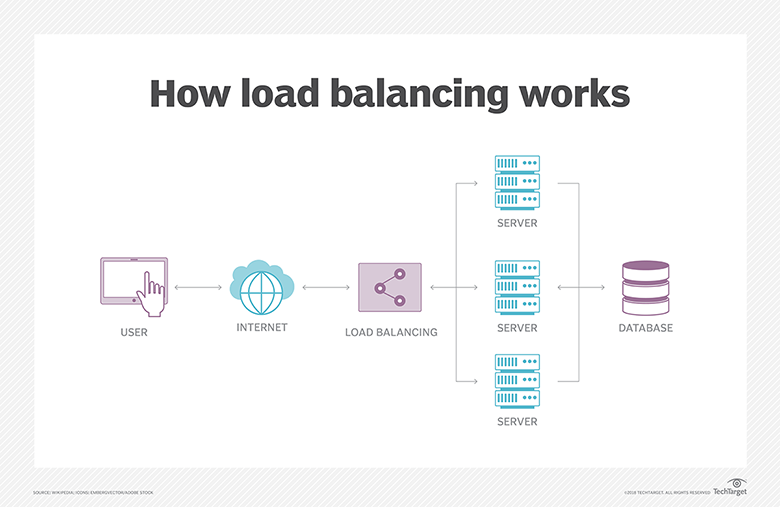
**1. What is load balancer?**

 A [load balancer](https://www.radware.com/Products/Alteon/) is a piece of hardware (or virtual hardware) that acts like a reverse proxy to distribute network and/or application traffic across different servers. A load balancer is used to improve the concurrent user capacity and overall reliability of applications. A load balancer helps to improve these by distributing the workload across multiple servers, decreasing the overall burden placed on each server.



2. What are the types of load balancers?

When talking about types of load balancers, it’s also important to note there are hardware load balancers, software load balancers, and virtual load balancers.

* **Hardware Load Balancer:** A hardware load balancer, as the name implies, relies on physical, on-premises hardware to distribute application and network traffic. These devices can handle a large volume of traffic but often carry a hefty price tag and are fairly limited in terms of flexibility.
* **Software Load Balancer:**A software load balancer comes in two forms—commercial or open-source—and must be installed prior to use. Like cloud-based balancers, these tend to be more affordable than hardware solutions.
* **Virtual Load Balancer:**A virtual load balancer differs from software load balancers because it deploys the software of a hardware load balancing device on a virtual machine.

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.

To illustrate, think of a program that wants to connect with another. Before it can establish a connection, it must first connect to an application gateway, which then accesses the desired system on its behalf. That way, the computer on the receiving end is protected from possible malicious attacks.

So, what is an application gateway in simple terms? 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 application gateway?  
 load balancer applicaton gateway

works with traffic at Layer 4     works with traffic at Layer 7

Load Balancer is free Application Gateway is billed per-hour

LBonly supports only Azure endpoints          AG can support any routable IP address.

5.How do you configure IIS web server in windows server? why it is important?

To enable IIS and the required IIS components on Windows 10, do the following:

1. Open **Control Panel** and click **Programs and Features > Turn Windows features on or off**.
2. Enable **Internet Information Services**.
3. Expand the **Internet Information Services** feature and verify that the web server components listed in the next section are enabled.
4. Click **OK**.

Required IIS components

The IIS components listed below satisfy the minimum requirements to run the Web Adaptor. If other IIS components are enabled, they do not need to be removed.

* Web Management Tools
  + IIS 6 Management 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 4.5
    - ASP.NET 4.5
    - ISAPI Extensions
    - ISAPI Filters
    - WebSocket Protocol
  + Common HTTP Features
    - Default Document
    - Static Content
  + Security
    - Basic Authentication
    - Request Filtering
    - Windows Authentication

Most commonly, **IIS** is **used** to host ASP.NET web applications and static websites. It can also be **used as** an FTP server, host WCF services, and be extended to host web applications built on other platforms such as PHP. There are built-in authentication options such as Basic, ASP.NET, and Windows auth

6.What is public ip ,private ip?

A public IP address is an IP address that can be accessed directly over the internet and is assigned to your network router by your internet service provider (ISP). Your personal device also has a private IP that remains hidden when you connect to the internet through your router’s public IP.

Using a public IP address to connect to the internet is like using a P.O. box for your snail mail, rather than giving out your home address. It’s a little bit safer, but a lot more visible.

A **private IP address** is a non-Internet facing **IP address** on an internal network. **Private IP addresses** are provided by network devices, such as routers, using network **address** translation (NAT). ... **Private IP** addressing uses **addresses** from the class C range reserved for NAT (192.168. 0.0 – 192.168.

7..what sub net and v net?

**subnet** (subnetwork) A **subnet**, or subnetwork, is a segmented piece of a larger network. More specifically, **subnets** are a logical partition of an IP network into multiple, smaller network segments. The Internet Protocol (IP) is the method for sending data from one computer to another over the internet.

An Azure **Virtual Network** (**VNet**) is a representation of your own network in the cloud. ... When you create a **VNet**, your services and VMs within your **VNet** can communicate directly and securely with each other in the cloud.

8.what is v net 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 (healthy or not) is working properly or not?

Use **Azure Monitor** to send emails for Health **Service** Faults ... **Azure Monitor** **works**, how to install **Azure Monitor**, and how to configure it to send you notifications. ... logging on **your** cluster, the next step is to **properly** configure log analytics. ... from the drop-down list if the default selected is **not** appropriate.

10.what are the different types of disks we have when you create VM?

So in VMware there are 3 **types of disks you** can assign **to** your virtual server at the time of creation or later. Thin **Disks** & Thick **Disks**. When **we create** a **vm we need to** allocate some **disk** space **to** the **vm** for used as the storage. **Disk** is used from the datastore which is added into the vSphere from the Storage LUN

11.what is auto scalling?

Autoscaling, also spelled auto scaling or auto-scaling, and sometimes also called automatic scaling, is a method used in cloud computing that dynamically adjusts the amount of computational resources in a server farm - typically measured by the number of active servers - automatically based on the load on the farm.

12.what is inbound and outbound rules?

**Inbound rules** filter traffic passing from the network to the local computer based on the filtering conditions specified in the **rule**. Conversely, **outbound rules** filter traffic passing from the local computer to the network based on the filtering conditions specified in the **rule**.

13.what is proxy server?

a proxy server is a server application or appliance that acts as an intermediary for requests from clients seeking resources from servers that provide those resources

14.what is backend pools?

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

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

A port number is a way to identify a specific process to which an Internet or other network message is to be forwarded when it arrives at a [server](https://whatis.techtarget.com/definition/server). For the Transmission Control Protocol and the User Datagram Protocol, a port number is a 16-[bit](https://whatis.techtarget.com/definition/bit-binary-digit) [integer](https://whatis.techtarget.com/definition/integer) that is put in the header appended to a message unit. This port number is passed logically between [client](https://searchenterprisedesktop.techtarget.com/definition/client) and server transport layers and physically between the transport layer and the [Internet Protocol](https://searchunifiedcommunications.techtarget.com/definition/Internet-Protocol) layer and forwarded on.

**Ports** 0 through 1023 are defined as well-known **ports**. Registered **ports** are from 1024 to 49151. The remainder of the **ports** from 49152 to 65535 **can** be used dynamically by applications.

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). ... 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.

**No. of bits on IP Address:**32

**Capable of Addresses:**4.3 billion

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

**18. How to Check CPU Utilization?**

1. Start **the** Task Manager. Press **the** buttons Ctrl, Alt and Delete all at **the** same time. ...
2. Choose "Start Task Manager." This will open **the** Task Manager Program window.
3. Click **the** "Performance" tab. In this screen, **the** first box shows **the** percentage of **CPU usage**.

19.what is ip address and host name?

In the Internet, a **hostname** is a domain name assigned to a host computer. This is usually a combination of the host's local name with its parent domain's name. ... This kind of **hostname** is translated into an **IP address** via the local hosts file, or the Domain Name System (DNS) resolver.

20. what is RDP, 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. The user employs RDP client software for this purpose, while the other computer must run RDP server software.

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