What is Splunk?

An Analytical Tool (Head/Parent Tool for monitoring all other important parameters of a server).

**Some Major Parameters Monitored:**



[This Photo](https://www.finsmes.com/2020/11/splunk-to-buy-flowmill.html) by Unknown Author is licensed under [CC BY-NC-ND](https://creativecommons.org/licenses/by-nc-nd/3.0/)

C Drive TGIM SCCM CS LAPS RSA NTP Patching

Checkpoints to Troubleshoot:

* Latest Version to be installed.
  + - * 7.3 for Windows OS (Current)
      * 7.2 for Linux OS (Current)
* Make sure Ports are Open from Source to Destination IP
  + - * telnet destination\_IP port\_no
      * Dev:
        + telnet 172.17.11.61 8089 , telnet 172.17.11.61 9997
      * Prod:
        + telnet 172.17.8.179 8089 , telnet 172.17.8.197 9997,

telnet 172.17.8.198 9997

* + Configuration Files should be Inline.
    - * inputs.conf
      * deploymentclient.conf
      * server.conf

Please refer to snaps below for respective files and their content:

M

Some Points to be Noted:

* + Hostname should be the same on all 4:

1. On Server
2. In Personal Inventory owned by respective OS Teams.
3. In Centralized Inventory (At Common Path)
4. In Splunk/Master Inventory (updated on weekends).

* + Ensure server is not Powered Off/Decommissioned
    - * Check for Inventory Updation Cases
  + Any other Server – Specific / OS Related Issue:
    - * Server Not reachable due to network/hang state issue.
      * Space Issue on Server (unable to install new version)