

Module 2: Essential Troubleshooting Tools

This module covers some essential tools for network diagnostics, log analysis, debugging, and external web services.

Command-Line Tools

Command-line tools are indispensable for quick and precise troubleshooting of network and server issues. Below are key tools and their applications:

1. ping

- **Purpose:** Tests the connectivity between the local machine and a remote server.
- **Usage:** `ping example.com`
- **Output:** Round-trip time, packet loss, and network latency.

```
dann@home1ab:~$ ping woza.co.ke
PING woza.co.ke (23.162.56.108) 56(84) bytes of data.
64 bytes from mtl101c.truehost.cloud (23.162.56.108): icmp_seq=1 ttl=49 time=721 ms
64 bytes from mtl101c.truehost.cloud (23.162.56.108): icmp_seq=2 ttl=49 time=516 ms
64 bytes from mtl101c.truehost.cloud (23.162.56.108): icmp_seq=3 ttl=49 time=435 ms
64 bytes from mtl101c.truehost.cloud (23.162.56.108): icmp_seq=4 ttl=49 time=411 ms
64 bytes from mtl101c.truehost.cloud (23.162.56.108): icmp_seq=5 ttl=49 time=342 ms
64 bytes from mtl101c.truehost.cloud (23.162.56.108): icmp_seq=6 ttl=49 time=503 ms
^C
--- woza.co.ke ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5130ms
rtt min/avg/max/mdev = 342.005/487.919/720.734/119.133 ms
```

2. traceroute (Linux) / tracert (Windows)

- **Purpose:** Traces the path packets take to reach a destination server.
- **Usage:** `traceroute example.com` or `tracert example.com`

- **Output:** Hop-by-hop details to identify network bottlenecks or failures.

```
dann@homeLab:~$ traceroute woza.co.ke
traceroute to woza.co.ke (23.162.56.108), 64 hops max
 1  192.168.1.1  3.167ms  1.363ms  1.352ms
 2  100.64.0.1  283.910ms  202.873ms  208.803ms
 3  172.16.251.46  205.068ms  200.454ms  204.918ms
 4  206.224.65.208  516.142ms  488.185ms  533.494ms
 5  206.224.65.178  204.130ms  203.117ms  205.104ms
 6  62.115.37.20  208.964ms  200.807ms  204.178ms
 7  * * *
 8  130.117.1.1  206.979ms  154.639ms  256.727ms
 9  64.125.29.59  308.436ms  306.598ms  245.996ms
10  * 64.125.28.37  334.417ms *
11  154.54.44.162  273.357ms  307.315ms  306.283ms
12  154.54.45.42  308.048ms  306.484ms  235.752ms
13  * * *
14  * * *
```

3. **dig** (Domain Information Groper)

- **Purpose:** Queries DNS records to troubleshoot domain-related issues.
- **Usage:** **dig example.com A**
- **Output:** Returns DNS record details such as IP address, TTL, and authoritative nameservers.

```

dann@home1ab:~$ dig woza.co.ke A
; <<> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<> woza.co.ke A
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 14416
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags; udp: 65494
;; QUESTION SECTION:
;woza.co.ke.                IN      A

;; ANSWER SECTION:
woza.co.ke.                6696   IN      A      23.162.56.108

;; Query time: 1 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Dec 18 10:02:00 EAT 2024
;; MSG SIZE rcvd: 55

```

4. netstat

- **Purpose:** Displays active network connections and port usage.
- **Usage:** **netstat -tuln**
- **Useful for checking if certain ports are open, e.g port 25.**
- **Output:** Lists listening ports, protocols, and established connections.

```

[root@srv ~]# netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp    0      0 0.0.0.0:25              0.0.0.0:*               LISTEN
tcp    0      0 0.0.0.0:8090            0.0.0.0:*               LISTEN
tcp    0      0 0.0.0.0:443             0.0.0.0:*               LISTEN
tcp    0      0 127.0.0.1:██████████    0.0.0.0:*               LISTEN
tcp    0      0 0.0.0.0:993             0.0.0.0:*               LISTEN
tcp    0      0 0.0.0.0:995             0.0.0.0:*               LISTEN

```

5. nslookup

- **Purpose:** Resolves domain names to IP addresses and queries DNS records.
- **Usage:** **nslookup example.com**

- **Output:** Provides details about DNS resolution and authoritative servers.

```
dann@homelab:~$ nslookup woza.co.ke
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
Name:   woza.co.ke
Address: 23.162.56.108

dann@homelab:~$ █
```

6. whois

- **Purpose:** Retrieves domain registration information.
- **Usage:** **whois example.com**
- **Output:** Displays registrar details, domain status, and expiration date.

```
dann@homelab:~$ whois woza.co.ke
Domain Name: woza.co.ke
Registry Domain ID: 649148-KENIC
Registrar URL:
Updated Date: 2024-10-10T14:57:38Z
Creation Date: 2018-02-16T18:47:15Z
Registry Expiry Date: 2025-02-16T18:47:15Z
Registrar Registration Expiration Date: 2025-02-16T18:47:15Z
Domain Status: active https://icann.org/epp#active
Registrar: Truehost Cloud Limited
Registrar IANA ID: P051332644V
```

Log Analysis Tools

Log files provide critical insights into server behavior, errors, and performance. These tools help extract and analyze relevant information:

1. grep

- **Purpose:** Searches for specific patterns within log files.
- **Usage:** **grep "error" /var/log/apache2/error.log**

- **Output:** Lists all lines containing the keyword "error."

```
dann@home1ab:~$ grep "error" /var/log/apache2/error.log
dann@home1ab:~$ █
```

2. awk

- **Purpose:** Processes and extracts data from log files.
- **Usage:** **awk '{print \$1, \$4}' /var/log/apache2/access.log**
- **Output:** Extracts the first and fourth columns, such as IP addresses and timestamps.

```
dann@home1ab:~$ awk '{print $1, $4}' /var/log/apache2/access.log
::1 [18/Dec/2024:10:09:59
::1 [18/Dec/2024:10:10:00
::1 [18/Dec/2024:10:10:00
::1 [18/Dec/2024:10:10:04
::1 [18/Dec/2024:10:10:05
::1 [18/Dec/2024:10:10:05
::1 [18/Dec/2024:10:10:05
::1 [18/Dec/2024:10:10:06
dann@home1ab:~$ █
```

Debugging Tools

Advanced debugging tools are useful for isolating and analyzing system or application-level issues:

1. strace

- **Purpose:** Traces system calls made by a process.
- **Usage:** **strace -p <process_id>**
- **Output:** Detailed system call information for debugging applications.

```
[root@srv ~]# strace -p 861681
strace: Process 861681 attached
select(6, [3 4 5], NULL, NULL, {tv_sec=16, tv_usec=370828}
) = 0 (Timeout)
rt_sigprocmask(SIG_SETMASK, ~[ILL TRAP ABRT BUS FPE SEGV CONT SYS RTMIN RT_1], NULL, 8) = 0
openat(AT_FDCWD, "postmaster.pid", O_RDWR) = 10
read(10, "861681\n/var/lib/pgsql/data\n17314"... , 8191) = 102
close(10) = 0
getpid() = 861681
rt_sigprocmask(SIG_SETMASK, [], NULL, 8) = 0
select(6, [3 4 5], NULL, NULL, {tv_sec=60, tv_usec=0}) = ? ERESTARTNOHAND (To be restarted if no handle
r)
--- SIGUSR1 {si_signo=SIGUSR1, si_code=SI_USER, si_pid=861688, si_uid=26} ---
stat("logrotate", 0x7ffc1e640cb0) = -1 ENOENT (No such file or directory)
getpid() = 861681
getpid() = 861681
clone(child_stack=NULL, flags=CLONE_CHILD_CLEARTID|CLONE_CHILD_SETTID|SIGCHLD, child_tidptr=0x7f706cf70
150) = 677887
rt_sigreturn({mask=[]}) = -1 EINTR (Interrupted system call)
rt_sigprocmask(SIG_SETMASK, ~[ILL TRAP ABRT BUS FPE SEGV CONT SYS RTMIN RT_1], NULL, 8) = 0
rt_sigprocmask(SIG_SETMASK, [], NULL, 8) = 0
select(6, [3 4 5], NULL, NULL, {tv_sec=60, tv_usec=0}) = ? ERESTARTNOHAND (To be restarted if no handle
r)
```

External Web Services

Online tools complement command-line utilities by offering additional insights and verification:

1. DNSChecker.org

- **Purpose:** Verifies DNS propagation globally.
- **Usage:** Enter the domain name to check record updates across multiple locations.

The screenshot shows the DNSChecker website interface. The browser address bar displays 'dnschecker.org/#A/woza.co.ke'. The site has a blue header with the 'DNSCHECKER' logo. A navigation bar includes 'Home', 'All Tools', 'DNS Lookup', and 'Public DNS List'. The main content area is divided into two sections: 'DNS CHECK' and 'CHECK DNS PROPAGATION'. The 'DNS CHECK' section shows a search for 'woza.co.ke' with a dropdown menu set to 'A'. Below the search bar, there are controls for 'CD Flag' (checked), 'Refresh' (20 sec), and a list of DNS servers with their IP addresses and status (all green checkmarks). The 'CHECK DNS PROPAGATION' section includes a text description and a 'DNS Propagation Map by DNSChecker.org' which is partially visible as a world map.

Location	IP Address	Status
San Francisco CA, United States OpenDNS	23.162.56.108	✓
Mountain View CA, United States Google	23.162.56.108	✓
Berkeley, US Quad9	23.162.56.108	✓
Virginia, United States VeriSign Global Registry Services	23.162.56.108	✓
United States CenturyLink	23.162.56.108	✓
San Francisco, US	23.162.56.108	✓

2. DNSSEC Debugger (<https://dnssec-debugger.verisignlabs.com/>)

- **Purpose:** Analyzes and validates DNSSEC configurations.
- **Usage:** Enter the domain name to check for DNSSEC-related issues.

dnssec-debugger.verisignlabs.com/woza.co.ke

VERISIGN // LABS

Domain Name: Detail: [more\(+\)](#) / [less\(-\)](#)

Analyzing DNSSEC problems for **woza.co.ke**

.	<ul style="list-style-type: none"> Found 2 DNSKEY records for . DS=20326/SHA-256 verifies DNSKEY=20326/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=20326 and DNSKEY=20326/SEP verifies the DNSKEY RRset
ke	<ul style="list-style-type: none"> Found 1 DS records for ke in the . zone DS=17597/SHA-256 has algorithm RSASHA256 Found 1 RRSIGs over DS RRset RRSIG=81050 and DNSKEY=81050 verifies the DS RRset Found 2 DNSKEY records for ke DS=17597/SHA-256 verifies DNSKEY=17597/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=17597 and DNSKEY=17597/SEP verifies the DNSKEY RRset
woza.co.ke	<ul style="list-style-type: none"> No DS records found for woza.co.ke in the ke zone No DNSKEY records found ns2.cloudoon.com is authoritative for woza.co.ke woza.co.ke A RR has value 23.162.56.108 No RRSIGs found
woza.co.ke	<ul style="list-style-type: none"> ns1.cloudoon.com is authoritative for woza.co.ke woza.co.ke A RR has value 23.162.56.108 No RRSIGs found
woza.co.ke	<ul style="list-style-type: none"> ns3.cloudoon.com is authoritative for woza.co.ke woza.co.ke A RR has value 23.162.56.108 No RRSIGs found

3. whois.com

- **Purpose:** Provides domain registration details.
- **Usage:** Enter the domain name to view registrar and owner information.

The screenshot shows the Whois.com website interface. The browser address bar displays "whois.com/whois/woza.co.ke". The Whois logo is in the top left, with navigation links for Domains, Hosting, Servers, Email, Security, Whois, and Deals. A search box on the right contains the text "Enter Domain or IP". The main content area displays "woza.co.ke" with a refresh icon and "Updated 5 days ago". Below this, there are two sections: "Domain Information" and "Registrant Contact".

Domain Information	
Domain:	woza.co.ke
Registrar:	Truehost Cloud Limited
Registered On:	2018-02-16
Expires On:	2025-02-16
Updated On:	2024-10-10
Status:	active
Name Servers:	ns3.cloudoon.com ns2.cloudoon.com ns1.cloudoon.com

Registrant Contact	
Organization:	Cloudpap
Country:	KE

4. IntoDNS.com

- **Purpose:** Offers a comprehensive DNS health check.
- **Usage:** Enter the domain name to get insights into DNS configuration, mail servers, and potential issues.



woza.co.ke

Report

Work in progress!
Follow intoDNS on [Twitter](#)

[send feedback](#)

Category	Status	Test name	Information
Parent		Domain NS records	Nameserver records returned by the parent servers are: ns2.cloudoon.com. [49.12.105.164] (NO GLUE) [TTL=86400] ns3.cloudoon.com. [158.69.211.95] (NO GLUE) [TTL=86400] ns1.cloudoon.com. [51.79.165.162] (NO GLUE) [TTL=86400] ns.anycast.ke. or.ke was kind enough to give us that information.
		TLD Parent Check	WARNING: Looks like the parent servers do not have information for your TLD when asked. This is ok but can be confusing.
		Your nameservers are listed	Good. The parent server ns.anycast.ke. or.ke has your nameservers listed. This is a must if you want to be found as anyone that does not know your DNS servers will first ask the parent nameservers.
		DNS Parent sent Glue	The parent nameserver ns.anycast.ke. or.ke is not sending out GLUE for every nameservers listed, meaning he is sending out your nameservers host names without sending the A records of those nameservers. It's ok but you have to know that this will require an extra A lookup that can delay a little the connections to your site. This happens a lot if you have nameservers on different TLD (domain.com for example with nameserver ns.domain.org.)
		Nameservers A records	Good. Every nameserver listed has A records. This is a must if you want to be found.
NS		NS records from your nameservers	NS records got from your nameservers listed at the parent NS are: ns1.cloudoon.com [51.79.165.162] [TTL=86400] ns2.cloudoon.net [49.12.105.164] [TTL=86400]
		Recursive Queries	Good. Your nameservers (the ones reported by the parent server) do not report that they allow recursive queries for anyone.