**Sample technical questions**

**What is the difference between Kerberos and NTLM**

Kerberos is the name of a computer network authentication protocol, which allows individuals to communicate over a non-secure network to prove their identity to one another in a secure manner. It is also a suite of free software published by the Massachusetts Institute of Technology (MIT) that implements this protocol. Its designers aimed primarily at a client-server model, and it provides mutual authentication both the user and the server verify each other's identity. Kerberos protocol messages are protected against eavesdropping and replay attacks.

NTLM is easy to track. And sniff

**See top process**

Ps -tuna

**In Linux, run levels:**

Run level 0, level 1 , level 2 , level 3 ….5

**Linux Command:**

<https://www.geeksforgeeks.org/top-command-in-linux-with-examples/>

**Stateful firewall**

Before the development of stateful firewalls, firewalls were *stateless*. A stateless firewall treats each [network frame](https://en.wikipedia.org/wiki/Frame_(telecommunications)) or [packet](https://en.wikipedia.org/wiki/Packet_(information_technology)) individually. Such [packet filters](https://en.wikipedia.org/wiki/Packet_filter) operate at the OSI [Network Layer](https://en.wikipedia.org/wiki/Network_Layer) (layer 3) and function more efficiently because they only look at the [header](https://en.wikipedia.org/wiki/Header_(computing)) part of a [packet](https://en.wikipedia.org/wiki/Packet_(information_technology)).[[3]](https://en.wikipedia.org/wiki/Stateful_firewall#cite_note-3) They do not keep track of the packet context such as the nature of the traffic.[[4]](https://en.wikipedia.org/wiki/Stateful_firewall#cite_note-4) Such a firewall has no way of knowing if any given packet is part of an existing connection, is trying to establish a new connection, or is just a rogue packet. Modern firewalls are connection-aware (or state-aware), offering network administrators finer-grained control of network traffic.

**Firewall or UTM**

A firewall is a device which blocks network traffic at the IP and IP:port (socket) levels. Some have stateful inspection such that it monitors the initial TCP handshake and some do not. Generally a firewall is used for blocking entire protocols and types of traffic, but it doesn't look into the actual content.

Unified Threat Management takes it a step further. A solution of this type will be a firewall, however it will do deeper inspection into the packets at layers 5, 6 or 7 (see OSI model). In addition to firewall functionality, UTM should also include functionality which is termed Intrusion Detection and/or Intrusion Prevention (IDS or IPS), network based anti-virus or other malware prevention.

So lets use an example:

A firewall might be configured to permit HTTP port 80 traffic between two hosts. However, you could have someone sending a SQL injection attack on port 80 to the web server, which in turn sends it to the backend DB, thereby corrupting your system. A UTM or IPS system would block that attack, while a firewall would not.

In a small or medium-sized business, UTM makes more sense because you're bundling functionality onto a single stack and you probably have more generalists than specialists in network security.

In a large enterprise, however, typically we have functionality separated out into firewalls, IPS devices, anti-virus, anti-malware, layer-7 inspection, etc.

So to net it out, a firewall does inspection at layer 4 on the OSI model while UTM will look at 4, 5, 6 and 7.

---------------------------------------------------

**AES** is asymmetric cryptographic algorithm, while **RSA** is an asymmetric (or public key) cryptographic algorithm. Encryption and decryption is done **with a** single key in **AES**, while you use separate keys (public and private keys) in **RSA**. The strength **of** a 128-bit **AES** key is roughly equivalent to 2600-bits **RSA** key.

---------------------------

**1) Explain what is Windows Server?**

Windows server is a series of server operating systems developed by Microsoft Corporation.

**2) Explain in windows DNS server what is Primary, Secondary and Stub zone?**

In windows DNS server,

* Primary Zone: In this, the file is saved as normal text file with filename (.dns).
* Secondary Zone: It maintains a read-only copy of zone database on another DNS server. Also, it acts as a back-up server to the primary server by providing fault tolerance and load balancing
* Stub Zone: It consists of a copy of name server and SOA records which is used for reducing the DNS search orders. When stub zones were made available, it became a solution to overcome this security issue. What is also beneficial about Stubs, is you can AD integrate them instead of manually creating a Stub on each individual DC. This way the zone will be available domain or forest-wide, depending on replication scope.

**3) Explain what does IntelliMirror do?**

IntelliMirror helps to reconcile desktop settings, applications and stored files for users especially for those users who move between workstations or those who works offline

**4) In the case when MSI file is not available, how you can install an app?**

To add the application using the Software Installer.**ZAP text file** can be used rather than the windows installer

**5) Explain how you can set up remote installation procedure without giving access to user?**

To do that, you have to go to,

gponame> User Configuration > Windows Settings > Remote Installation Services > Choice Options

**6) What does it mean by “tattooing” the Registry ?**

“ Tattooing” the registry means user can modify and view user preference that are not stored in the maintained portions of the Registry. Even if the group policy is changed or removed, the user preference will still persist in the registry.

**7) Mention how many types of queries DNS does?**

The types of queries DNS does are

* Iterative Query
* Recursive Query

**8) Explain what is the primary function of the domain controller?**

Primary function of the domain controller is to validate users to the networks, it also provide a catalog of Active Directory Objects.

**9) What information is required when TCP/IP is configured on Window Server?**

To configure a TCP/PI client for an IPv4 client, you have to provide the IP address and the subnet mask.

**10) Explain what does it mean caching only server in terms of DNS?**

The caching only DNS server provides information related to queries based on the data it contains in its DNS cache.

**11) Explain what is the way to configure the DHCP server such that it allocates the same IP address to certain devices each time the address is removed?**

To configure the DHCP server, you can create a **reservation** for the device. To create a reservation, you must know the MAC hardware address of the device. To determine the MAC address for a network device you can use the ipconfig or nbs tat command line utilities.

**12)**  **Explain what is LDAP?**

To look up for the information from the server, e-mail and another program follows or uses the internet protocol. This protocol is referred as LDAP or Lightweight Directory Access Protocol.

**13) Explain what is SYSVOL folder?**

It is a set of files and folders that is stored on the local hard disk of each domain controller in a domain and are replicated by the FRS ( File Replication Service). These files contain group or user policy information.

**14) Explain what is the difference between a thread and a computer process?**

Computer Process: In computing, a process is an instance of a computer program that is executed sequentially by a computer system which can run several computer programs concurrently.

Thread: A thread is a several executable program that work together as a single process. For instance, one thread might send an error message to the user; another might handle error signals while the third thread might be executing the original action.

**15) Explain what is INODE?**

INODE holds the metadata of files; INODE is a pointer to a block on the disk, and it is unique.

In simple words, it is a unique number allocated to a file in UNIX-like OS.

**16) Explain what is RAID in Windows Server?**

For storing same data at a different place RAID or Redundant Array of Independent Disks strategy is used. It is a strategy for building **fault tolerance and increase the storage capacity**. On separate drives it allows you to combine one or more volumes so that they are accessed by a single drive letter

**17) Explain what is the purpose of deploying local DNS servers?**

A local DNS server provides the local mapping of fully qualified domain names to IP addresses. To resolve remote requests related to the domains names on your network, local DNS servers can provide record information to remote DNS servers.

**18) To check TCP/IP configurations and IP connectivity, what are the two command line utilities that can be used?**

**Ipconfig:** To check the computer’s IP configuration, command ipconfig can be used and also it can be used to renew the client’s IP address if it is provided by a DHCP server.

**Ping:** To check the connection between the local computer and any of the other computer device on the network Ping command is used

**19) Explain if it is possible to connect Active Directory to other 3rd party Directory services?**

Yes, you can connect other vendors directory services with Microsoft version. By using dirXML or LDAP to connect to other directories.

**20) Explain where is the AD database is held?**

AD database is saved in %systemroot%/ntds. Files that controls the AD structure are

* ntds.dit
* edb.log
* res1.log
* res2.log
* edn.chk

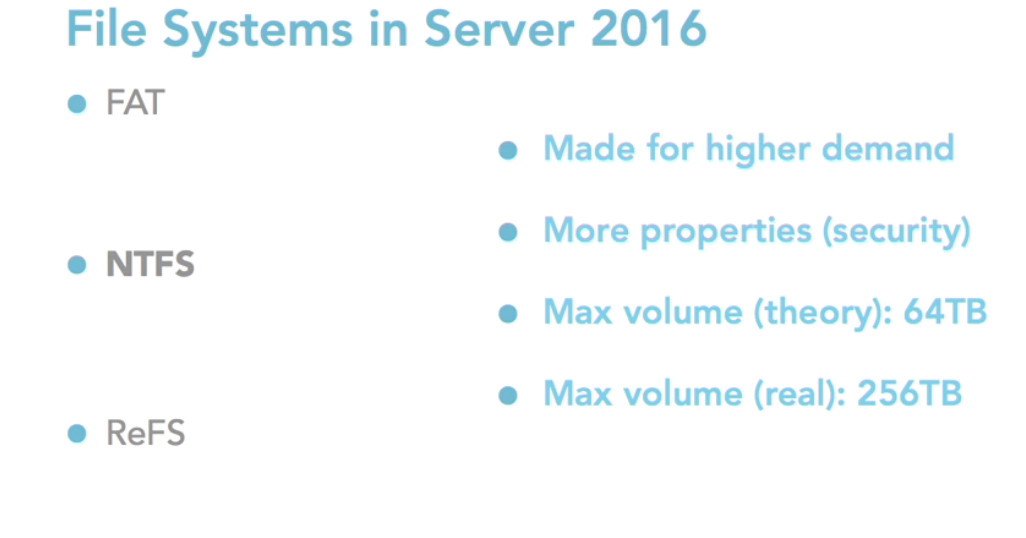
**21) Explain what is the major difference between NTFS ( New Technology File System) or FAT (File Allocation Table) on a local server?**

For local users FAT (File Allocation Table) and FAT32 provides security, while NTFS ( New Technology File System) provides security for domain users as well as local users. NTFS provides file level security which is not possible through FAT32.

**22) Mention what windows server 2008 service is used to install client operating system over the network?**

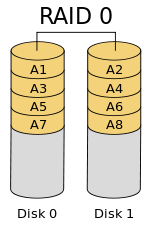
WDE ( Windows Deployment Services ) allows you to install client and server operating systems over the network to any computer with a PXE enabled network interface

The Resilient File System (ReFS) is Microsoft’s newest file system, designed to maximize data availability, scale efficiently to large data sets across diverse workloads, and provide data integrity by means of resiliency to corruption. It seeks to address an expanding set of storage scenarios and establish a foundation for future innovations.



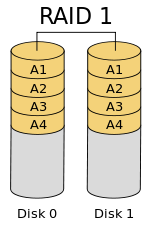
**RAID 0 (Strip)**

* Not Fault Tolerant
* Performance benefit



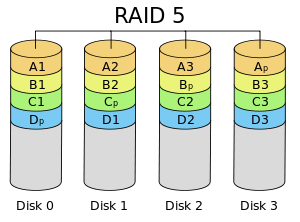
**RAID 1 (mirror)**

* Fault-Tolerant
* Performance benefit



**RAID 5**

* Fault-Tolerant
* At least 3 disks ( one parity - two data)
* performance benefit



**NFS(Network File Share)**

NFS is good for **UNIX server-to-server** file sharing. However it is incompatible with Windows clients, and is useless for Mac file sharing clients due to missing features, and compatibility and performance problems with Mac apps.

**SMB/CIFS (Server Message Block)**

The native Windows network file sharing protocol is the preferred protocol for Windows clients.

**AFP(Apple Filing Protocol)**

AFP is clearly superior to SMB or NFS for Mac OS 8.1-OS X 10.8 clients

AFP is the native file and printer sharing protocol for Macs and it supports many unique Mac attributes that are not supported by other protocols. So for the best performance, and 100% compatibility, AFP should be used.

**What are the basic commands to troubleshoot connectivity between vSphere Client /vCenter to ESX server?**

service mgmt–vmware restart (restarts host agent(vmware–hostd) on vmware esx server)

service vmware-vpxa restart (restarts Vcenter agent service)

service network restart (restarts management networks on ESX)

**What is vCenter Agent?**

VC agent is an agent installed on ESX server which enables communication between VC and ESX server. This Agent will be installed on ESX/ESXi will be done when you try to add the ESx host in Vcenter.

**What is the command used to restart SSH, NTP & Vmware Web access?**

It is very important to understand the command to start and stop services. So i have covered basic service restart command in the below *VMware interview questions.*

Service sshd restart

Service ntpd restart

Service vmware–webaccess restart

**What are the types of Ports groups in ESX/ESXi?**

There are 3 types of port groups in ESX

1.Service console port group

2.VMkernel Port group

3. Virtual machine port group

There are only 2 types of port group in ESXi

1. Vmkernel Port group

2.Virtual Machine Port group

**What is VMKernel ?**

VMWare Kernel is a Proprietary kernel of vmware and is not based on any of the flavors of Linux operating systems, .VMkernel requires an operating system to boot and manage the kernel. A service console is being provided when VMWare kernel is booted. Only service console is based up on Redhat Linux OS not VMkernel.

**What is the use of Service Console port ?**

Service console port group required to manage the ESX server and it acts as the management network for the ESX. vCenter/vSphere Client uses the service console IP’s to communicate with the ESX server. This is one of the frequently asked **VMware interview questions.**

**What is the use of VMKernel Port ?**

Vmkernel port is used by ESX/ESXi for vmotion, ISCSI & NFS communications. ESXi uses Vmkernel as the management network since it don’t have service console built with it.

**What is the use of Virtual Machine Port Group?**

Virtual Machine port group is used by Virtual machine communication.

All the Virtual Machines which are configured in VM Port Group are able to connect to the other machines on the network. So this port group enables communication between vSwitch and Physical Switch by the use of uplink (Physical NIC) associated with the port group.

**What is the default number of ports configured with the Virtual Switch?**

When the time of Virtual switch created, Vswitch is created with 56 ports by default. We can extend the no of ports by editing the vswitch properties.

**What are the different types of Partitions in ESX server?**

/ -root

Swap

/var

/Var/core

/opt

/home

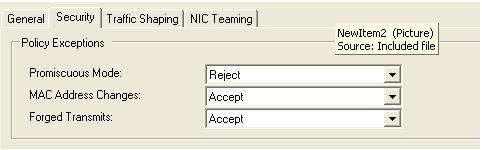
/tmp

**What are the security options available for ESX vswitch?**

Promiscuous Mode – Reject

MAC Address changes – Accept

Forged Transmits – Accept

****

**What is Promiscuous Mode ? it is like port span in cisco**

If the promiscuous mode set to Accept, all the communication is visible to all the virtual machines, in other words all the packets are sent to all the ports on vSwitch. It can be useful when you are running virtual machines with network sniffers to capture packet in that network.

**What is MAC Address changes?**

All the virtual machines nics are provide with the MAC address at the time of creation and it is stored in .VMX file. If the packet doesn’t match with the MAC address as same as in the .VMX file , it does not allow incoming traffic to the VM by setting this option as reject.

If it is set as Accept,ESX accepts requests to change the effective MAC address to other than the MAC address save din the .VMX file.

**What is Forged Transmits ?**

Which is same as the Mac Address changes setting but it worked for the outgoing traffic but the MAC address changes setting is for incoming traffic.

**What is a VLAN?**

A [VLAN](http://www.vmwarearena.com/vlan-tagging-vst-est-vgt-on-vmware/) is the Virtual LAN which is used to broke down the Broadcast traffic into many logical groups. Basically, one physical switch comprises of one broadcast domain. VLAN used to separate the one broadcast domain into many small pieces to separate the networks within the broadcast domain.

**What are the types of VLAN tagging in Vsphere?**

There are 3 types of VLAN tagging available in Vsphere.

1.Virtual Switch Tagging (VST)

2.External Switch Tagging (EST)

3.Virtual Guest Tagging (VGT)

**What is VST , EST & VGT?**

**VST**

1.1 VST uses 802.1q VLAN trunks and tagged traffic.

1.2 Tagging for all packets is performed by the Virtual Switch before leaving the ESX/ESXI host

1.3 Port groups on the Virtual switch of ESX server should be configured with VLAN ID (1-4094)

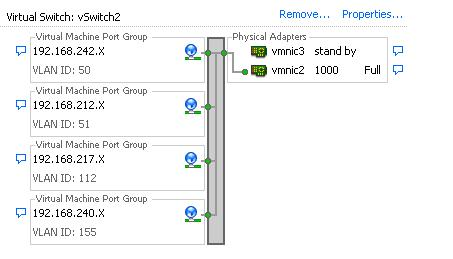
1.4 vSwitch responsibility is to strip off the vlan tag and send packet to virtual machine in corresponding port group.

1.5 Reduces the number of Physical nics on the server by running all the VLANs over one physical nic. Better solution would be keep 2 nics for redundancy.

1.6 Reduces number of cables from ESX server to physical switch.

1.7 The physical switch port connecting the uplink from the ESX should be configured as Trunk port.

1.8 virtual machine network Packet is delivered to vSwitch and before it is sent to physical switch the packet is tagged with vlan id according to the port group membership of originating virtual machine



### **2.External Switch Tagging (EST)**

2.1 In EST, the ESX host doesn’t see any VLAN tags and does not handle any VLAN tagging.

2.2 All the tagging operation is done by the physical switch and the virtual switch is not aware of that.

2.3 Number of physical nics = no of VLANs connected to ESX

2.4 Port groups on the Virtual switch of ESX server need not be configured with the VLAN number or configure VLAN ID 0 (if it is not native VLAN)

2.5 Count of NICS and cable connected to ESX is more as compared to the VST approach.

2.6 The physical switch port connecting the uplink from the ESX should be configured as Access port assigned to specific Virtual LAN

2.7 virtual machine network Packet is delivered to the physical switch without any tagging operation performed by the virtual switch.