DNS: It turns domain names into IP address, DNS port no: 53

Types of Records:

A: to host IPV4 addresses

PTR : reverse look up to A( host record)

MX: for the mail servers

SOA : State of Authority, it tells about how to communicate with the secondary DNS records

NS: Name server records, it acts as forwarders

CName: Alias to the host records

DHCP: Dynamically assign IP address to the organisation

It is a Dynamic host configuration protocol: it helps in configuration of all the devices and users on the IP network.

Port No: 67

HTTP: web server works on http protocol, port no:80 or 880

SSL: It is a secure socket layer, it works on 443 port

TCP is a connection-oriented protocol, get the acknowledgment

IP/UDP is a connection less protocol, no acknowledgement.

OSI 7 layers of communication,

Timeline

Description automatically generated with medium confidence

Works:

HTTP: SSL port

Server Hardware support( power, network, storage connectivity, hardware drivers, Bios drivers, Bios updates) and OS support ( patch updations, OS hardening(stopping of unnecessary services,) software installations, )

Cyber security

1. apply group policies and passwords
2. restrict user access on resources using permissions
3. Regular OS patching
4. Enable Auditing

Azure

Security Center : continuously scanning azure services for any loop holes

Azure AD:

NSG

Network ACL

Update manger

Install the software in the server with vendors

Increase the hardware based on the performance and load.

Incidents:

2 types of tickets in Service Now

1.Alerts : Server down, Hardware issues( disk issues, memory issues) and service (windows services) Ex: windows time service. Network interface issues(packet loss)

Performance issues: Task manager: which process is taking more CPU and memory. How long is taking ? Is it genuine load or not? Check the event viewer, contact the server owner with your findings and with his permission we can kill the process.

2. Service requests / breakages /outages.

Service request Ex: Add memory to VM

Install application on VM

Create a VM

Breakages: Web server down, In breakages & outages based on the severity & priority command center team will open bridge call and access the impact and bring back the services as soon as possible.

VMWare:

VMware Vcenter : To manage ESX servers, ESX clusters and guest VMs

VMware ESXi /VMware ESx: VMware Esx is a bear metal operating system installed on a hard ware.

A hypervisor is a program that enables multiple operating systems to share a single hardware host.  Each [operating system](https://career.guru99.com/top-50-operating-system-interview-questions/) has the host’s processor, memory and other resources all to itself.  The hypervisor controls the resources and host processor, allocating what is required for each operating system in turn and make sure that the guest operating system cannot disrupt each other.

We can use combined hardware resources like CPU, memory, network into isolated VMs

Host machine: Esx

Guest machine: On the Esx we create windows or linux VMs

ESX is managed by portal

**Explain VMware DRS?**

VMware DRS stands for Distributed Resource Scheduler; it dynamically balances resources across various host under a cluster or resource pool.

ESXi is a small foot print of ESX , it is more secure

.vmdk – Vharddisk filename is

ESX cluster main features are Vmware HA & DRS (distributed resource scheduler – Load balance)

Challaenges faced:

Situation:

Applications owner notified us that the application performance is reduced drastically from past couple of days.

This is a Java in house application on Dell Poweredge server(on premise)

Action:

I verified the event log for recent changes.

Later I enabled Performance Monitor on inhouse application for two days.

While checking the event logs, I observed that there are few patches updated last week on this server.

Both hardware and software patches are applied last week.

I was under impression that this may be the cause of this issue.

Resolution:

Removed (uninstall ) the OS kernel patch and observed that he application performance came to normal.

Lessons learned:

Should not apply OS patches and hardware patches same time.

Do End to End thorogh test on Dev and testing environments before applying it into production.

Make sure same hardware, same OS, Same Patches configured development, test and production.

In this case development is HP hardware, production is Dell hardware.

We request monitoring team to monitor on this inhouse application to generate alerts proactively

2.

Situation:

Some users are unable to connect the file server and access the file share, where as some users are able to connect and access the file share without any issues.

Action:

I checked in the event viewer on the fileserver and on the end user machine.

Enable the network monitor on file server and on the end user machine, monitored for 6 hours

Verified with ping and tracert commands on both sides.

Noticed that some packets are not reaching to destination( file server )

Resolution:

Started a bridge call with the network team

Provided the proof of event viewer, network monitor to the Network team

Network team did research and found that they updated Network switch firmware

Inturn they engaged cisco and they fixed the issue by reverting back their changes.

Issued got resolved.

Network team told that root cause is firware update.

Lessons learned: Network team need to notify us about the changes.