Module-4: Understand Performance tuning aspects & basic Security for Infrastructure

Assignment Solution

edureka!

Version 1.0

1) What are the Sources of Network Slowness?

1. Sources of Network Slowness

- NIC duplex and speed incompatibilities
- Network congestion
- Poor routing
- Bad cabling
- Electrical interference
- An overloaded server at the remote end of the connection
- Misconfigured DNS

2) How will you Use ping to Test Network Connectivity and for troubleshooting?

One of the most common methods used to test connectivity across multiple networks is the ping command. Ping sends ICMP echo packets that request a corresponding ICMP echo-reply response from the device at the target address. Because most servers will respond to a ping query it becomes a very handy tool. A lack of response could be due to:

1. A server with that IP address doesn't exist
2. The server has been configured not to respond to pings
3. A firewall or router along the network path is blocking ICMP traffic
4. You have incorrect routing. Check the routes and subnet masks on both the local and remote servers and all routers in between. A classic symptom of bad routes on a server is the ability to ping servers only on your local network and nowhere else. Use traceroute to ensure you're taking the correct path.
5. Either the source or destination device having an incorrect IP address or subnet mask.

There are a variety of ICMP response codes which can help in further troubleshooting

You may get a "Destination Host Unreachable" message. The message is caused by your router or server knowing that the target IP address is part of a valid network, but is getting no response from the target server. There are a number of reasons for this:

If you are trying to ping a host on a directly connected network:

1. The client or server might be down, or disconnected for the network.
2. Your NIC might not have the correct duplex settings; you may verify this with the mii-tool command.
3. You might have the incorrect type of cable connecting your Linux box to the network. There are two basic types, straight through and crossover.
4. In the case of a wireless network, your SSID or encryption keys might be incorrect.

If you are trying to ping a host on remote network:

The network device doesn't have a route in its routing table to the destination network and sends an ICMP reply type 3 which triggers the message. The resulting message might be Destination Host Unreachable or Destination Network Unreachable.

```
[root@smallfry tmp]# ping 192.168.1.105
PING 192.168.1.105 (192.168.1.105) from 192.168.1.100 : 56(84) bytes of data.
From 192.168.1.100 icmp_seq=1 Destination Host Unreachable
From 192.168.1.100 icmp_seq=2 Destination Host Unreachable
From 192.168.1.100 icmp_seq=3 Destination Host Unreachable
From 192.168.1.100 icmp_seq=4 Destination Host Unreachable
From 192.168.1.100 icmp_seq=5 Destination Host Unreachable
From 192.168.1.100 icmp_seq=6 Destination Host Unreachable
--- 192.168.1.105 ping statistics ---
8 packets transmitted, 0 received, +6 errors, 100% loss, time 7021ms, pipe 3
[root@smallfry tmp]#
```

3) How will you Use Using telnet to Test Network Connectivity and for troubleshooting?

An easy way to tell if a remote server is listening on a specific TCP port is to use the telnet command. By default, telnet will try to connect on TCP port 23, but you can specify other TCP ports by typing them in after the target IP address. HTTP uses TCP port 80, HTTPS uses port 443.

Here is an example of testing server 192.168.1.102 on the TCP port 22 reserved for SSH:

```
[root@bigboy tmp]# telnet 192.168.1.102 22
```

When using telnet troubleshooting, here are some useful guidelines to follow that will help to isolate the source of the problem:

- Test connectivity from the remote PC or server.
- Test connectivity on the server itself. Try making the connection to the loopback address as well as the NIC IP address. If the server is running a firewall package such as the Linux iptables software, all loopback connectivity is allowed, but connectivity to desired TCP ports on the NIC interface might be blocked sometimes. Further discussion of the Linux iptables package is covered in a later section.
- Test connectivity from another server on the same network as the target server. This helps to eliminate the influence of any firewalls protecting the entire network from outside.

Connection Refused Messages

You will get a connection refused message for one of the following reasons:

- The application you are trying to test hasn't been started on the remote server.
- There is a firewall blocking and rejecting the connection attempt

Here is some sample output:

```
[root@bigboy tmp]# telnet 192.168.1.100 22
Trying 192.168.1.100...
telnet: connect to address 192.168.1.100: Connection refused
[root@bigboy tmp]#
```

telnet Timeout or Hanging

The telnet command will abort the attempted connection after waiting a predetermined time for a response. This is called a timeout. In some cases, telnet won't abort, but will just wait indefinitely. This is also known as hanging. These symptoms can be caused by the one of the following reasons:

- The remote server doesn't exist on the destination network. It could be turned off.
- A firewall could be blocking and not rejecting the connection attempt, causing it to timeout instead of being quickly refused.

```
[root@bigboy tmp]# telnet 216.10.100.12 22
Trying 216.10.100.12...
telnet: connect to address 216.10.100.12: Connection timed out
[root@bigboy tmp]#
```

4) Which popular packages for viewing the flow of packets through your Linux box's NIC card?

The tcpdump command is one of the most popular packages for viewing the flow of packets through your Linux box's NIC card. It is installed by default on RedHat/Fedora Linux and has very simple syntax, especially if you are doing simpler types of troubleshooting.

One of the most common uses of tcpdump is to determine whether you are getting basic two-way communication. Lack of communication could be due to the following:

- Bad routing
- Faulty cables, interfaces of devices in the packet flow
- The server not listening on the port because the software isn't installed or started
- A network device in the packet path is blocking traffic; common culprits are firewalls, routers with access control lists and even your Linux box running iptables.

Useful tcpdump Expressions

tcpdump command expression	Description
host host-address	View packets from the IP address host-address
icmp	View icmp packets
tcp port port-number	View TCP packets with packets with either a source or destination TCP port of port-number
udp port port-number	View UDP packets with either a source or destination UDP port of port-number

5) Advantages of firewall?

1. Features: just try to find a pre-built firewall with Socks support, a good caching proxy server, support for both 1 to many and 1 to 1 NAT at the same time, support for multiple parallel upstream paths, and multiple internal networks, and several different mutually incompatible virtual private networks.

2. Fine grain control and monitoring: netfilter gives you much more control than most packet filtering packages do (e.g. rules depending on the time of day, how busy the machine is, how much traffic there is of a specific kind, who owns a process generating traffic, etc.)

3. When (not if) security holes are discovered you can deal with them by patching software. You don't have to disconnect your network and cross your fingers hoping that Company X will decide to produce an updated firmware for your particular two-years-out-of-date firewall in the near future (if you don't think this is a problem, talk to somebody with a two year old SNMP managed switch. I've got a nice big rack-mount 10/100 switch made by HP that is essentially a several thousand dollar paperweight. I have found no indication from the manufacturer that they've even started working on an update to correct the SNMP security flaws which they've known about for well over a year at this point).

4. Speed. Most off the shelf firewall boxes are designed for use with consumer grade cable and DSL connections. The ones I've tried all tend to max out at between 2 and 6 mbps for traffic actually going through the packet filter. Higher end firewalls can handle more traffic, but they are MUCH more expensive (I'm used to seeing them for around $5000us and up) and tend to be neither quick to install nor low-maintenance.

5. Trust. Security through obscurity is a concept that has repeatedly been shown not to work. Closed source products provide manufacturers with opportunity to routinely gloss over serious design flaws, ignore security holes (until they hit the popular media) and include undocumented back doors that customers aren't aware of until it's too late. In contrast Linux allows you control over all the source code that goes into making your firewall, you can see exactly what it does, and you can check for yourself that it doesn't include serious known exploits or back doors. This is what free software is all about.

6) What should be the approach for Troubleshooting something isn't getting through our firewall

If something isn't getting through our firewall you have to find out if the firewall is stopping it or you have some other configuration issue. The fact that logging to the console of dropped packets is enabled by the script you can tell right away if the firewall is stopping the traffic. Packet information will be displayed on the screen. This indicates that rules aren't correct for what you're trying to accomplish because the firewall is dropping the packets you want to go through.

If traffic isn't getting through but you're not getting any packet information displayed on the screen, it's likely something with the configuration of the system behind the firewall. No packet information was being displayed on the screen (i.e. the firewall wasn't dropping anything).

When the Web server gets a request from a browser on the Internet, it will try and respond to the address that was given as the source address in the request. This source address will be that of the system that's trying to browse to your server over the Internet. This address won't be on the DMZ network, and without a valid gateway address specified in the/etc/network/interfaces file, the Web server won't know how to get to the non-local system.