Here are some Splunk search commands for server health checks, covering CPU, memory, disk, network, and process monitoring. These will help you proactively monitor and troubleshoot server health issues.

1. CPU Usage Monitoring

Check average CPU usage per server

```
index=your_index sourcetype=cpu_usage | stats avg(usage) as avg_cpu by host | sort - avg_cpu
```

Identify servers with high CPU usage (>80%)

```
index=your_index sourcetype=cpu_usage | stats avg(usage) as avg_cpu by host | where avg_cpu > 80
```

CPU utilization over time

```
index=your_index sourcetype=cpu_usage | timechart avg(usage) by host
```

2. Memory Usage Monitoring

Check memory usage per server

```
index=your_index sourcetype=memory_usage | stats avg(used_memory) as avg_memory by host | sort - avg_memory
```

Find servers running low on available memory (<10% free)

```
index=your_index sourcetype=memory_usage | eval free_percent=(free_memory/total_memory)*100 | where free_percent < 10
```

Memory utilization trends

```
index=your_index sourcetype=memory_usage | timechart avg(used_memory) by host
```

3. Disk Usage Monitoring

Check disk space usage across all servers

```
index=your_index sourcetype=disk_usage | stats avg(used_space) as avg_disk by host | sort - avg_disk
```

Identify servers with critical disk usage (>90%)

```
index=your_index sourcetype=disk_usage | eval disk_percent=(used_space/total_space)*100 | where disk_percent > 90
```

Disk I/O performance

```
index=your_index sourcetype=disk_io | timechart avg(reads) as read_ops, avg(writes) as write_ops by host
```

4. Network Performance Monitoring

Check network bandwidth usage

```
index=your_index sourcetype=network_usage | stats avg(bandwidth_in) as avg_in, avg(bandwidth_out) as avg_out by host
```

Find servers with high network latency (>100ms)

```
index=your_index sourcetype=network_latency | stats avg(latency) as avg_latency by host | where avg_latency > 100
```

Monitor dropped packets over time

```
index=your_index sourcetype=network_errors | timechart sum(dropped_packets) by host
```

5. Process & Service Monitoring

Find top processes consuming the most CPU

```
index=your_index sourcetype=process_usage | stats avg(cpu_usage) as avg_cpu by process_name | sort - avg_cpu
```

List critical services that are down

```
index=your_index sourcetype=service_status | search status="down" | table _time, host, service_name, status
```

Monitor service restarts in the last 24 hours

```
index=your_index sourcetype=service_status status="restarted" earliest=-24h | stats count by service_name, host
```

6. Server Uptime & Availability

Check system uptime for all servers

```
index=your_index sourcetype=system_uptime | table host, uptime
```

Identify servers that rebooted in the last 24 hours

```
index=your_index sourcetype=system_uptime earliest=-24h | search uptime < 600 | table _time, host, uptime
```

Monitor server availability over time

```
index=your_index sourcetype=server_availability | timechart count by host
```

7. Overall Server Health Score

Calculate a simple health score based on CPU, memory, and disk usage

```
index=your_index sourcetype=cpu_usage OR sourcetype=memory_usage OR sourcetype=disk_usage

| eval health_score=100-(cpu_usage*0.4)-(memory_usage*0.3)-(disk_usage*0.3)

| stats avg(health_score) as avg_health by host

| sort avg_health
```