Common Commands:

- **sar -d** (will show you the disc utilization)
- **nfsqd** (will show you over subscription on a IPS)
- **top** (will show you the running processes)
- **htop** (a more visual interface for top)
- **cat data.[number] | msgdump -H | less** (will cat the data file pump it to message dump. the -H doesn't show headers and then goes to less. -s shows stats)
- **NitroStarted** (will show you the status of Nitro on a Receiver or IPS)
- **NitroStart --nod** (will start Nitro processes on a reciever and wait till they are loaded before giving you a prompt)
- **NitroStop --nod** (will stop the Nitro processes on the receivers)
- **NitroStopped** (will show you the status of the NitroStop)
- **service httpd restart** (if you get an httpd <defunct> this will restart it)
- **service cpservice stop** (will stop the ESM processes)
- **service cpservice start** (will start the ESM processes)
- **service network restart** (will restart the network on an ESM)
- **ifconfig** (will show you the IP addresses of the device as well as other useful information)
- **cat /proc/mdstat** (will show you if the softraid is okay)
- **ssh root@[ip_address]** (connect to a box)
- **cat /etc/buildstamp** (show the current version of software box is on)
- **cat /etc/upgrade.history** (show the dates and versions they have upgraded from and to)
- **bg** (commonly used after cpservice stop then ctrl+z to show the background)
- **tcpdump -nni eth[eth#] host [IP of the datasource] and port[port_number]** (show you incoming traffic from that address on optional port)
- **md5sum [file]** (gives you the checksum of the file good to check on update files)
- **tail -f /var/log/messages** (will tail the messages file so anything new that appears will display)
- **ethtool eth[eth number]** (will allow you to set settings on specific eth)
- **chmod 775 [file]** (give correct rights to a file to run on the box)
- **less [file_name] | grep [search criteria]** (show a file and then searching for specific item)
- **date** (gives current date and time)
- **scp [file] root@[ip_address]:/[location]** (secure copies a file from your directory to specified location)
- **scp root@[ip_address]:/[location and file to copy] /[location to save]** (secure copies a file from remote location to your desktop)
- **ps auxf** (show services on box)
- **ps auxf | grep [service]** (will show if specfic service is running)
- **iptables -nvL** (show you if data is being brought in for the data sources)
- **reboot** (will reboot the box)
- **dmidecode | grep Serial** (will show you the serial of the box)
- **cli32** (opens the raid controller)
- **disk info** (gives you disk info)
- **vsf info**
- **rsf info**
- **shredthesystem** (removes all data on device)
- **dsstatus [Vips_ID]** (shows you the current status of parser,collector and filter)
- **watch -d [command]** (refreshes the command every 2 seconds)
- **df -h** (shows you the disk info)
- **du** (shows the sizes of the directories)
- **du -sh** (shows the total size of a directory)
- **du -ch** (shows all the folders in the directory and their sizes as well as a total)
- **du -h / | grep [1-9]G** (shows any files > nG in size in all directories)
- **rm .ssh/known_hosts** (this will remove the hosts in the file so you can ssh)
- **echo callhome >> /etc/rc.d/rc.local** (will add the callhome so after a reboot it stays open)
- **wget path_to_file** (if on a esm you can ssh to the correct folder run this command and it will get the update file for you)
- **cat /var/log/messages | grep -i 'Event Stats' > receiver_events.txt** (output all of the event collection statistics to a text file)
- **df_audit -d /var/log/data/inline/thirdparty.logs/[vips_id] -f** (this will fix all files in a data source that could have a bad byte count -f will do all files)
- **nsql /usr/local/ess/data/connect_esm.sql** (opens the database)
- **strace -p [process_id]** (trace the process to see what other processes it's tied to)

- **ifconfig eth0 mtu 1300** (sets the MTU setting to 1300 until the box is restarted to set it permanently add command to rc.local)
- **find / -iname [search criteria]** (searches every directory for the criteria mentioned)
- **enable_bypass** (turn bypass on, in an IPS)
- **disable_bypass** (turn bypass off, in an IPS)
- **reset_bypass** (reboots the box and resets the nic)
- **install_bypass** (power off the box and allows you replace the nic and then once booted back up it will do the restart_bypass)
- **nsql /usr/local/ess/data/connect_esm.sql** (connect to the database)
- **NitroTID** (command to pull information about partitions and so forth, advanced)
- **DBCheck** (checks the status of all the tables if they are corrupt or not, advanced commands used)
- **killall -1 syslogcollector** (restarts syslogcollector and sync's the thirdparty.conf settings)
- **ls | wc -l** (give you the total count of data sources in thirdparty.logs)
- **ls -R / | grep -i -e data.* -e wmi.* | wc -l** (will give you a total count if you are in the thirdparty.logs directory of total wmi and data files)
- **ls -R / | wc -l** (will give you a total count of files in that directory you are in)
- **find . \(-name "data.*" -o -name "wmi.*" \) -print | wc -l** (only files no directories)
- **who** (shows who is currently logged in)
- **w** (shows what people who are logged in are doing)
- **last** (shows history of logins and reboots)
- **AlertsGetTrimMinutes** (shows the compression settings of events)
- **AlertsSetTrimMinutes 0 0 0 0** (turns compression off, advanced)
- **ConnectionsGetTrimMinutes** (shows the compression settings of flows)
- **ConnectionsSetTrimMinutes 0 0 0 0** (turns compression off, advanced)
- **ha_status** (shows ha status)
- **crm status** (shows status of IPMI)
- **killall -HUP collectorsctl** (tells collectorsctl to restart any stopped collector)
- **history** (shows the commands run on the box)
- **find /var/log/data/inline/thirdparty.logs/* -name '*' -daystart -mtime +2 -exec rm -v {} \;** (finds all the files in thirdparty.logs older than 2 days and deletes them)

Directories/files:

- **/var/log/data/inline/thirdparty.logs/** (this is the location of all the data sources data files)
- **/var/log/messages** (this file hosts most of the logs that go on in the box)
- **/etc/NitroGuard/thirdparty.conf** (this is where all the data sources are written to)
- **/usr/local/ess/data/NitroError.log** (database errors)
- **/usr/local/ess/data/** (this file contains database rebuild files and various database files also the connect.sql on an ESM)
- **/var/log/data/inline/** (this contains the connect.sql for all other devices)
- **/usr/local/ess/update/** (location where to put upgrade **file** on ESM to reboot and upgrade)
- **/usr/local/NitroGuard/** (location where to put the upgrade file on all other devices to reboot and upgrade)
- **/usr/local/ess/SoftwareUpdates/** (location NitroView saves all upgrade files to push to other devices and ESM)
- **/usr/local/ess/CPConsoleServer.cfg** (ESM Net Settings)
- **/etc/NitroGuard/globals.conf** (ELM/REC Net Settings)
- **/etc/rc.d/init.d/nitromode** (other devices Net Settings)
- **/etc/rc.d/rc.local** (file to modify to add permanent callhome into)
- **/usr/lib/** (Lib .so files to replace if needed)
- **/etc/NitroGuard/vipsdef** (stores the vips information)
- **/var/log/data/inline/ecs/upload** (correlation files are stored here)

Advanced Commands:

-
  ```
  DBCheck -d '/usr/local/ess/data/ngcp.dfl' -u 'LOCDB327|CPDB126' -c
  ```