Alert: **A notification or any abnormality that brings to your notice.**

1. **OS based**
2. **Service related**
3. **Connectivity**
4. **Resources**

Alert types:

1. Information
2. Minor Alert
3. Major Alert
4. Critical Alert

**Server related Alerts:**

**CPU aler**t: High CPU alert : Create an Incident ticket → priority (2) → **troubleshooting**

Login to that particular server → top (cpu, memory, total number of processes, which process is consuming high cpu and high memory) → kill that particular process (kill -9 PID) → service restart. → incident ticket resolution add → close incident

**Memory Alert:** High Memory alert : Create an Incident ticket → priority (2) → **troubleshooting**

Login to that particular server → top (cpu, memory, total number of processes, which process is consuming high cpu and high memory) → kill that particular process (kill -9 PID) → service restart. → incident ticket resolution add → close incident

**Disk space Alert:**

**→ high disk space alert:**

**→ login to the server: df -h (which file system is utilizing more )**

**du -sch \* | grep G (to check the which files are consuming high space)**

**gzip -v filename**

**Or**

**tar -cvzf filename.tar.gz filename**

**→ move that files to archive server**

**sftp username@ipaddress of archive server**

**put \*.gz**

**exit**

**→ Remove zipped files; rm -rf \*.gz**

**OS related: Linux related alerts → incident ticket create → Linux Team → Drop a mail to the linux Team.**

**Application or Service Related alerts:**

**Tomcat Service is down**

**Apache Service is down**

**Application/Web Server is down**

**Application is couldn't able to server the traffic**

**No connection between services**

**Troubleshooting**

**: ps -ef | grep <service name>**

**systemctl status <service name>**

**Praksh: Task A: email/ splunk**

**Vikas Task B: Vikas → stopped httpd service**

**Krishna: Task c:**

**Murthy : Task D: monitoring tool monitor: alert**

**monitoring tool monitor: alert → incident create → We intentionally stopped httpd service as requested by Engg team.**

→ slack channel

→ Teams group

**No connection between services:**

**curl -k url of the service**

**netstat -tulpn | grep LISTEN**

**→ if the above validations are fine even if we triggered alert then we will restart the services.**

**→ systemctl stop <servicename>**

**→ systemvtl start <servicename>**

**→ ps -ef | grep <process.**

**→ kill -9 PID**

**Network Related Issues:**

**No Connectivity :**

**High Inbound/Outbound :**

**Ddos Attack : Cyber attack : Arbor / CLoud flare**

**Ping Issues : Connectivity issues (JIO/TATA)**

**Ip Address Issues : IP s not configured**

**Firewall/Gateway issues :**

**→ create servicenow incident and assign this ticket to n/w team and drop an email**

**DB Related Issues:GRAFANA DASHBOARD**

**DB Server Memory Status:**

**DB Server health status: weather it is running or not**

**Long running queries :**

**Blocking sessions :**

**Replication Lag :**

**→ create servicenow incident and assign this ticket to Database team and drop an email**

**ROBOTIC ALERTS:**

**We will configure robotic probes or robotic agents in all servers to fetch the metrics of the server. By any change if any robotic probe is not working then we will get robotic probe alerts.**

**→**