisioning of storage in which you provision more virtual storage than there is real physical capacity available.

Thick Lazy Zeroed

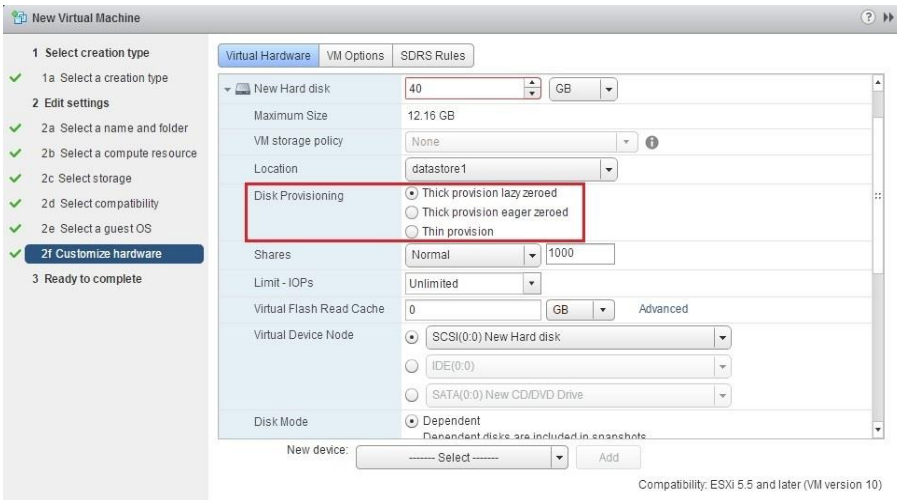
As opposed to thin-provisioned disks, thick provisioned disks allocate all the physical disk space on the creation of the virtual hard disk.

A 100GB virtual disk will consume 100GB of physical storage. Lazy zeroed disks do not wipe the allocated storage clean beforehand. With each first write, the storage block first needs to be zeroed. This adds some storage latency because there is additional I/O required.

Thick Eager Zeroed

Thick eager zeroed disks also allocate all the physical disk space and zero out all the storage blocks beforehand.

This disk type offers the best possible storage performance but is more inefficient and takes longer to provision.



New Hard disk	40 GB
Maximum Size	12.16 GB
VM storage policy	None
Location	datastore1
Disk Provisioning	● Thick provision lazy zeroed ○ Thick provision eager zeroed ○ Thin provision
Shares	Normal 1000
Limit - IOPs	Unlimited
Virtual Flash Read Cache	0 GB Advanced
Virtual Device Node	● SCSI(0:0) New Hard disk ○ IDE(0:0) ○ SATA(0:0) New CD/DVD Drive
Disk Mode	● Dependent Dependent disks are included in snapshots

New device: ------- Select ------- Add

Compatibility: ESXi 5.5 and later (VM version 10)

11. What is autoscaling?

Autoscaling provides the capability to run your application or workload with the required resources (resources, in this case, are virtual machines) without interruption. It assures you that the virtual machines you requested for your application are always available and up. If the virtual machines are interrupted, autoscaling replaces those faulty virtual machines with new ones.

Types of autoscaling

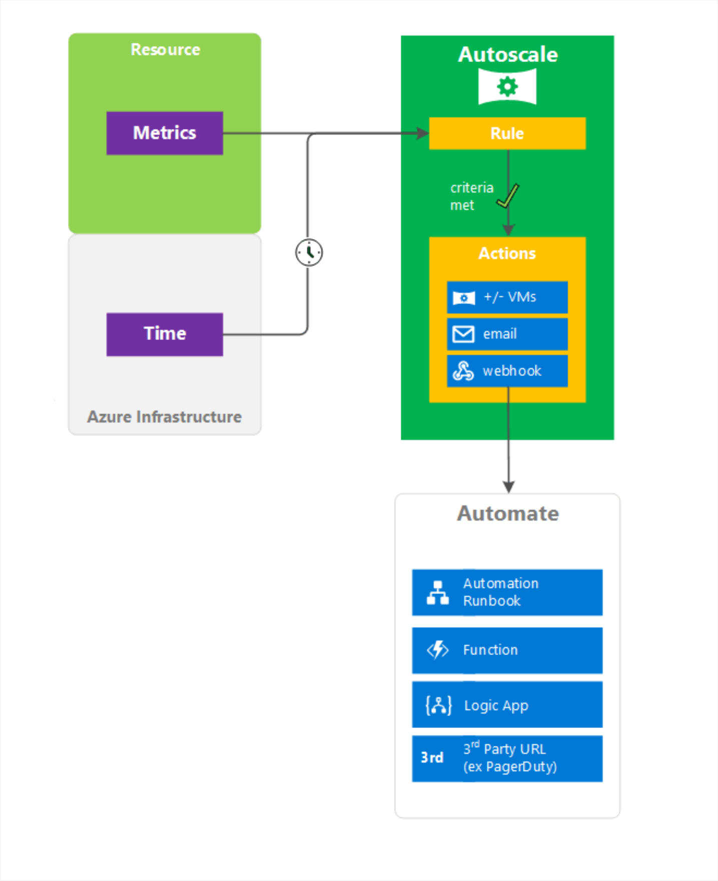
In general, there are two types of autoscaling –

Time-Based Autoscaling.

Metrics-Based Autoscaling.

Time-Based autoscaling is nothing but scaling based on the scheduled time. This type needs some extent of manual prediction of your demand. For example, suppose you know that your application experiences high traffic during certain times of the day, week or month and the number of virtual machines needed to meet that demand. In that case, you can configure the rules to spin up and shut down those needed virtual machines only during that specific time period.

On the other hand, Metrics-Based autoscaling enables the scaling activity to be based on the key performance metrics of your resource like CPU, Memory, Thread Count, etc.



12. What is inbound and outbound rules?

A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.

Default security rules

Azure creates the following default rules in each network security group that you create:

Inbound

AllowVNetInBound

ALLOWVNETINBOUND

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65000	Virtual Network	0-65535	Virtual Network	0-65535	Any	Allow

AllowAzureLoadBalancerInBound

ALLOWAZURELOADBALANCERINBOUND

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65001	AzureLoadBalancer	0-65535	0.0.0.0/0	0-65535	Any	Allow

DenyAllInbound

DENYALLINBOUND

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65500	0.0.0.0/0	0-65535	0.0.0.0/0	0-65535	Any	Deny

Outbound

AllowVnetOutBound

ALLOWVNETOUTBOUND

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65000	Virtual Network	0-65535	Virtual Network	0-65535	Any	Allow

AllowInternetOutBound

ALLOWINTERNETOUTBOUND

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65001	0.0.0.0/0	0-65535	Internet	0-65535	Any	Allow

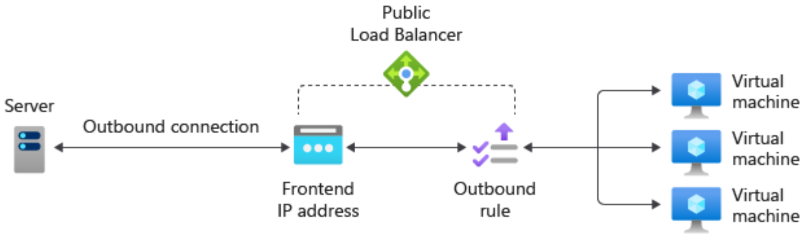
DenyAllOutBound

DENYALLOUTBOUND

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65500	0.0.0.0/0	0-65535	0.0.0.0/0	0-65535	Any	Deny

In the **Source** and **Destination** columns, *VirtualNetwork*, *AzureLoadBalancer*, and *Internet* are service tags, rather than IP addresses. In the protocol column, **any** encompasses TCP, UDP, and ICMP. When creating a rule, you can specify TCP, UDP, ICMP or Any. *0.0.0.0/0* in the **Source** and **Destination** columns represents all addresses. Clients like Azure portal, Azure CLI, or PowerShell can use * or any for this expression.

You cannot remove the default rules, but you can override them by creating rules with higher priorities.



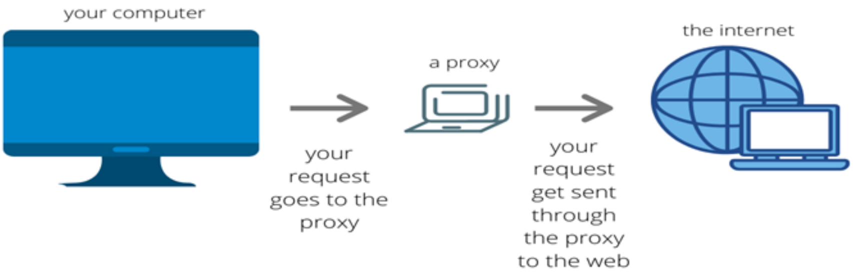
13. What is proxy server?

The **proxy server** is a computer on the internet that accepts the incoming requests from the client and forwards those requests to the destination server. It works as a gateway between the end-user and the internet. It has its own IP address. It separates the client system and web server from the global network.

In other words, we can say that the proxy server allows us to access any websites with a different IP address. It plays an intermediary role between users and targeted websites or servers. It collects and provides information related to user requests. The most important point about a proxy server is that it does not **encrypt traffic**.

There are two main purposes of proxy server:

To keep the system behind it anonymous.
To speed up access to a resource through caching.



14. What is backend pool?

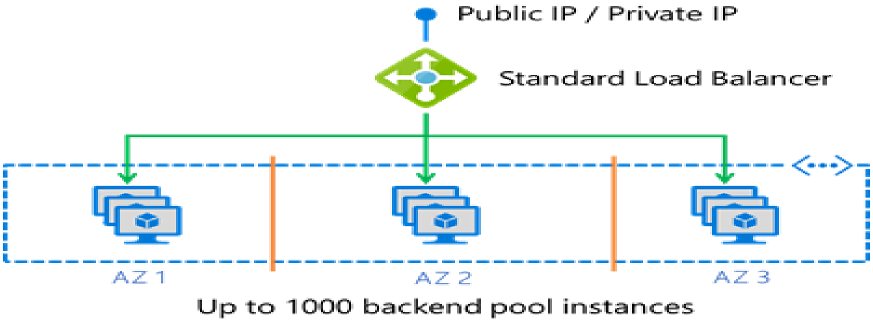
The backend pool is a critical component of the load balancer. The backend pool defines the group of resources that will serve traffic for a given load-balancing rule.

There are two ways of configuring a backend pool:

Network Interface Card (NIC)

Combination of IP address and Virtual Network (VNET) Resource ID

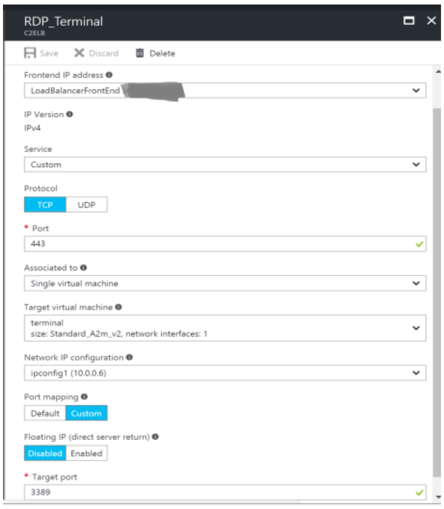
Configure your backend pool by NIC when using existing virtual machines and virtual machine scale sets. This method builds the most direct link between your resource and the backend pool.



15. What is port number? What are the allowed number for port and how it can be configurable?

Port number is the part of the addressing information used to identify the senders and receivers of messages in computer networking. Different port numbers are used to determine what protocol incoming traffic should be directed to.

Ports are represented by 16-bit numbers. 0 to 1023 are restricted port numbers are as they are used by well-known protocol services. 1024 to 49151 are registered port numbers means it can be registered to specific protocols by software corporations and in last 49152 to 65536 are used as private ports means they can be used by anybody.



RDP_Terminal
C2ELB

Frontend IP address
LoadBalancerFrontEnd [redacted]

IP Version
IPv4

Service
Custom

Protocol
[✓ TCP] UDP

* Port
443

Associated to
Single virtual machine

Target virtual machine
terminal
size: Standard_A2m_v2, network interfaces: 1

Network IP configuration
ipconfig1 (10.0.0.6)

Port mapping
Default [✓ Custom]

Floating IP (direct server return)
[✓ Disabled] Enabled

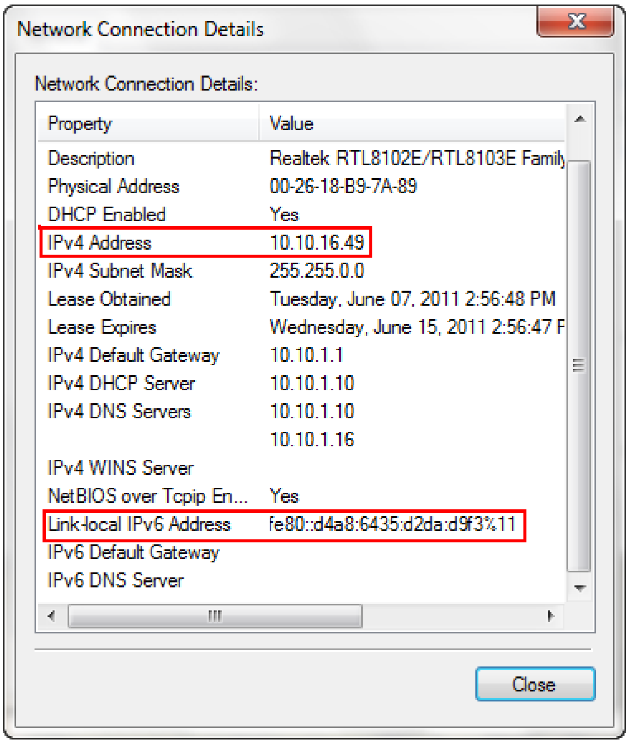
* Target port
3389

16. What is IPV4 and IPV6?

The **Internet Protocol version 4 (IPv4)** is a protocol for use on packet-switched **Link Layer networks** (e.g. **Ethernet**). IPv4 provides an addressing capability of approximately 4.3 billion addresses.

The **Internet Protocol version 6 (IPv6)** is more advanced and has better features compared to IPv4. It has the capability to provide an infinite number of addresses. It is replacing IPv4 to accommodate the growing number of networks worldwide and help solve the IP address exhaustion problem.

One of the differences between IPv4 and IPv6 is the appearance of the IP addresses. IPv4 uses four 1-byte decimal numbers, separated by a dot (i.e. **192.168.1.1**), while IPv6 uses hexadecimal numbers that are separated by colons (i.e. **fe80: d4a8:6435: d2d8: d9f3b11**).



Network Connection Details:

Property	Value
Description	Realtek RTL8102E/RTL8103E Famil
Physical Address	00-26-18-B9-7A-89
DHCP Enabled	Yes
IPv4 Address	10.10.16.49
IPv4 Subnet Mask	255.255.0.0
Lease Obtained	Tuesday, June 07, 2011 2:56:48 PM
Lease Expires	Wednesday, June 15, 2011 2:56:47 F
IPv4 Default Gateway	10.10.1.1
IPv4 DHCP Server	10.10.1.10
IPv4 DNS Servers	10.10.1.10 10.10.1.16
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	fe80::d4a8:6435:d2da:d9f3%11
IPv6 Default Gateway	
IPv6 DNS Server	

Below is the summary of the differences between the IPv4 and IPv6:

	IPv4	IPv6
No. of bits on IP Address	32	128
Format	decimal	hexadecimal
Capable of Addresses	4.3 billion	infinite number
How to ping	ping XXX.XXX.XXX	ping6

Advantages of IPv6 over IPv4:

- IPv6 simplified the router's task compared to IPv4.
- IPv6 is more compatible to mobile networks than IPv4.
- IPv6 allows for bigger payloads than what is allowed in IPv4.
- IPv6 is used by less than 1% of the networks, while IPv4 is still in use by the remaining 99%.

17. How do you check the what are the applications running on your vm?

```
public bool DetectVirtualMachine ()
  {
     bool result = false;
   const string MICROSOFTCORPORATION ="microsoft corporation";
     try
     {
        ManagementObjectSearcher searcher =
           new ManagementObjectSearcher ("root\\CIMV2","SELECT * FROM Win32_BaseBoard");

        foreach (ManagementObject queryObj in searcher. Get ())
        {
          result = queryObj["Manufacturer"]. ToString (). ToLower () ==
MICROSOFTCORPORATION.ToLower();
        }
        return result;
     }
     catch (ManagementException ex)
     {
        return result;
     }
  }
```

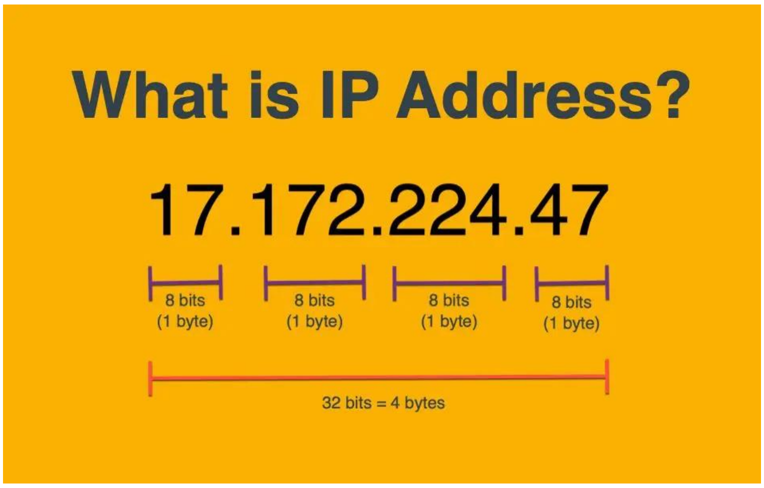
18. How do you check your CPU utilization?

There are two ways to check the CPU utilization of webapp in azure.

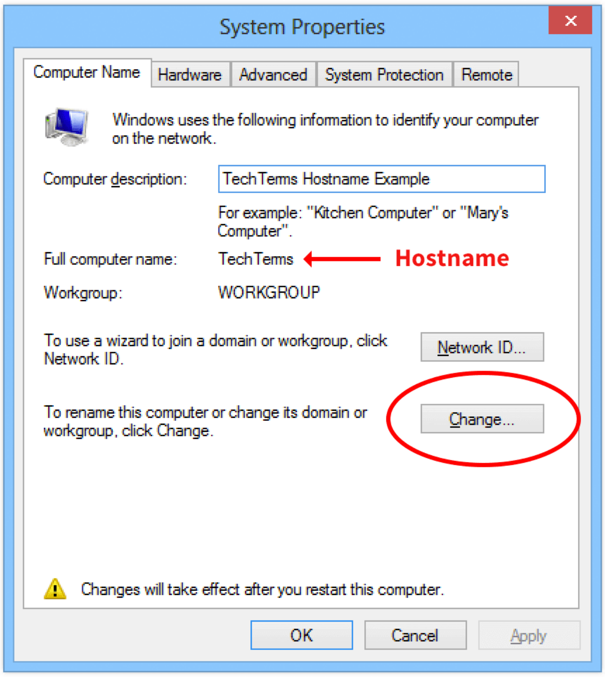
1. App service Plan -> Overview -> CPU Percentage chart. (Overall CPU utilization of the resource in the app service plan)
2. Go to specific azure resource such as web app and then click on Diagnose and solve problem -> Availability and Performance -> CPU Usage.

19. What is Ip address, hostname?

An Internet Protocol address is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. An IP address serves two main functions: host or network interface identification and location addressing.



In computer networking, a hostname is a label that is assigned to a device connected to a computer network and that is used to identify the device in various forms of electronic communication, such as the World Wide Web. Hostnames may be simple names consisting of a single word or phrase, or they may be structured.



Windows uses the following information to identify your computer on the network.

Computer description: TechTerms Hostname Example

For example: "Kitchen Computer" or "Mary's Computer".

Full computer name: TechTerms

Workgroup: WORKGROUP

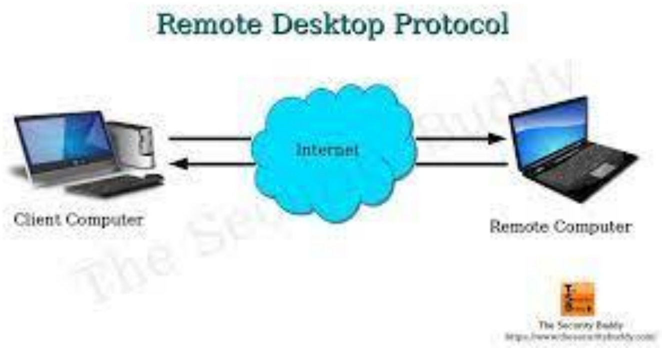
To use a wizard to join a domain or workgroup, click Network ID.

To rename this computer or change its domain or workgroup, click Change.

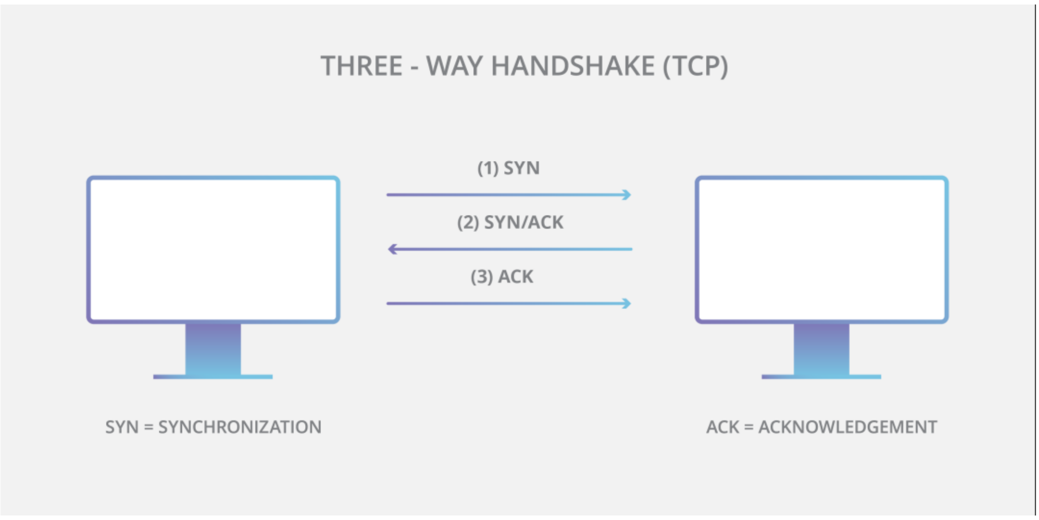
Changes will take effect after you restart this computer.

20. What is RDC/TCP/SSH?

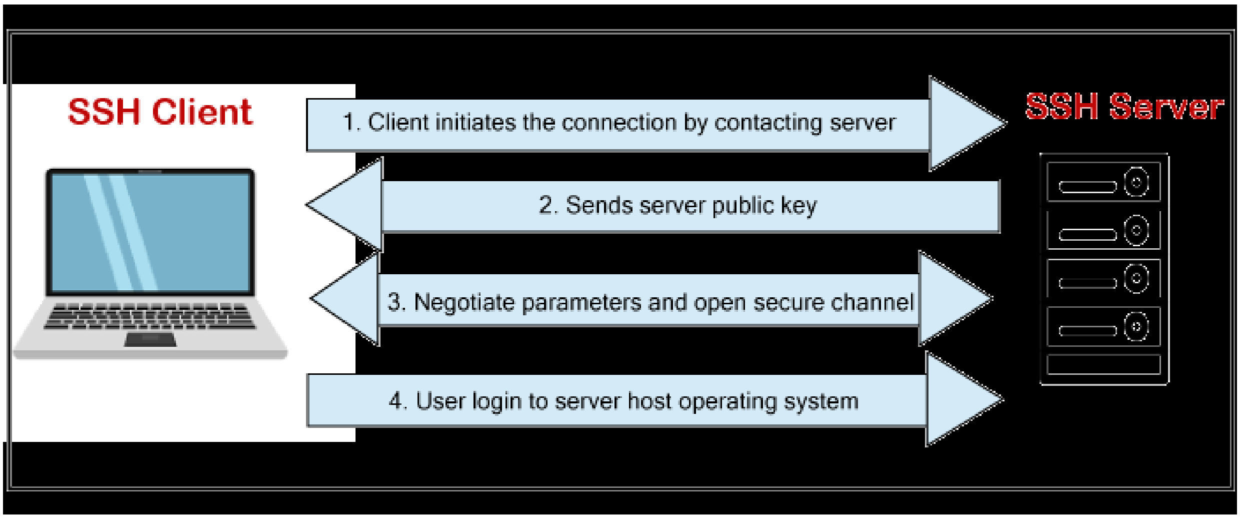
RDP: Remote Desktop Protocol is a proprietary protocol developed by Microsoft which provides a user with a graphical interface to connect to another computer over a network connection.



TCP: The Transmission Control Protocol is one of the main protocols of the Internet protocol suite. It originated in the initial network implementation in which it complemented the Internet Protocol. Therefore, the entire suite is commonly referred to as TCP/IP.



SSH: The Secure Shell Protocol is a cryptographic network protocol for operating network services securely over an unsecured network. Typical applications include remote command-line, login, and remote command execution, but any network service can be secured with SSH.


SSH Client
1. Client initiates the connection by contacting server
SSH Server
2. Sends server public key
3. Negotiate parameters and open secure channel
4. User login to server host operating system