Splunk Enterprise Deployment Guide with Best Practices and Some Useful Configurations

Prepared By: Faisal Rafiq Khan
Track Lead – SecOps & Threat Management
https://splunk.com

splunk> enterprise

Verify that **wget** is installed for **Linux v9**

```
[root@localhost faisal]# yum install wget
Updating Subscription Management repositories.
Last metadata expiration check: 2:42:10 ago on Wed 17 Jul 2024 03:41:52 PM PKT.
Package wget-1.21.1-7.el9.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@localhost faisal]#
```

Not to install Splunk using **root** add user for your choice

```
[root@localhost faisal]# adduser splunk
[root@localhost faisal]#
```

New **user** added and verified

```
[root@localhost faisal]# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin
systemd-coredump:x:999:997:systemd Core Dumper:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:998:996:User for polkitd:/:/sbin/nologin
sssd:x:997:995:User for sssd:/:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
pipewire:x:996:993:PipeWire System Daemon:/run/pipewire:/usr/sbin/nologin
libstoragemgmt:x:991:991:daemon account for libstoragemgmt:/:/usr/sbin/nologin
tss:x:59:59:Account used for TPM access:/:/sbin/nologin
geoclue:x:990:989:User for geoclue:/var/lib/geoclue:/sbin/nologin
cockpit-ws:x:989:988:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:988:987:User for cockpit-ws instances:/nonexisting:/sbin/nologin
flatpak:x:987:986:User for flatpak system helper:/:/sbin/nologin
colord:x:986:985:User for colord:/var/lib/colord:/sbin/nologin
setroubleshoot:x:985:984:SELinux troubleshoot server:/var/lib/setroubleshoot:/usr/sbin/nologin
clevis:x:984:983:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/usr/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
gnome-initial-setup:x:983:982::/run/gnome-initial-setup/:/sbin/nologin
chrony:x:982:981:chrony system user:/var/lib/chrony:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/usr/sbin/nologin
dnsmasq:x:981:980:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
faisal:x:1000:1000:Faisal:/home/faisal:/bin/bash
vboxadd:x:980:1::/var/run/vboxadd:/bin/false
splunk:x:1001:1001::/home/splunk:/bin/bash
[root@localhost faisal]#
```

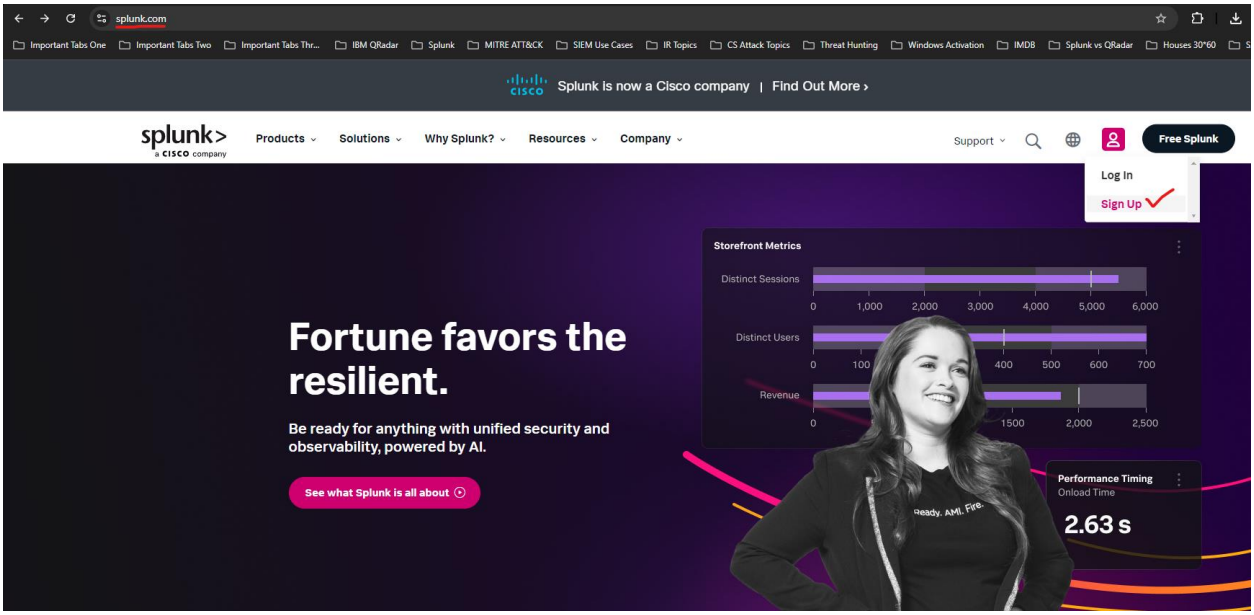
Set **password** for new user

```
[root@localhost faisal]# passwd splunk
Changing password for user splunk.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost faisal]#
```

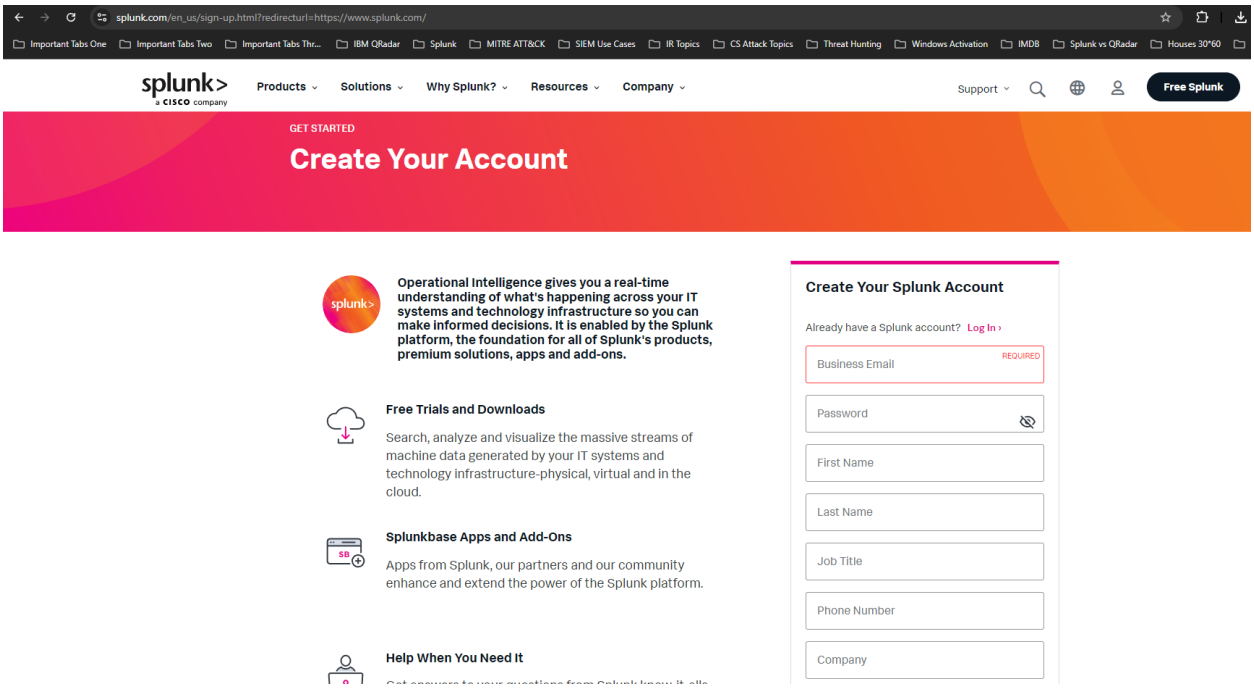
Installation **directory > /opt/**

```
[root@localhost faisal]# cd /opt
[root@localhost opt]#
[root@localhost opt]#
[root@localhost opt]#
```

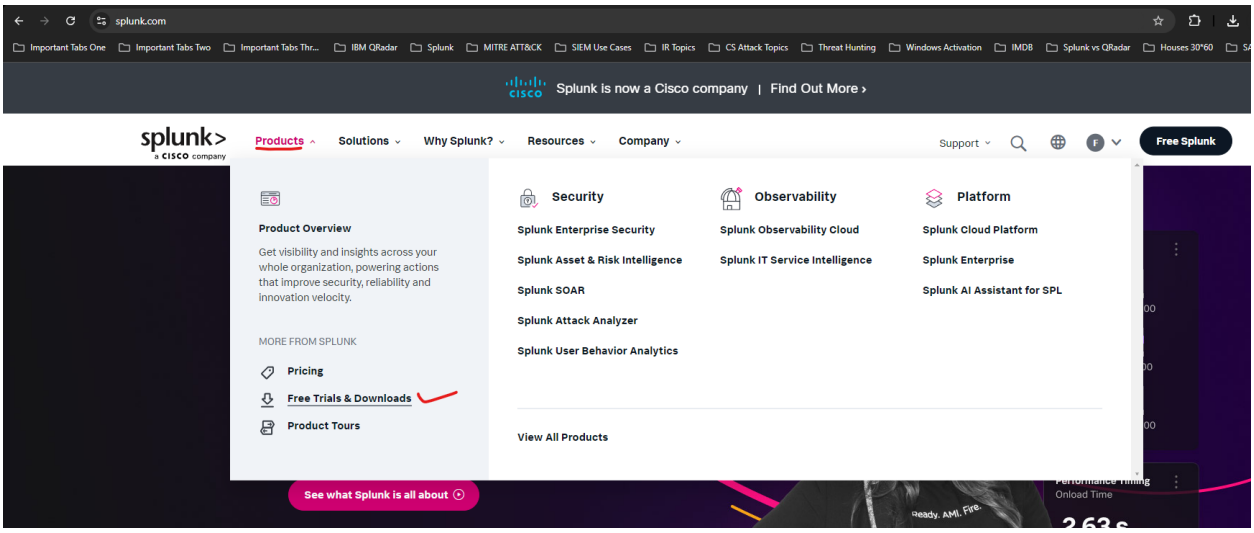
URL: **splunk.com** (Sign up for new account or Log in)



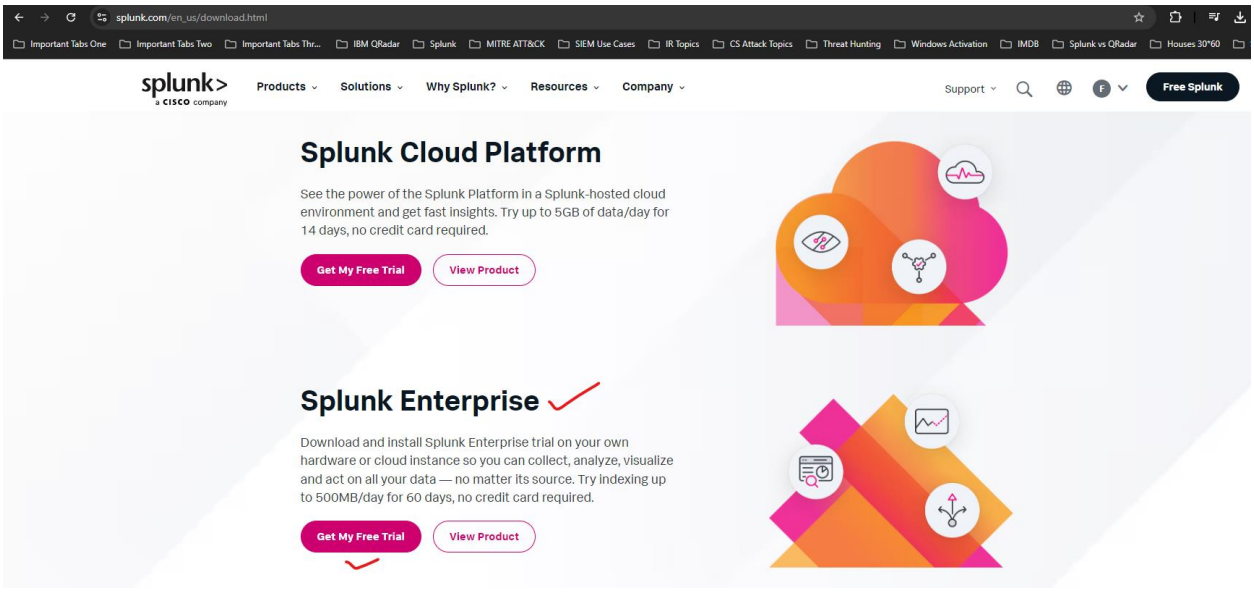
Create a **new** account for **Splunk**



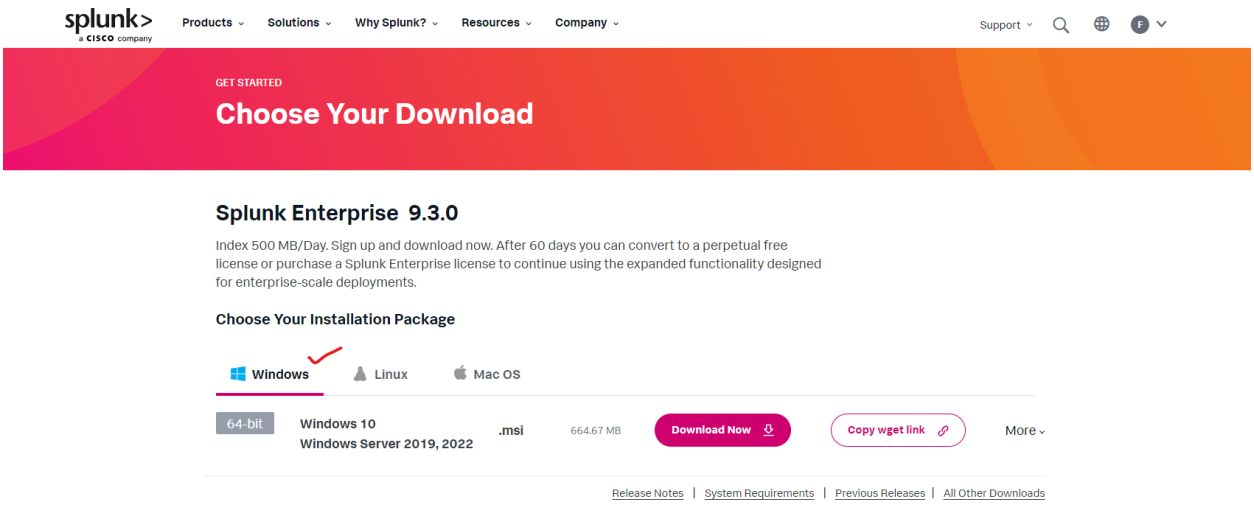
After log in click on **Production** > Free Trials & Downloads



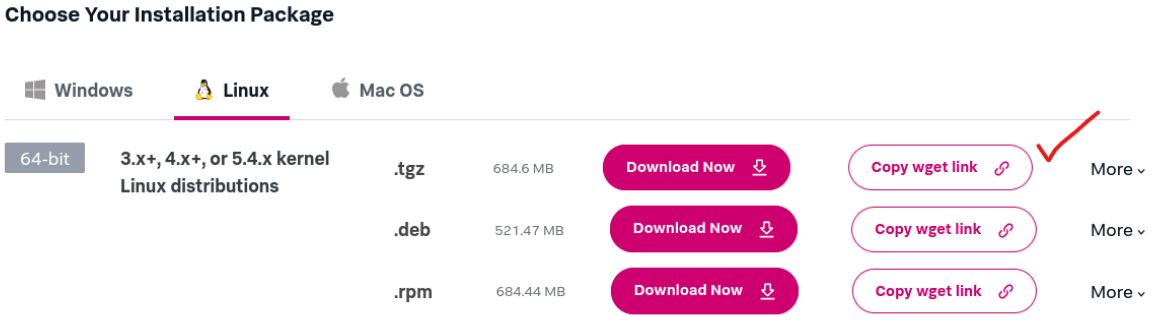
Install **Splunk Enterprise**



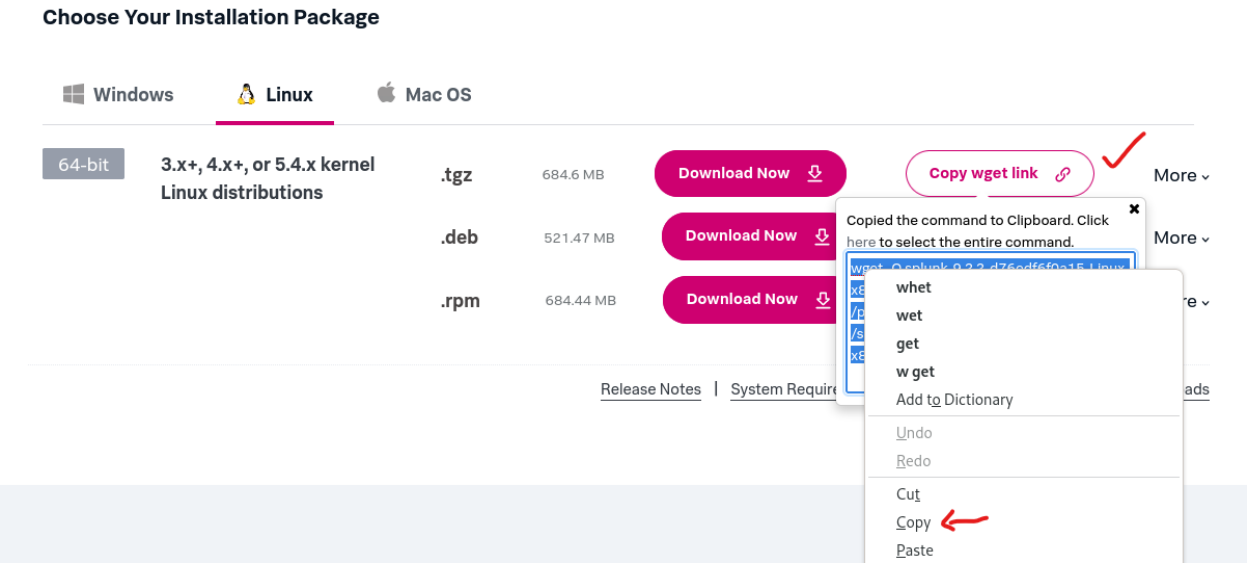
Click on **Widows** if you want to install Splunk on Windows platform



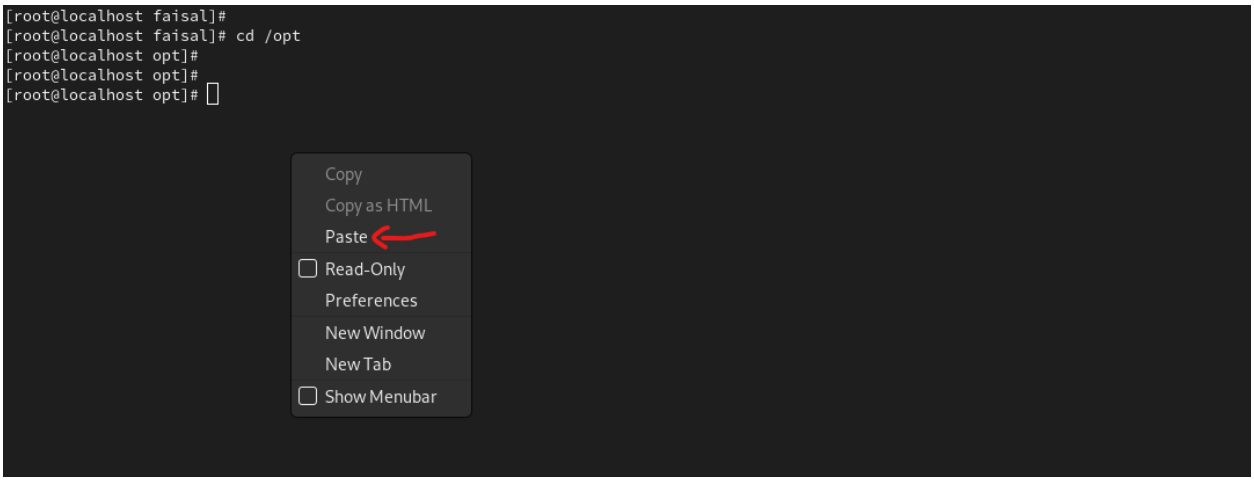
Click on **Linux** if you want to install Splunk on Linux platform
In my case I've installed Splunk on Linux 64bit with **tgz**



Copy **wget** link



Installation directory should be **/opt/** and paste the copied wget link



The **wget** link has been pasted and click enter to proceed…

The **download** process has been initiated

```
[root@localhost opt]# wget -O splunk-9.2.2-d76edf6f0a15-Linux-x86_64.tgz "https://download.splunk.com/products/splunk/releases/9.2.2/linux/splunk-9.2.2-d76edf
6f0a15-Linux-x86_64.tgz"
--2024-07-17 18:38:45--  https://download.splunk.com/products/splunk/releases/9.2.2/linux/splunk-9.2.2-d76edf6f0a15-Linux-x86_64.tgz
Resolving download.splunk.com (download.splunk.com)... 18.64.141.113, 18.64.141.92, 18.64.141.42, ...
Connecting to download.splunk.com (download.splunk.com)|18.64.141.113|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 717851455 (685M) [binary/octet-stream]
Saving to: 'splunk-9.2.2-d76edf6f0a15-Linux-x86_64.tgz'

splunk-9.2.2-d76edf6f0a15-Linux-x86_64.  20%[==============>                                                    ] 137.85M  5.77MB/s    eta 99s
```

The **Splunk** setup is **downloaded**

```
splunk-9.2.2-d76edf6f0a15-Linux-x86_64. 100%[=================================================================================>] 684.60M  5.82MB/s    in 2m 7s

2024-07-17 18:40:52 (5.41 MB/s) - 'splunk-9.2.2-d76edf6f0a15-Linux-x86_64.tgz' saved [717851455/717851455]

[root@localhost opt]# ls -lh
total 685M
-rw-r--r--. 1 root root 685M Jun 26 14:35 splunk-9.2.2-d76edf6f0a15-Linux-x86_64.tgz
drwxr-xr-x. 8 root root  136 Jul 17 15:03 VBoxGuestAdditions-7.0.14
[root@localhost opt]#
```

The **ownership** will be changed from root to splunk user (**as created before**)

```
[root@localhost opt]# ls -lh
total 685M
-rw-r--r--. 1 root root 685M Jun 26 14:35 splunk-9.2.2-d76edf6f0a15-Linux-x86_64.tgz
drwxr-xr-x. 8 root root  136 Jul 17 15:03 VBoxGuestAdditions-7.0.14
[root@localhost opt]#
```

The **ownership** is changed to splunk user

```
[root@localhost opt]# chown splunk:splunk splunk-9.2.2-d76edf6f0a15-Linux-x86_64.tgz
[root@localhost opt]# ls -lh
total 685M
-rw-r--r--. 1 splunk splunk 685M Jun 26 14:35 splunk-9.2.2-d76edf6f0a15-Linux-x86_64.tgz
drwxr-xr-x. 8 root   root    136 Jul 17 15:03 VBoxGuestAdditions-7.0.14
[root@localhost opt]#
```

Now, **switch user** as splunk

```
[root@localhost opt]#
[root@localhost opt]# su splunk
[splunk@localhost opt]$
```

Give **sudo privilege** to splunk user (**For Ubunto users > usermod -aG sudo username**)

```
[root@localhost opt]#
[root@localhost opt]#
[root@localhost opt]# usermod -aG wheel splunk
[root@localhost opt]#
```

Uncompressed the Splunk setup (The **-xzvf** flags tell the tar command to extract files from an archive)

```
[splunk@localhost opt]$
[splunk@localhost opt]$ sudo tar -xzvf splunk-9.2.2-d76edf6f0a15-Linux-x86_64.tgz
```

Untar process has been started

```
splunk/lib/python3.7/site-packages/splunk/clilib/log_handlers.py
splunk/lib/python3.7/site-packages/splunk/clilib/migration_helpers/
splunk/lib/python3.7/site-packages/splunk/clilib/migration_helpers/field_actions.py
splunk/lib/python3.7/site-packages/splunk/clilib/migration_helpers/__init__.py
splunk/lib/python3.7/site-packages/splunk/clilib/migration_helpers/app_maps.py
splunk/lib/python3.7/site-packages/splunk/clilib/cli.py
splunk/lib/python3.7/site-packages/splunk/clilib/__init__.py
splunk/lib/python3.7/site-packages/splunk/clilib/train.py
splunk/lib/python3.7/site-packages/splunk/clilib/index.py
splunk/lib/python3.7/site-packages/splunk/clilib/bundle.py
splunk/lib/python3.7/site-packages/splunk/clilib/i18n.py
splunk/lib/python3.7/site-packages/splunk/clilib/cli_common.py
splunk/lib/python3.7/site-packages/splunk/clilib/test_bundle_paths.py
splunk/lib/python3.7/site-packages/splunk/clilib/migration.py
splunk/lib/python3.7/site-packages/splunk/clilib/deploy.py
splunk/lib/python3.7/site-packages/splunk/clilib/apps.py
splunk/lib/python3.7/site-packages/splunk/clilib/test_clilib.py
splunk/lib/python3.7/site-packages/splunk/clilib/_internal.py
splunk/lib/python3.7/site-packages/splunk/clilib/info_gather.py
splunk/lib/python3.7/site-packages/splunk/clilib/validate.py
splunk/lib/python3.7/site-packages/splunk/clilib/exports.py
splunk/lib/python3.7/site-packages/splunk/search/
splunk/lib/python3.7/site-packages/splunk/search/Transformer.py
splunk/lib/python3.7/site-packages/splunk/search/searchUtils.py
splunk/lib/python3.7/site-packages/splunk/search/__init__.py
splunk/lib/python3.7/site-packages/splunk/search/TransformerUtil.py
splunk/lib/python3.7/site-packages/splunk/search/Parser.py
splunk/lib/python3.7/site-packages/splunk/testing.py
splunk/lib/python3.7/site-packages/splunk/admin.py
splunk/lib/python3.7/site-packages/splunk/auth.py
splunk/lib/python3.7/site-packages/splunk/scripting/
splunk/lib/python3.7/site-packages/splunk/scripting/update_scripts/
splunk/lib/python3.7/site-packages/splunk/scripting/update_scripts/test_edit_version.py
splunk/lib/python3.7/site-packages/splunk/scripting/update_scripts/edit_version.py
splunk/lib/python3.7/site-packages/splunk/scripting/update_scripts/edit_dashboard_version.py
splunk/lib/python3.7/site-packages/splunk/scripting/__init__.py
splunk/lib/python3.7/site-packages/splunk/WebFeatures.py
splunk/lib/python3.7/site-packages/splunk/version.py
```

All done

```
splunk/etc/system/default/props.conf
splunk/etc/system/default/datamodels.conf
splunk/etc/system/default/livetail.conf
splunk/etc/system/default/distsearch.conf
splunk/etc/system/default/transforms.conf
splunk/etc/system/default/global-banner.conf
splunk/etc/system/default/health.conf
splunk/etc/system/default/serverclass.conf
splunk/etc/system/default/workflow_actions.conf
splunk/etc/system/default/metric_rollups.conf
splunk/etc/system/local/
splunk/etc/system/local/README
splunk/etc/disabled-apps/
splunk/etc/disabled-apps/README
splunk/etc/deployment-apps/
splunk/etc/deployment-apps/README
splunk/etc/manager-apps/
splunk/etc/manager-apps/_cluster/
splunk/etc/manager-apps/_cluster/default/
splunk/etc/manager-apps/_cluster/default/indexes.conf
splunk/etc/manager-apps/_cluster/local/
splunk/etc/manager-apps/_cluster/local/README
[splunk@localhost opt]$
```

Now, the splunk directory is available to start the Splunk first time…

```
[splunk@localhost opt]$ ls -lah
total 685M
drwxr-xr-x.  4 root   root    103 Jul 17 19:07 .
dr-xr-xr-x. 18 root   root    235 Jul 17 14:45 ..
drwxr-xr-x. 12 splunk splunk 4.0K Jun 13 06:18 splunk
-rw-r--r--.  1 splunk splunk 685M Jun 26 14:35 splunk-9.2.2-d76edf6f0a15-Linux-x86_64.tgz
drwxr-xr-x.  8 root   root    136 Jul 17 15:03 VBoxGuestAdditions-7.0.14
[splunk@localhost opt]$
```

Would change file owner to splunk user for all directories in /opt/splunk
"**Recursive**" implies that the operation will be performed for all files and directories (**and all files and directories within any directory**)

```
[root@localhost splunk]#
[root@localhost splunk]#
[root@localhost splunk]# chown -R splunk:splunk /opt/splunk
[root@localhost splunk]# cd /
```

Now, time to start the Splunk for the first time…

```
[splunk@localhost opt]$
[splunk@localhost opt]$
[splunk@localhost opt]$ sudo ./splunk/bin/splunk start
```

License agreement press “q” for quit

```
SPLUNK GENERAL TERMS

Last Updated: August 12, 2021

These Splunk General Terms ("General Terms") between Splunk Inc., a Delaware
corporation, with its principal place of business at 270 Brannan Street, San
Francisco, California 94107, U.S.A ("Splunk" or "we" or "us" or "our") and you
("Customer" or "you" or "your") apply to the purchase of licenses and
subscriptions for Splunk's Offerings. By clicking on the appropriate button,
or by downloading, installing, accessing or using the Offerings, you agree to
these General Terms. If you are entering into these General Terms on behalf of
Customer, you represent that you have the authority to bind Customer. If you
do not agree to these General Terms, or if you are not authorized to accept
the General Terms on behalf of the Customer, do not download, install, access,
or use any of the Offerings.

See the General Terms Definitions Exhibit attached for definitions of
capitalized terms not defined herein.

1. License Rights
(A) General Rights. You have the nonexclusive, worldwide, nontransferable and
nonsublicensable right, subject to payment of applicable Fees and compliance
with the terms of these General Terms, to use your Purchased Offerings for
your Internal Business Purposes during the Term and up to the Capacity
purchased.

(B) Copies for On-Premises Products. You have the right to make a reasonable
number of copies of On-Premises Products for archival and back-up purposes.

(C) Splunk Extensions. You may use Splunk Extensions solely in connection with
the applicable Purchased Offering subject to the same terms and conditions for
that Offering (including with respect to Term) and payment of any Fees
associated with the Splunk Extensions. Some Splunk Extensions may be made
available under license terms that provide broader rights than the license
rights you have to the applicable underlying Offering (e.g., if the Extension
is Open Source Software). These broader rights will apply to that Splunk
Extension. Splunk Extensions may be installed on Hosted Services pursuant to
our instructions.

(D) Trials, Evaluations, Beta and Free Licenses.
(i) Trials and Evaluations. Offerings provided for trials and evaluations are
2% viewed, press Space for next page or Enter for next line...
```

Type “y” for agree the license agreement

```
"Fees" means the fees that are applicable to the C&I Services, as identified
in the Statement of Work.

"Intellectual Property Rights" means all worldwide intellectual property
rights, including copyrights and other rights in works of authorship; rights
in trademarks, trade names, and other designations of source or origin; rights
in trade secrets and confidential information; and patents and patent
applications.

"Personnel" means any employee, consultant, contractor, or subcontractor of
Splunk.

"Splunk Preexisting IP" means, with respect to any C&I Services Materials, all
associated Splunk technology and all Intellectual Property Rights created or
acquired: (a) prior to the date of the Statement of Work that includes such
C&I Services Materials, or (b) after the date of such Statement of Work but
independently of the C&I Services provided under such Statement of Work.

"Statement of Work" means the statements of work and/or any and all applicable
Orders, that describe the specific services to be performed by Splunk,
including any materials and deliverables to be delivered by Splunk.

Do you agree with this license? [y/n]:
Do you agree with this license? [y/n]: y
```

Type **user** name as created for Splunk installation and the **password**

```
Do you agree with this license? [y/n]:
Do you agree with this license? [y/n]: y

This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username: splunk
Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
```

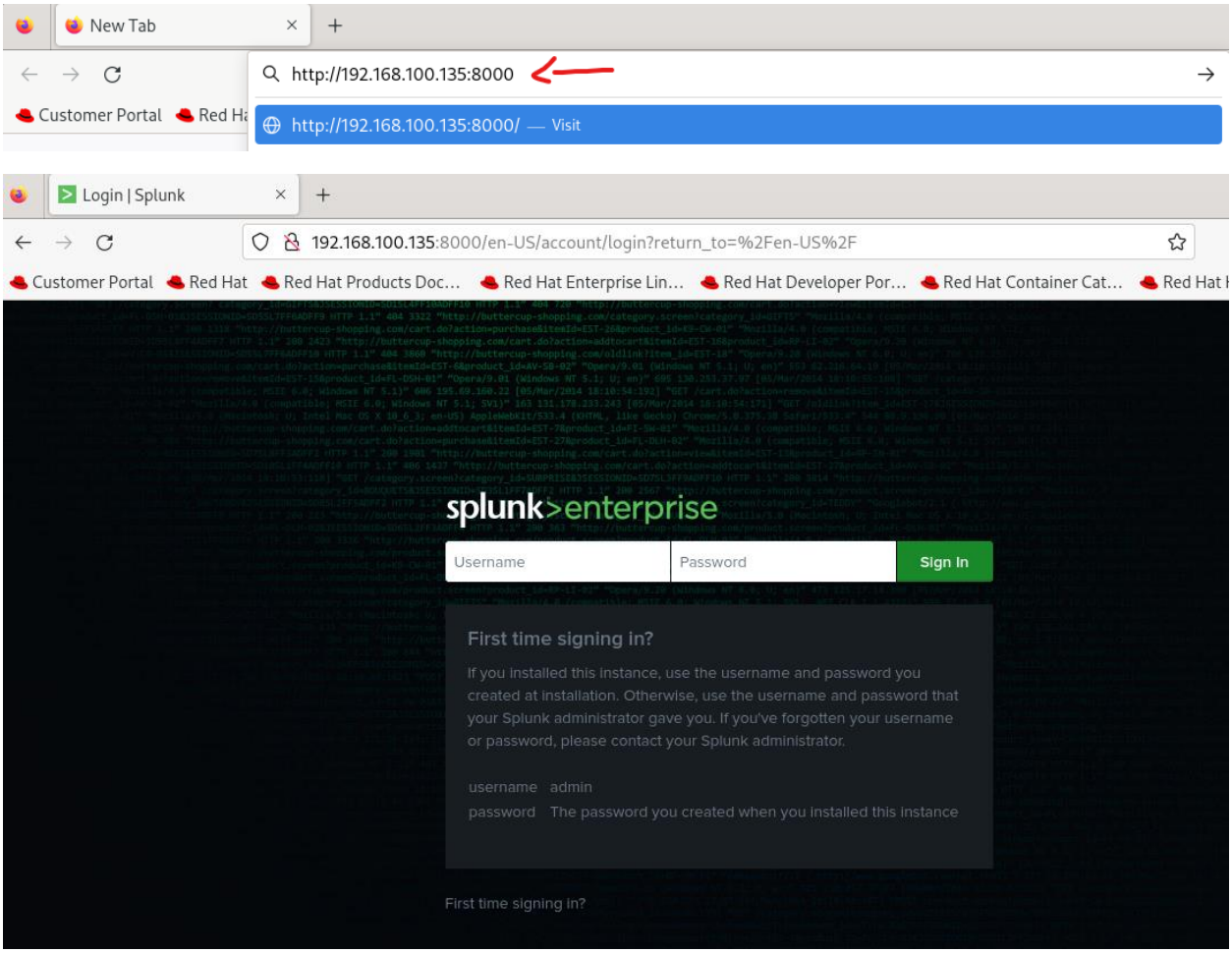
Service of Splunk **web UI** is in progress…

```
               Creating: /opt/splunk/var/spool/splunk
               Creating: /opt/splunk/var/spool/dirmoncache
               Creating: /opt/splunk/var/lib/splunk/authDb
               Creating: /opt/splunk/var/lib/splunk/hashDb
New certs have been generated in '/opt/splunk/etc/auth'.
        Checking critical directories...        Done
        Checking indexes...
               Validated: _audit _configtracker _dsappevent _dsclient _dsphonehome _internal _introspection _metrics _metrics_rollup _telemetry _thefishbucke
t history main summary
        Done
        Checking filesystem compatibility...  Done
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/opt/splunk/splunk-9.2.2-d76edf6f0a15-linux-2.6-x86_64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Generating a RSA private key
..............+++++
.....................................................+++++
writing new private key to 'privKeySecure.pem'
-----
Signature ok
subject=/CN=localhost.localdomain/O=SplunkUser
Getting CA Private Key
writing RSA key
PYTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for the httplib and urllib libraries shipped with the embedded Python int
erpreter; must be set to "1" for increased security
Done


Waiting for web server at http://127.0.0.1:8000 to be available.....................
```

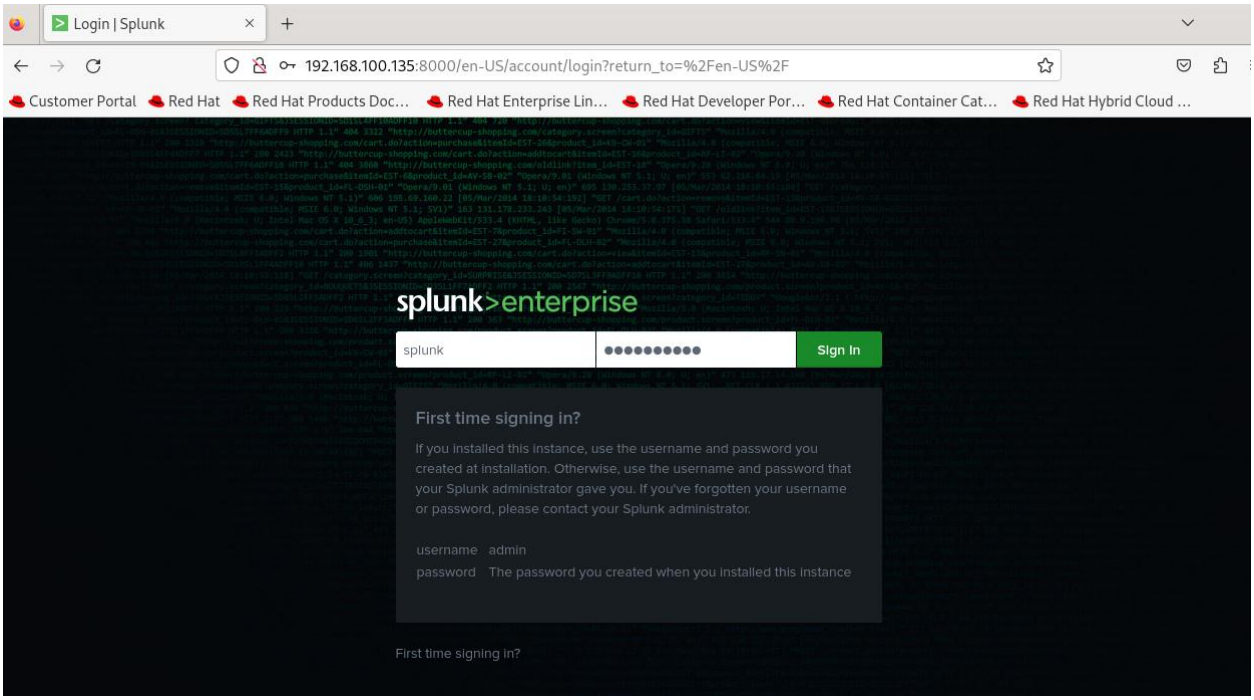
Now, the Splunk **web UI** available for access

```
.....................................................+++++
writing new private key to 'privKeySecure.pem'
-----
Signature ok
subject=/CN=localhost.localdomain/O=SplunkUser
Getting CA Private Key
writing RSA key
PYTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for the httplib and urllib libraries s
erpreter; must be set to "1" for increased security
Done


Waiting for web server at http://127.0.0.1:8000 to be available..............................  Done


If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://127.0.0.1:8000

[splunk@localhost opt]$
```

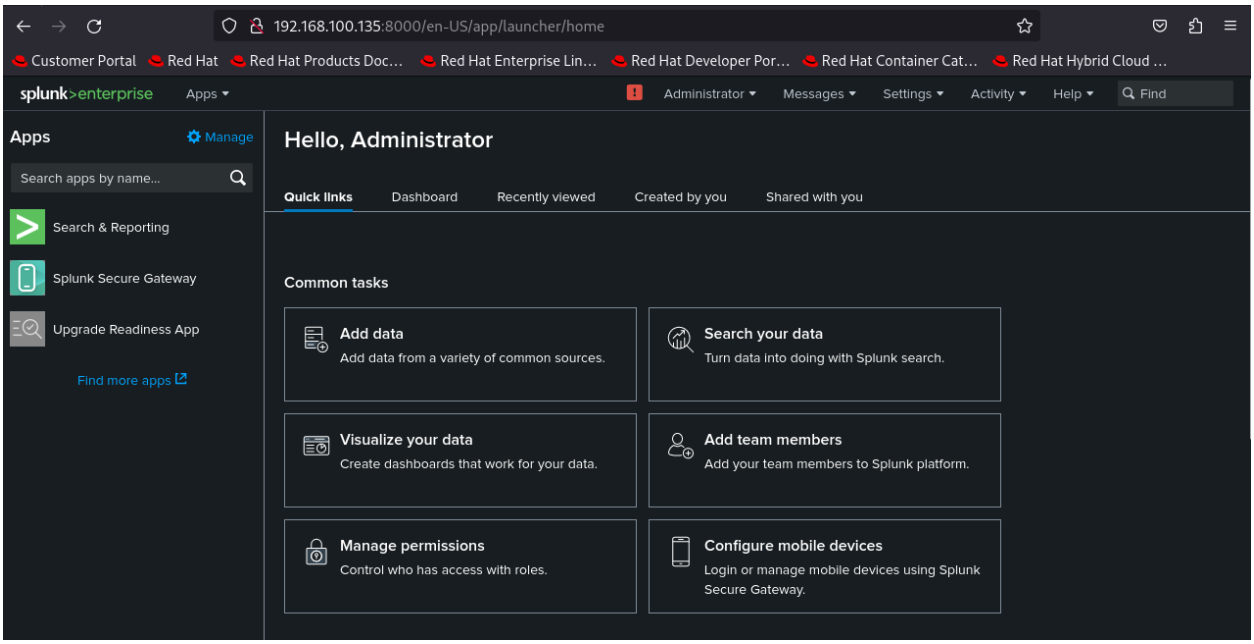
Type IP address and port 8000 to access the web UI



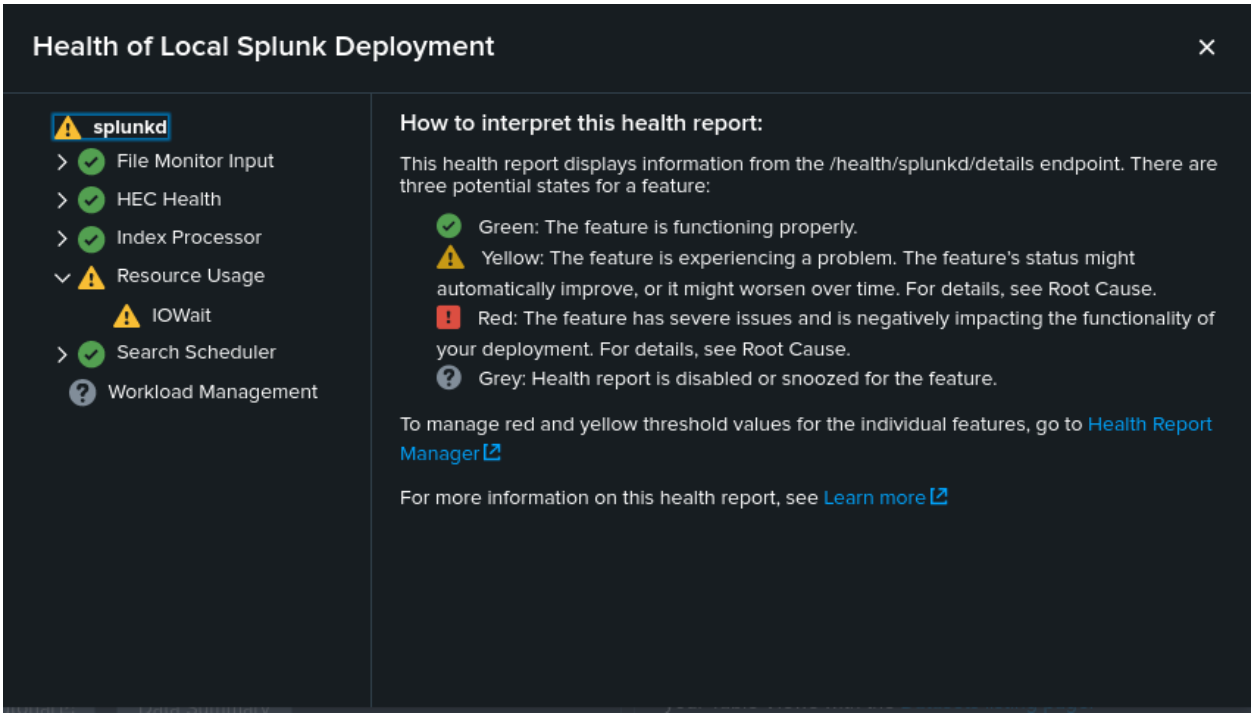
User: splunk and the password



Default screen of Splunk web UI



Ignore if you see the **IOWait** warning or error



Try some useful **Splunk commands**

Check the **status** of Splunk daemon

```
[splunk@localhost ~]$
[splunk@localhost ~]$ sudo /opt/splunk/bin/splunk status
splunkd is running (PID: 3472).
splunk helpers are running (PIDs: 3473 4179 4184 4373 4455 5364 9446 11774 11775).
[splunk@localhost ~]$
```

How to **stop** of Splunk service

```
[splunk@localhost ~]$
[splunk@localhost ~]$
[splunk@localhost ~]$ sudo /opt/splunk/bin/splunk stop
```

How to **restart** of Splunk service

```
[splunk@localhost ~]$
[splunk@localhost ~]$
[splunk@localhost ~]$ sudo /opt/splunk/bin/splunk restart
```

How to **start** of Splunk service

```
[splunk@localhost ~]$
[splunk@localhost ~]$
[splunk@localhost ~]$ sudo /opt/splunk/bin/splunk start
```

Help command give you an idea about all the different commands that you can use

```
[splunk@localhost ~]$
[splunk@localhost ~]$ sudo /opt/splunk/bin/splunk help
[sudo] password for splunk:
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.



Welcome to Splunk's Command Line Interface (CLI).

    Type these commands for more help:

        help [command]              type a command name to access its help page
        help [object]               type an object name to access its help page
        help [topic]                type a topic keyword to get help on a topic
        help commands               display a full list of CLI commands
        help clustering             commands that can be used to configure the clustering setup
        help shclustering           commands that can be used to configure the Search Head Cluster setup
        help control, controls      tools to start, stop, manage Splunk processes
        help datastore              manage Splunk's local filesystem use
        help distributed            manage distributed configurations such as
                                    data cloning, routing, and distributed search
        help forwarding             manage deployments
        help input, inputs          manage data inputs
        help licensing              manage licenses for your Splunk server
        help settings               manage settings for your Splunk server
        help simple, cheatsheet     display a list of common commands with syntax
        help tools                  tools to help your Splunk server
        help search                 help with Splunk searches

    Universal Parameters:

        The following parameters are usable by any command. For more details on each parameter, type "help [parameter]".

Syntax:

        [command] [object] [-parameter <value> | <value>]... [-uri][-auth]

      app         specify the app or namespace to run the command; for search, defaults to
                  the Search app

      auth        specify login credentials to execute commands that require you to be logged in
```

Help commands give you an overview about all the administration commands that you can uses

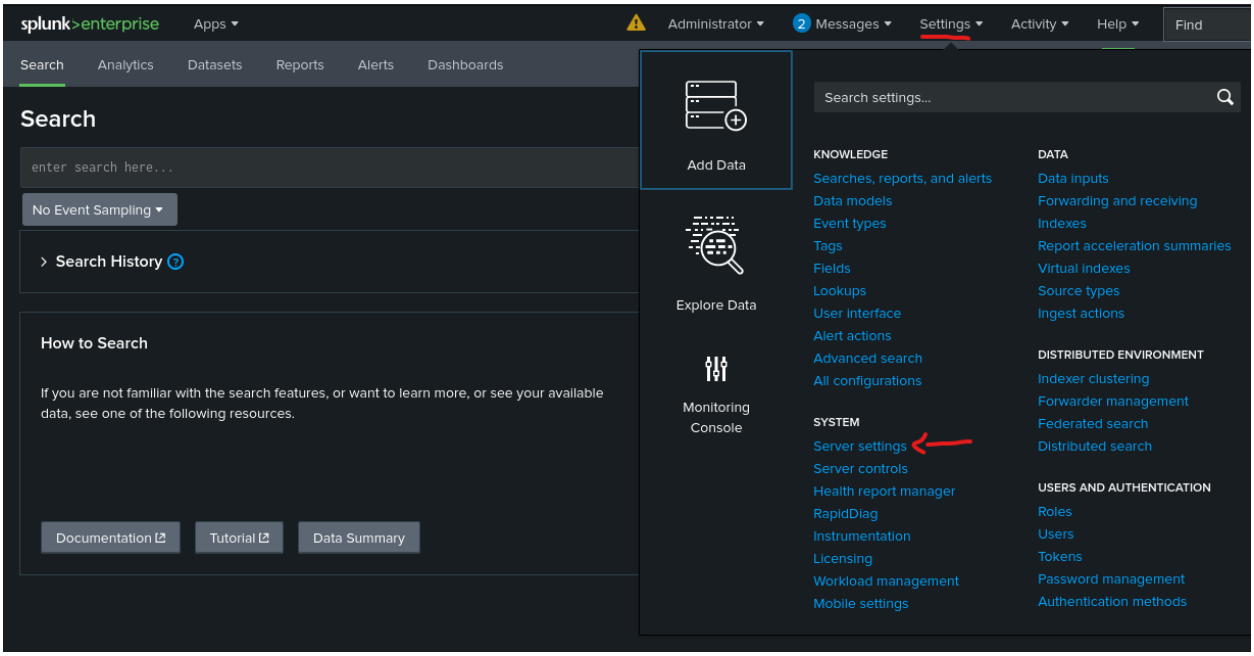
```
[splunk@localhost ~]$
[splunk@localhost ~]$ sudo /opt/splunk/bin/splunk help commands
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.



This page shows you the syntax and summary of the Splunk CLI commands. A command is an action
that you can perform on an object. Some commands don't require an object or parameters. Some
commands have a default parameter that can be specified by its value alone.

Syntax:

        ./splunk [command] [object] [-parameter <value>]...


Supported commands and objects:

        [command]           [objects]

        add                 [exec|forward-server|index|licenser-pools|licenses|manager|monitor|oneshot|
                            saved-search|search-server|tcp|udp|user]

        anonymize           source

        apply               cluster-bundle

        clean               [all|eventdata|globaldata|inputdata|userdata|kvstore|raft]

        cmd                 [btool|exporttool|importtool|locktest|locktool|parsetest|pcregextest|signtool|walklex]

        create              app

        createssl           NONE

        diag                NONE

        disable             [app|boot-start|deploy-client|deploy-server|
                            dist-search|index|kvstore-maintenance-mode|listen|local-index|maintenance-mode|shcluster-maintenance-mode|webserver|web-ssl]

        display             [app|boot-start|deploy-client|deploy-server|
                            dist-search|index|jobs|listen|local-index]
```

Also, you can use the following **link** for more >
https://docs.splunk.com/Documentation/Splunk/9.2.2/Admin/CLIadmincommands

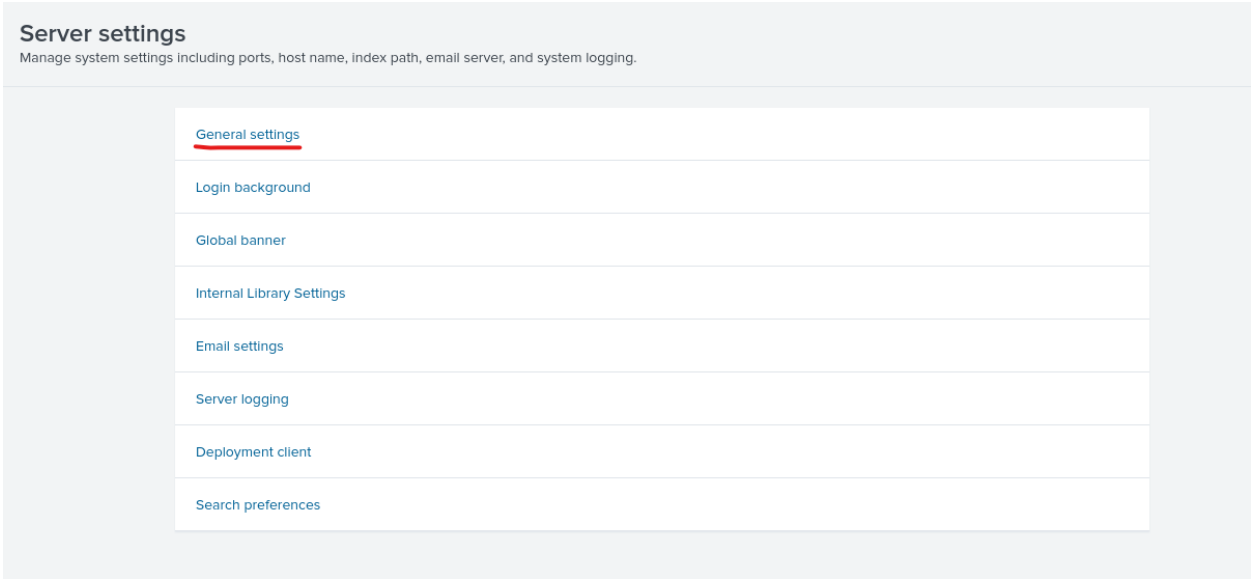
Administrative **CLI Commands**
https://docs.splunk.com/Documentation/Splunk/9.0.3/Admin/AbouttheCLI

Run Splunk Enterprise as a **systemd service**
https://docs.splunk.com/Documentation/Splunk/9.0.4/Admin/ConfigureSplunktostartatboottime

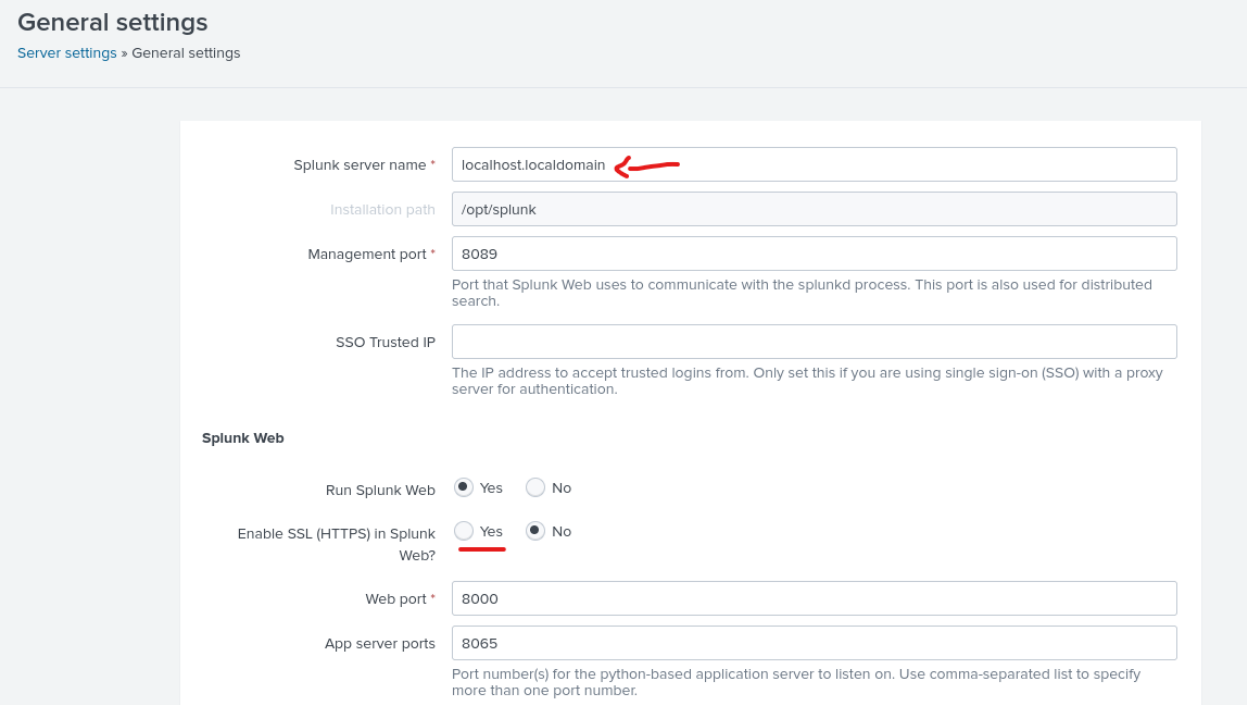
Let's do some basic changes on **Splunk UI**
Click on **Settings** and select **Server settings**



Click on **General settings**

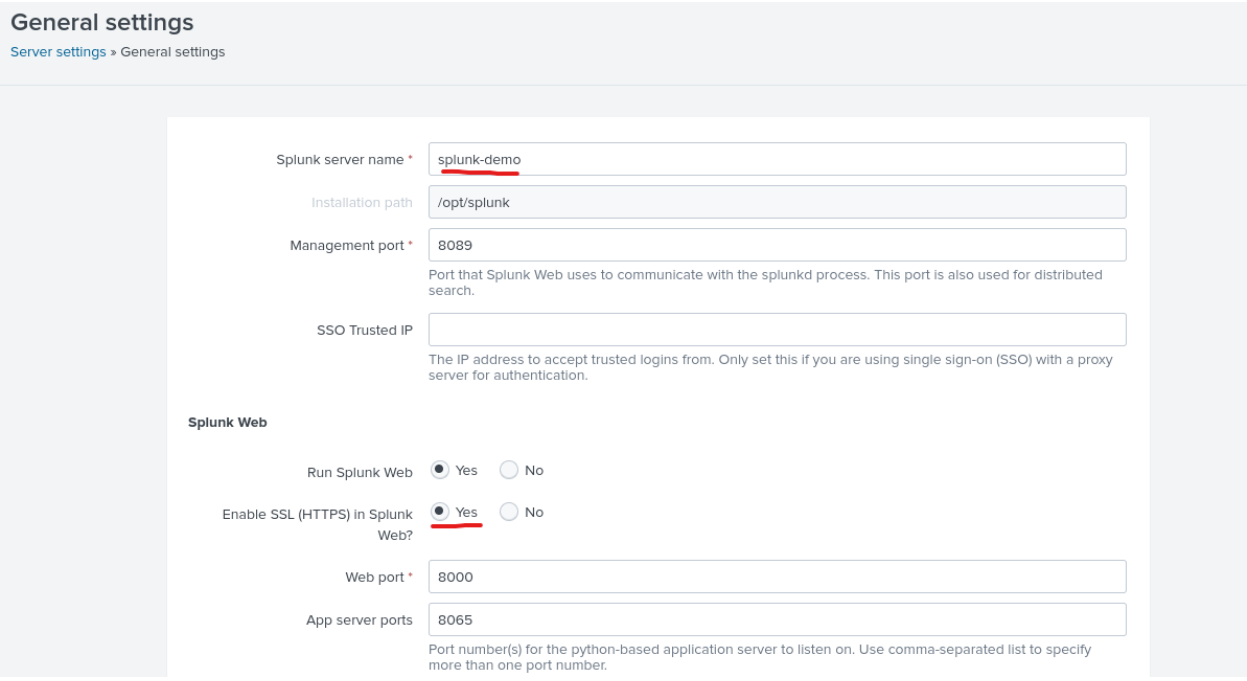


As you can see the **default setting**



Highlighted changes have been done from default

- Splunk server name
- Enabled HTTPS
- Save the changes



Web port * 8000

App server ports 8065

Port number(s) for the python-based application server to listen on. Use comma-separated list to specify more than one port number.

Session timeout * 1h

Set the Splunk Web session timeout. Use the same notation as relative time modifiers, for example 3h, 100s, 6d.

Index settings

Default host name splunk-demo

Sets the host field value for all events coming from this server.

Path to indexes /opt/splunk/var/lib/splunk

Pause indexing if free disk space (in MB) falls below * 5000

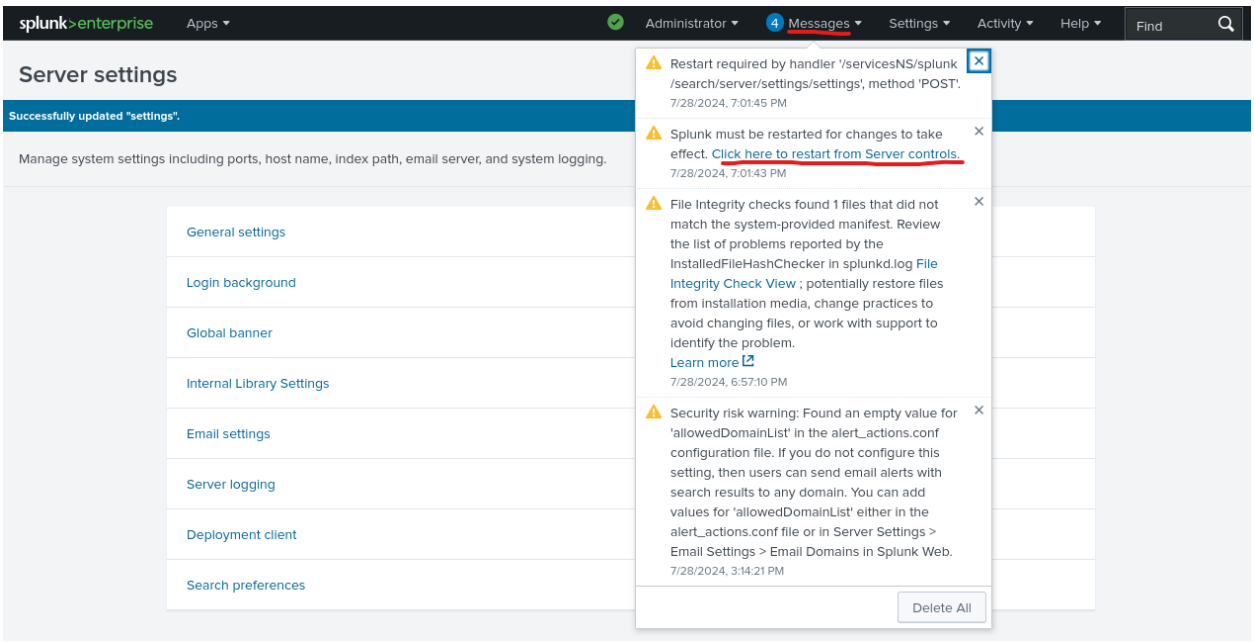
KV Store

Port * 8191

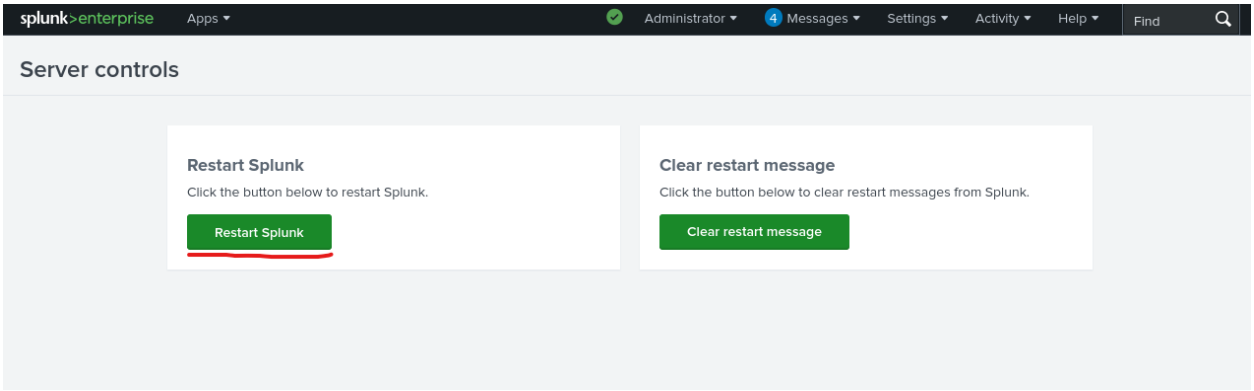
Port that splunkd uses to connect to the KV Store server.

Cancel Save

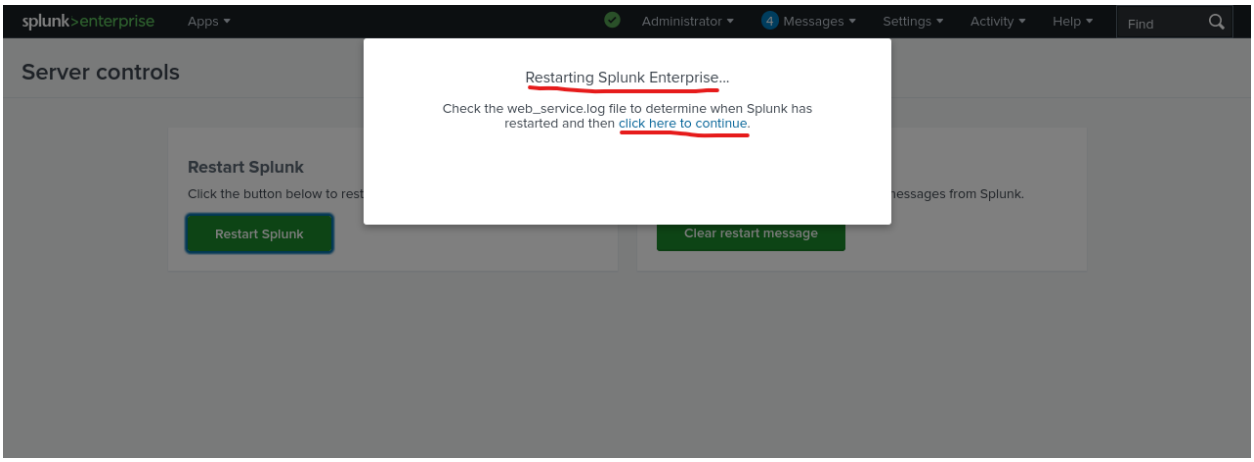
Click on **Messages** as highlighted in red and restart the **Splunk service**



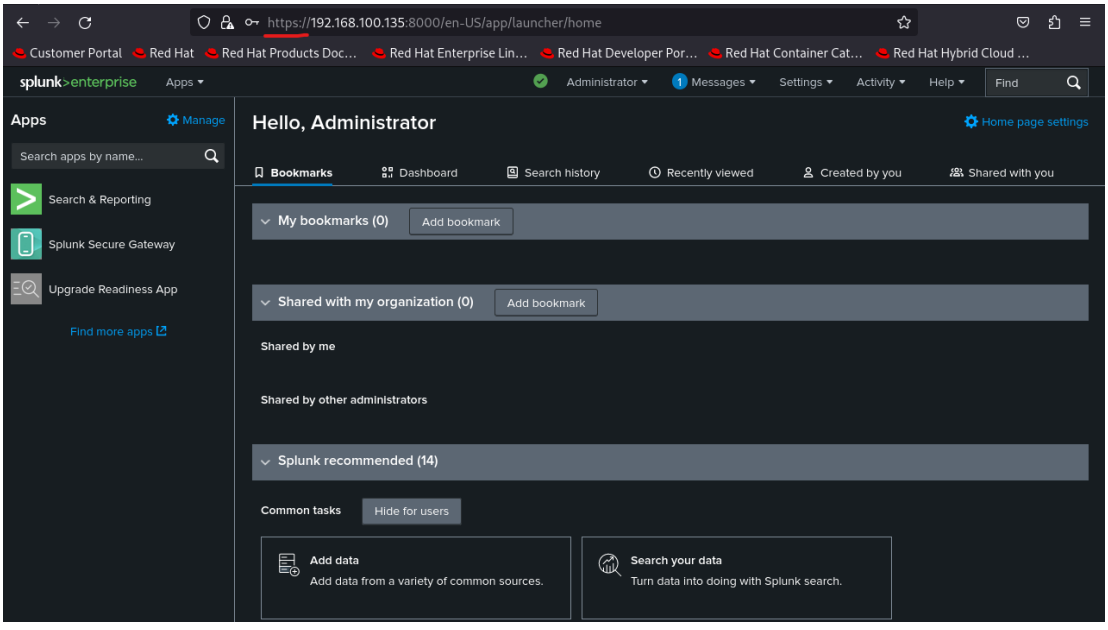
Now **Restart Splunk**



Restarting **Splunk service** is in progress… And select click here to continue



HTTPS protocol is now enabled



Splunk Health Check – Post Installation

Linux Server Recommendations

- Increase Ulimit Settings / Turn off THP

Note: Disabling THP will help improve Splunk performance and recommended to be disabled.

Check the status of THP

As per the snippet below showing {always} that means the THP is enabled

```
[root@localhost splunk]#
[root@localhost splunk]#
[root@localhost splunk]# cat /sys/kernel/mm/transparent_hugepage/enabled
[always] madvise never
[root@localhost splunk]#
```

Using the defrag to see the THP status

As per the snippet below showing {madvise} that means the THP is enabled

```
[root@localhost splunk]# cat /sys/kernel/mm/transparent_hugepage/defrag
always defer defer+madvise [madvise] never
[root@localhost splunk]#
```

Disable the THP temporarily by using the following command echo never

Note: The following changes will not be persistent when you reboot the device, so we need a short script to set them as persistent.

```
[root@localhost splunk]# cat /sys/kernel/mm/transparent_hugepage/defrag
always defer defer+madvise [madvise] never
[root@localhost splunk]# echo never > /sys/kernel/mm/transparent_hugepage/defrag
[root@localhost splunk]#
[root@localhost splunk]# cat /sys/kernel/mm/transparent_hugepage/defrag
always defer defer+madvise madvise [never]
[root@localhost splunk]#
```

splunk@localhost:/

```
[root@localhost /]#
[root@localhost /]#
[root@localhost /]# echo never > /sys/kernel/mm/transparent_hugepage/enabled
[root@localhost /]# echo never > /sys/kernel/mm/transparent_hugepage/defrag
[root@localhost /]# cat /sys/kernel/mm/transparent_hugepage/defrag
always defer defer+madvise madvise [never]
[root@localhost /]# cat /sys/kernel/mm/transparent_hugepage/enabled
always madvise [never]
[root@localhost /]#
```

To make these changes persistent across reboots to add this to the bottom of my **/etc/rc.local**

Note: There are multiple ways to disabled THP on Splunk

https://community.splunk.com/t5/Monitoring-Splunk/How-do-I-disable-Transparent-Huge-Pages-THP-and-confirm-that-it/m-p/124490

https://community.splunk.com/t5/Monitoring-Splunk/How-do-I-disable-Transparent-Huge-Pages-THP-and-confirm-that-it/m-p/124491

```
[root@localhost /]#
[root@localhost /]#
[root@localhost /]# cd /etc/rc.d/
[root@localhost rc.d]# ls -lah
total 16K
drwxr-xr-x.   3 root root   36 Jun 12 18:11 .
drwxr-xr-x. 132 root root 8.0K Aug  4  2024 ..
drwxr-xr-x.   2 root root   20 Aug  2 21:39 init.d
-rw-r--r--.   1 root root  474 Jun 12 18:11 rc.local
[root@localhost rc.d]# vi rc.local
```

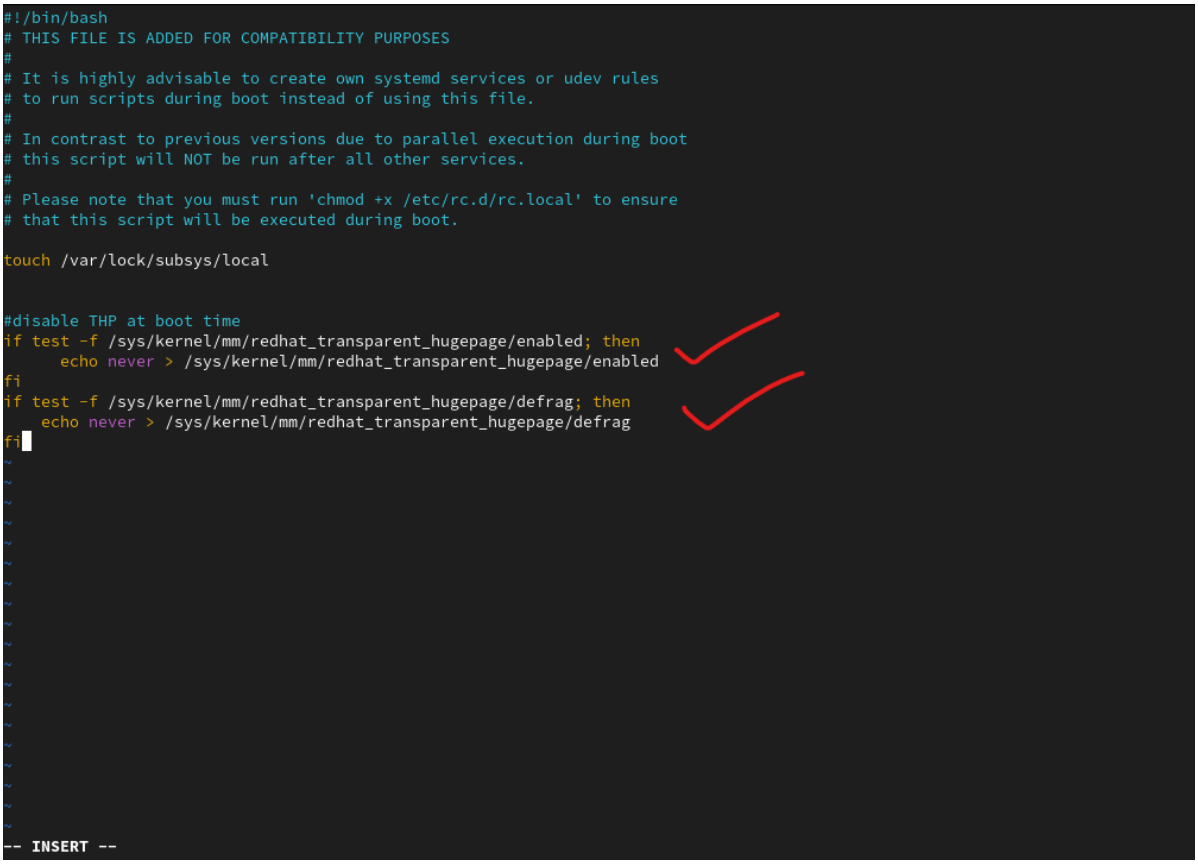
After **vi rc.local** you see the following screen and press **i** to insert the required lines in bottom

```
#!/bin/bash
# THIS FILE IS ADDED FOR COMPATIBILITY PURPOSES
#
# It is highly advisable to create own systemd services or udev rules
# to run scripts during boot instead of using this file.
#
# In contrast to previous versions due to parallel execution during boot
# this script will NOT be run after all other services.
#
# Please note that you must run 'chmod +x /etc/rc.d/rc.local' to ensure
# that this script will be executed during boot.

touch /var/lock/subsys/local

~
~
~
~
~
~
```

Add the following lines and press '**esc**' button to disable the insert text and type **:wq!** Save and exit the **vi**

```
#disable THP at boot time
if test -f /sys/kernel/mm/redhat_transparent_hugepage/enabled; then
    echo never > /sys/kernel/mm/redhat_transparent_hugepage/enabled
fi
if test -f /sys/kernel/mm/redhat_transparent_hugepage/defrag; then
   echo never > /sys/kernel/mm/redhat_transparent_hugepage/defrag
fi
```

Lines are added successfully



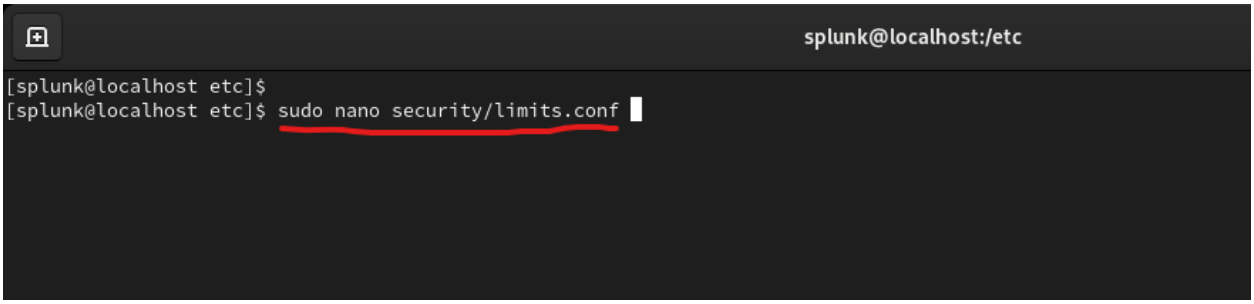
OR using the following script under **/etc/init.d** (Create a new file by typing **nano disable_thp**)

```
#!/bin/bash
### BEGIN INIT INFO
# Provides:          disable-thp
# Required-Start:    $local_fs
# Required-Stop:
# X-Start-Before:    couchbase-server
# Default-Start:     2 3 4 5
# Default-Stop:      0 1 6
# Short-Description: Disable THP
# Description:       Disables transparent huge pages (THP) on boot, to
improve
#                    Couchbase performance.
### END INIT INFO

case $1 in
  start)
    if [ -d /sys/kernel/mm/transparent_hugepage ]; then
      thp_path=/sys/kernel/mm/transparent_hugepage
    elif [ -d /sys/kernel/mm/redhat_transparent_hugepage ]; then
      thp_path=/sys/kernel/mm/redhat_transparent_hugepage
    else
```

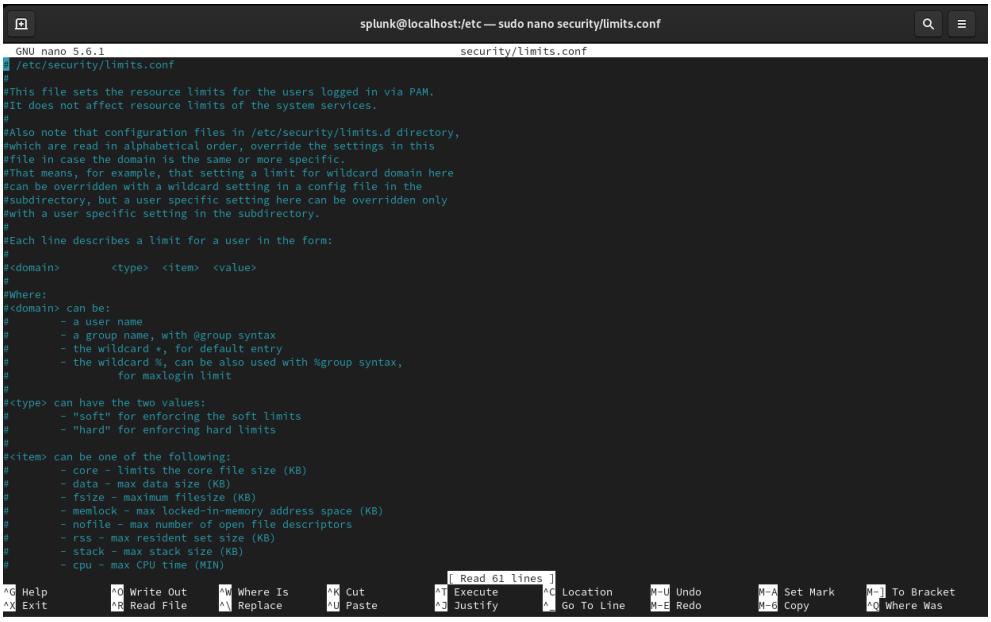
```
        return 0
    fi
    echo 'never' > ${thp_path}/enabled
    echo 'never' > ${thp_path}/defrag
    re='^[0-1]+$'
    if [[ $(cat ${thp_path}/khugepaged/defrag) =~ $re ]]
    then
      # RHEL 7
      echo 0  > ${thp_path}/khugepaged/defrag
    else
      # RHEL 6
      echo 'no' > ${thp_path}/khugepaged/defrag
    fi
    unset re
    unset thp_path
    ;;
esac
```

Now, how to increase **Ulimit** settings (Depending on your environment and needs)

https://www.splunk.com/en_us/blog/tips-and-tricks/whats-your-ulimit.html



You see the **limit.conf** file



And **add** the following lines at end of the file

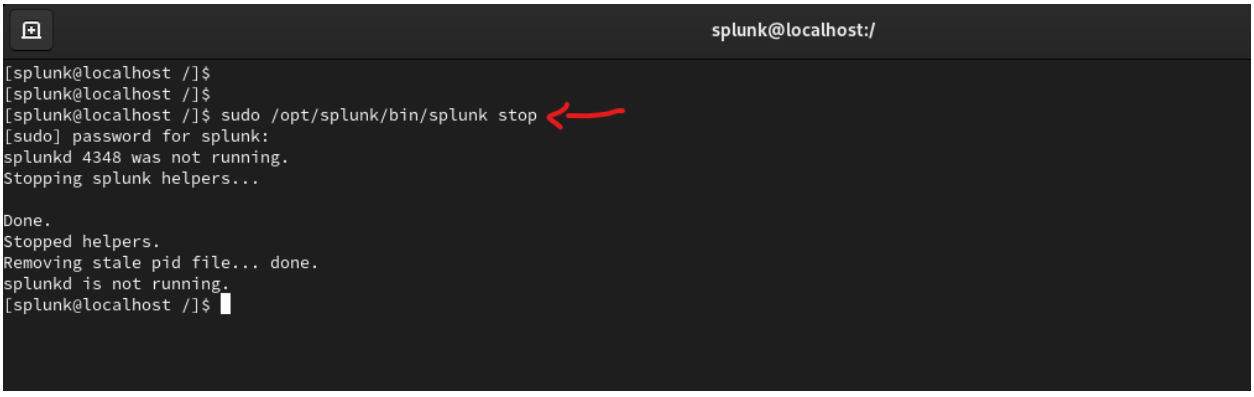
```
*         soft    nofile  unlimited
*         hard    nofile  unlimited
*         hard    core    unlimited
*         hard    nproc   unlimited
*         hard    data    unlimited
*         soft    data    unlimited
*         soft    nproc   unlimited
*         soft    core    unlimited
*         hard    cpu     unlimited
*         hard    fsize   unlimited
*         soft    fsize   unlimited
*         soft    sigpending  unlimited
*         hard    sigpending  unlimited

# End of file
```

```
*         soft    nofile    unlimited
*         hard    nofile    unlimited
*         hard    core      unlimited
*         hard    nproc     unlimited
*         hard    data      unlimited
*         soft    data      unlimited
*         soft    nproc     unlimited
*         soft    core      unlimited
*         hard    cpu       unlimited
*         hard    fsize     unlimited
*         soft    fsize     unlimited
*         soft    sigpending        unlimited
*         hard    sigpending        unlimited
```

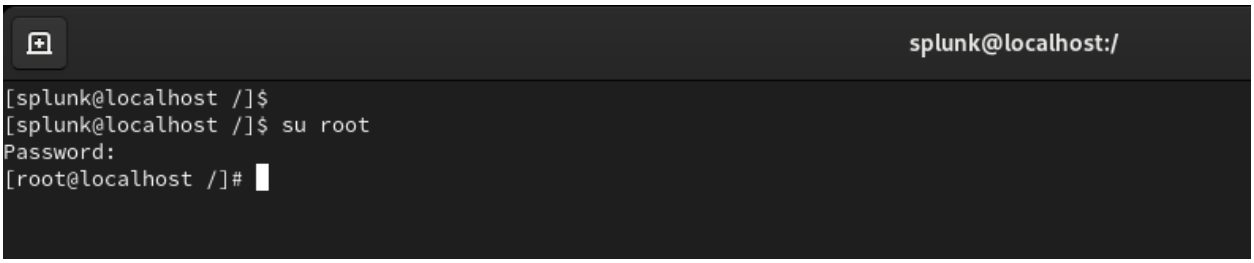
How to enable a **boot start**

https://docs.splunk.com/Documentation/Splunk/9.0.4/Admin/RunSplunkassystemdservice

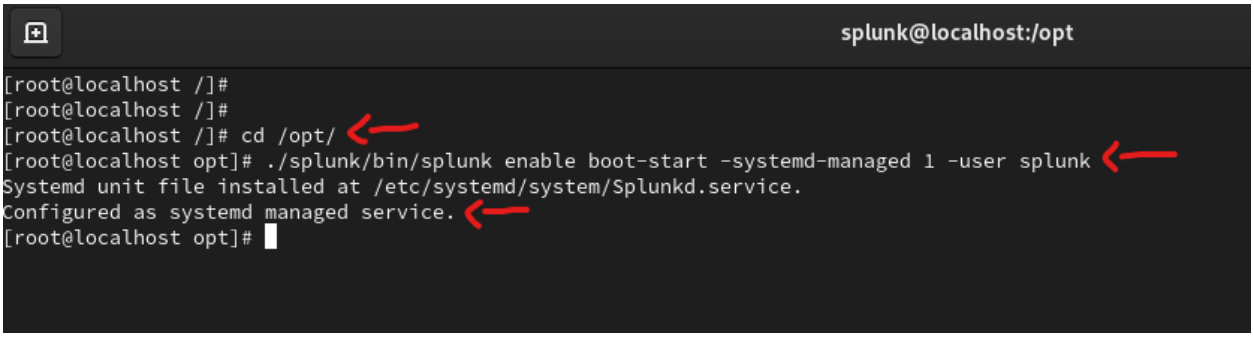
Need to stop **splunk service** first



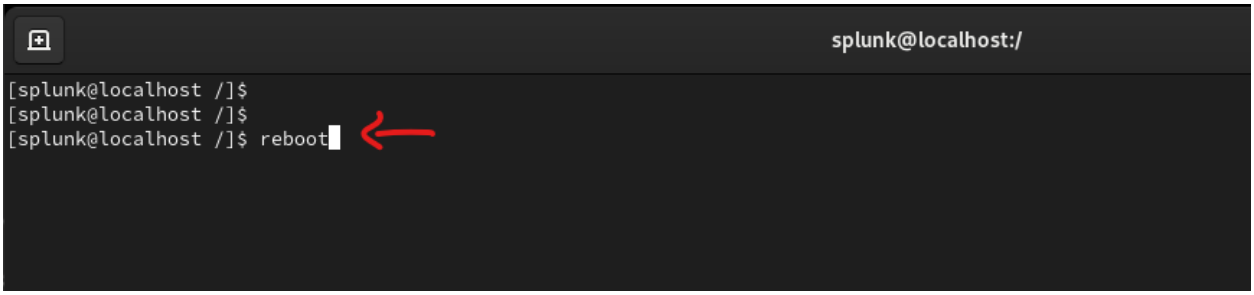
Jump to the root user



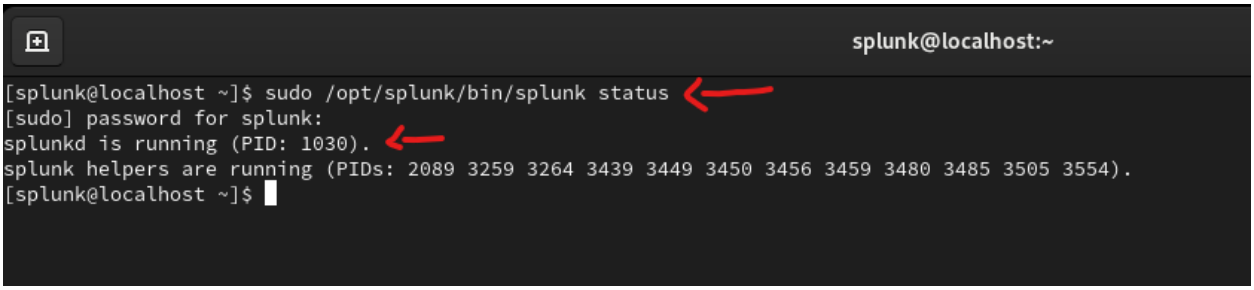
Jump to /opt/ directory and run the following command:
./splunk/bin/splunk enable boot-start -systemd-managed 1 -user splunk



Now, it's time to reboot the device. As you can see, the Splunk service has automatically started

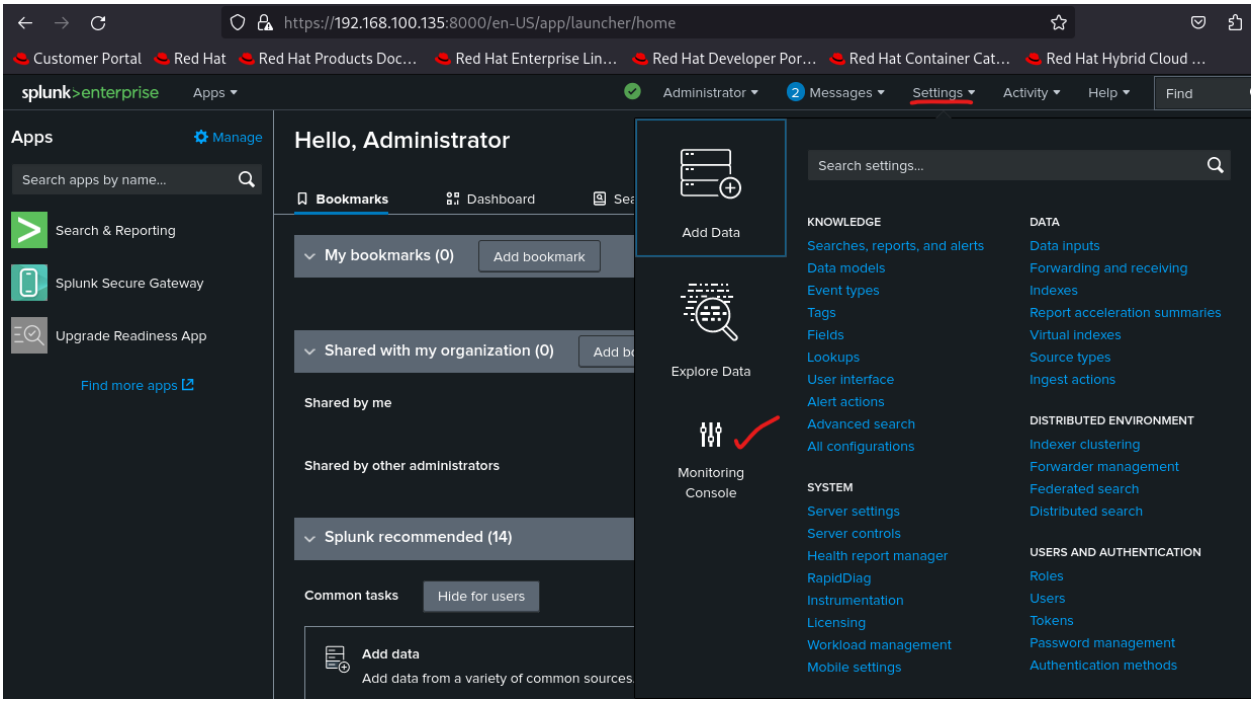


After reboot the splunk service has started automatically

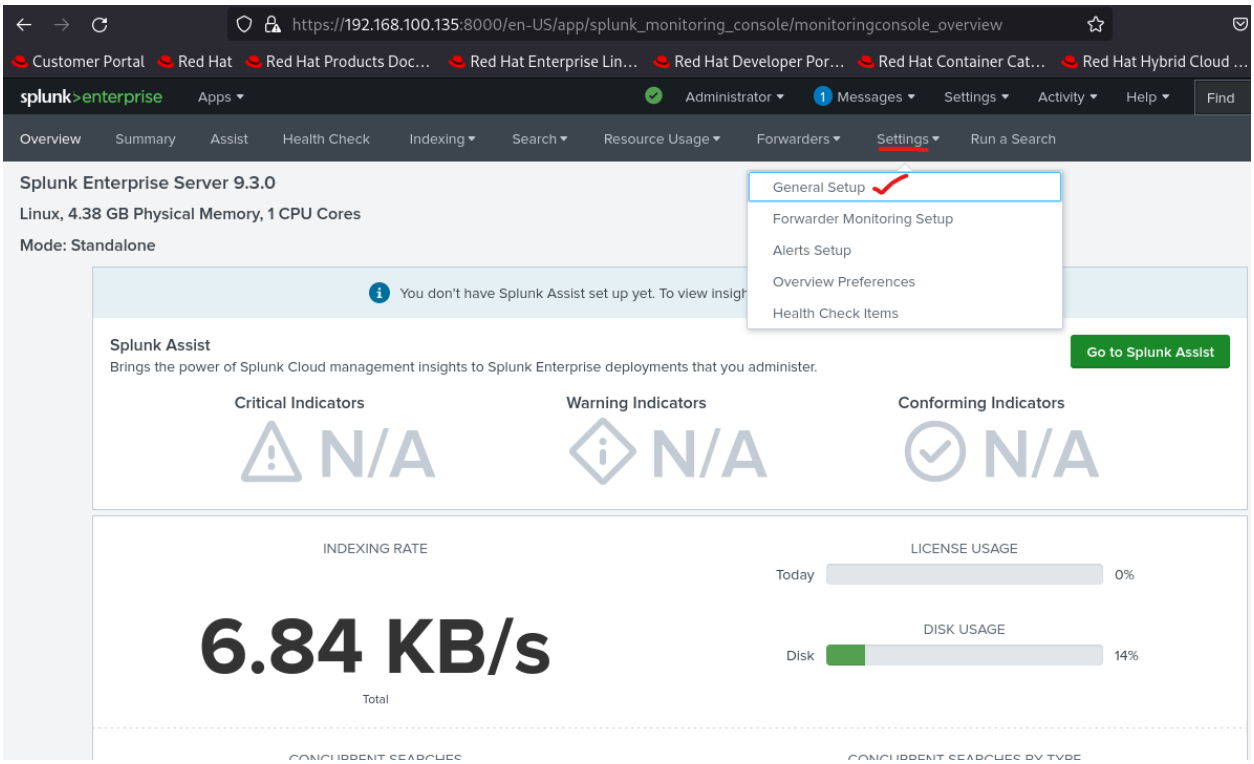


Post installation – **Health Checks**

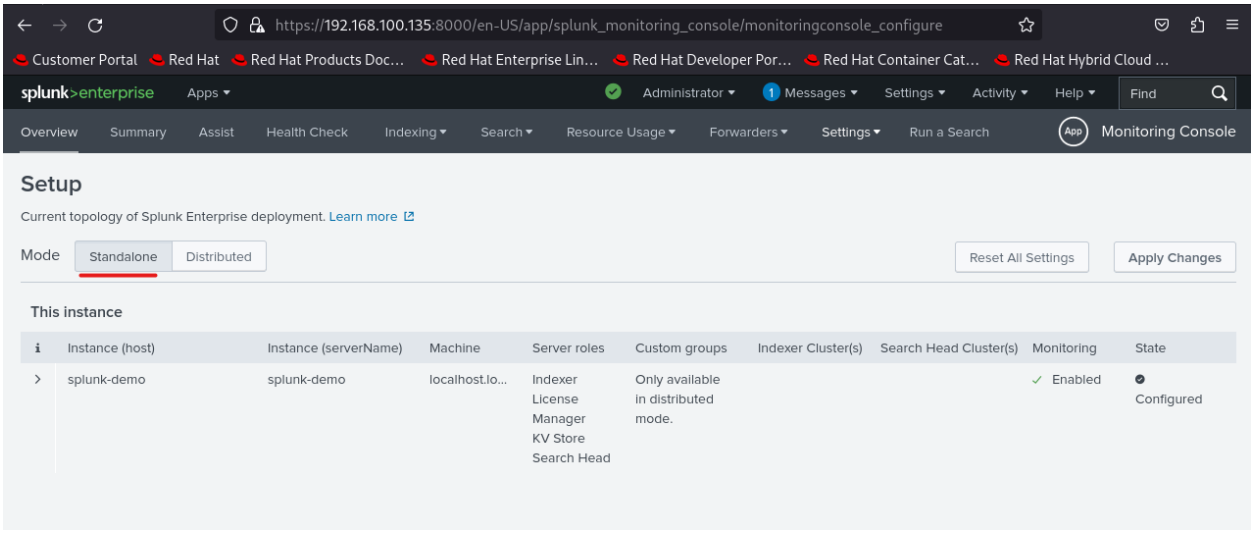
Log in to the Splunk UI > **Settings** > **Monitoring Console**



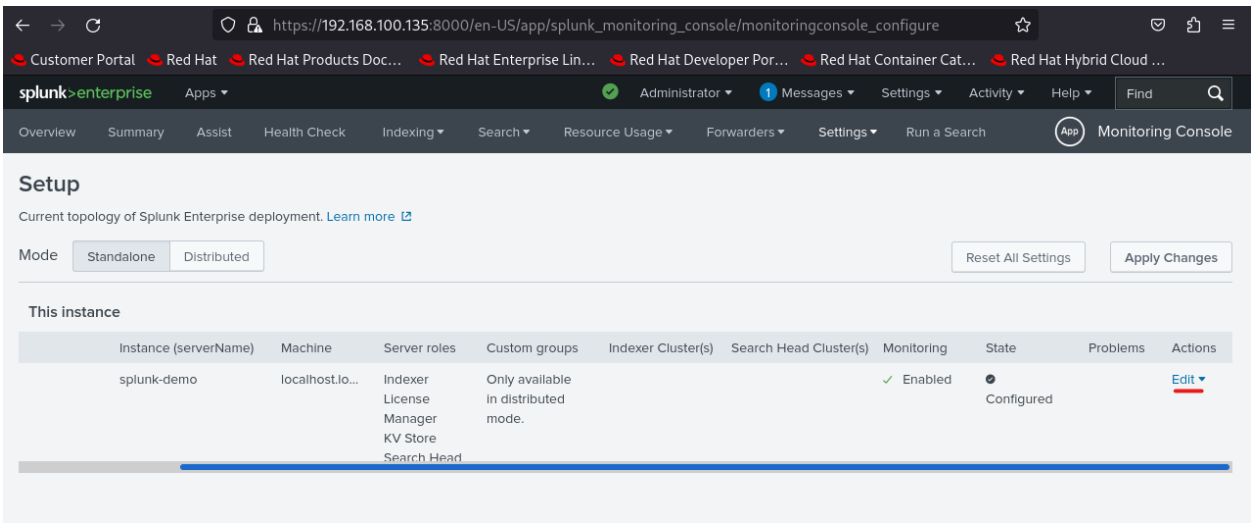
Go to the **Settings > General Setup**



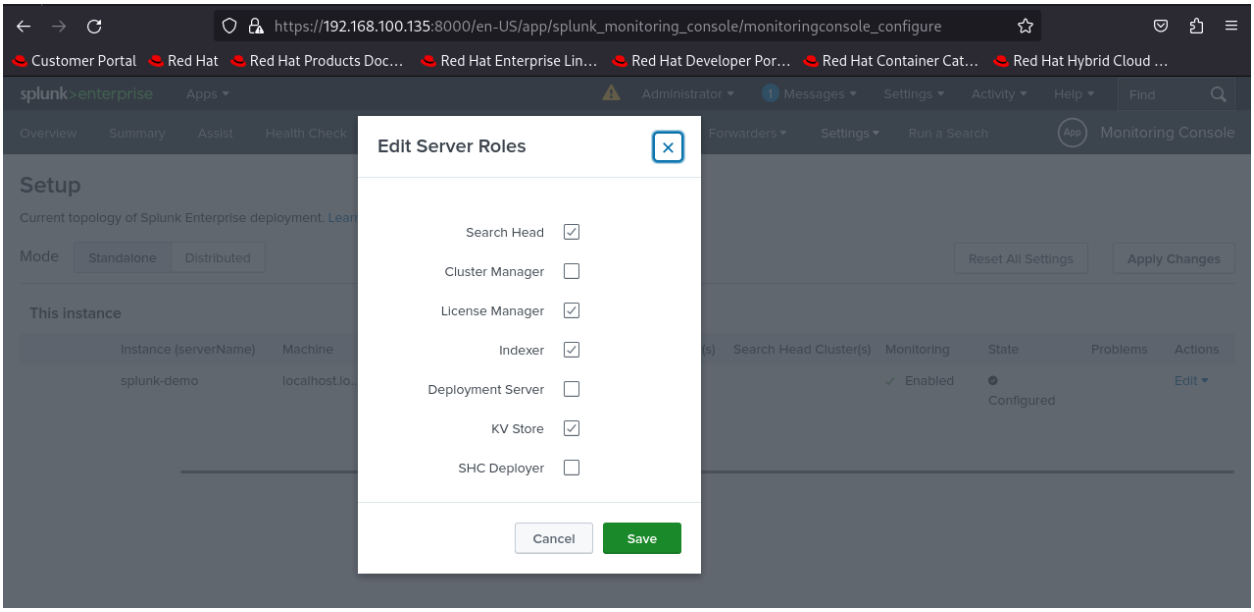
The mode is **Standalone**



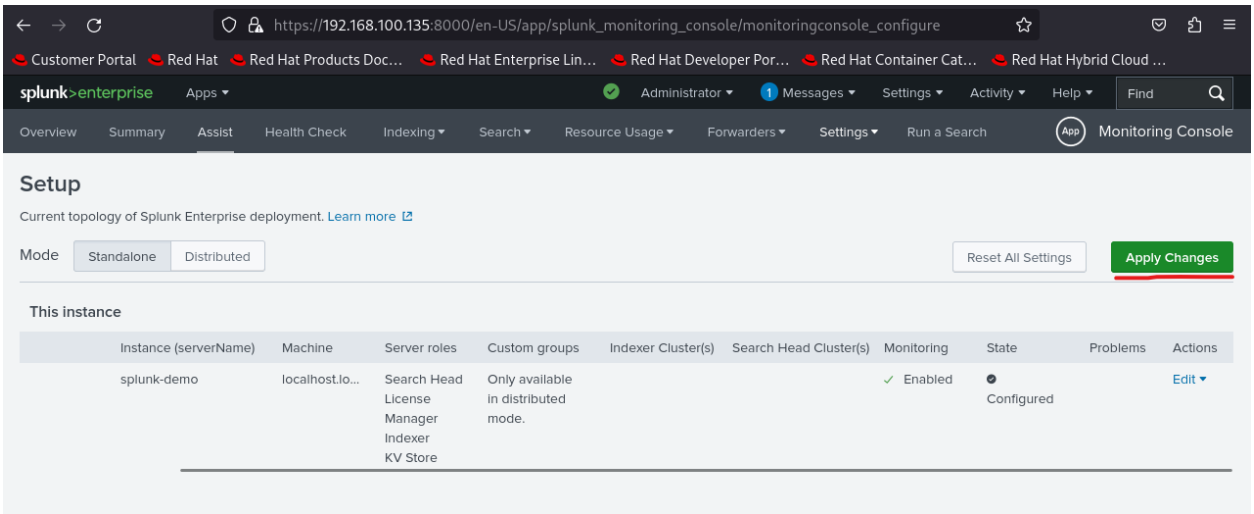
Scroll the page toward the right and click **Edit**



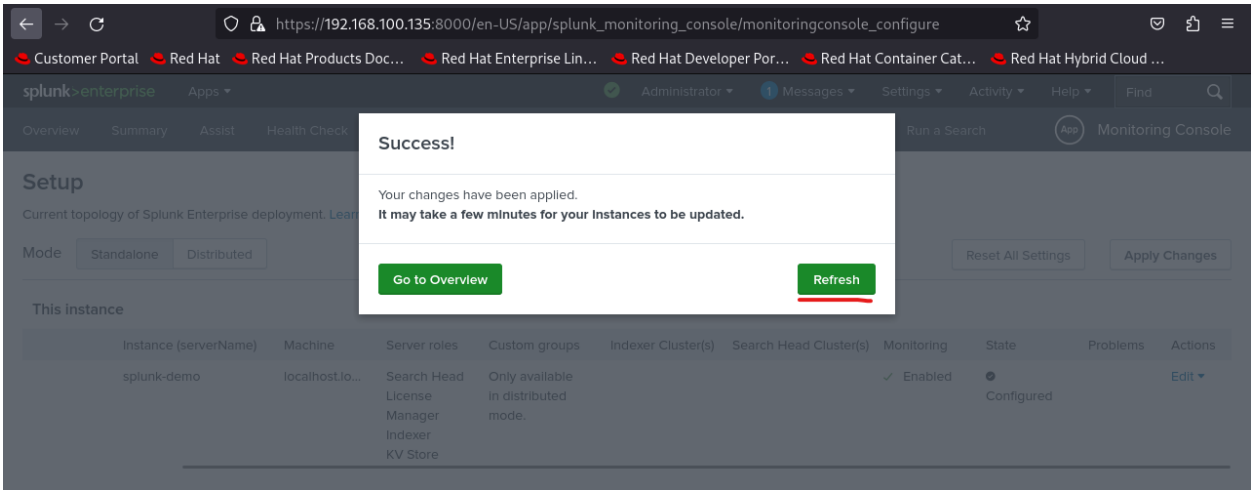
Now, these are the **roles** for **Standalone Splunk** instance click on **Save**



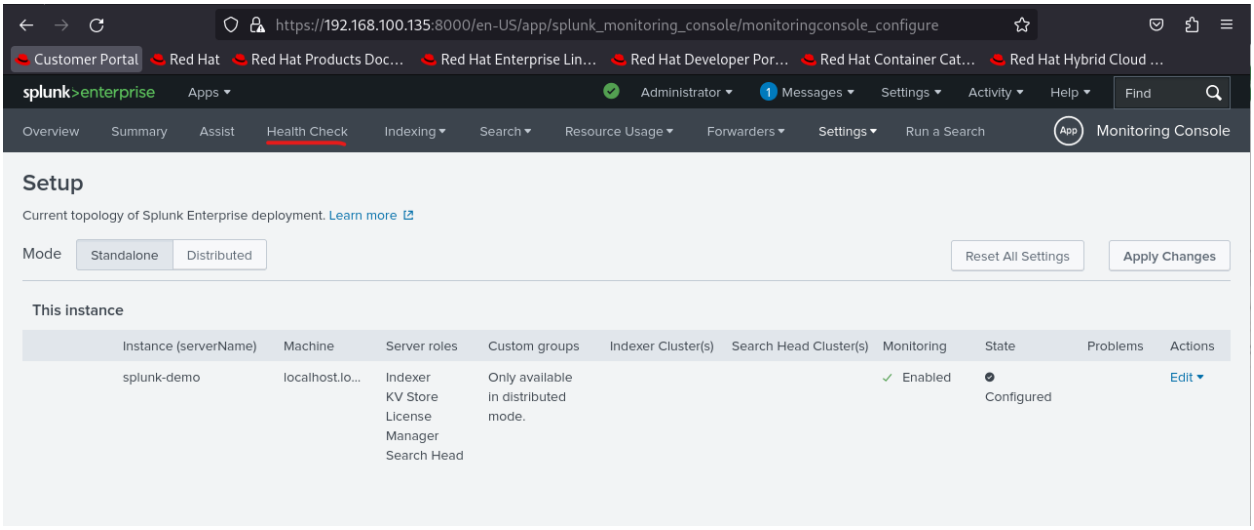
Click on **Apply Changes**



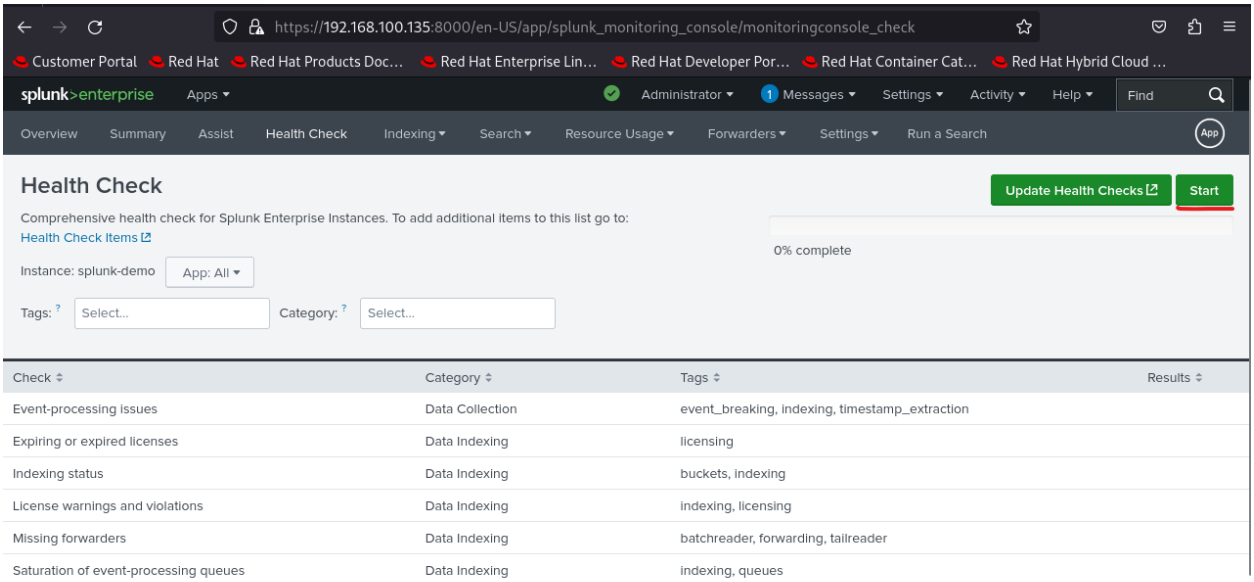
Hit **Refresh**



Click on **Health Check**

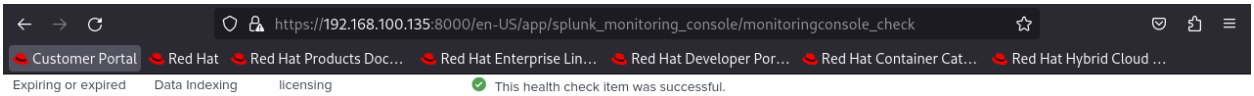


And hit **Start**



Check	Category	Tags	Results
Event-processing issues	Data Collection	event_breaking, indexing, timestamp_extraction	
Expiring or expired licenses	Data Indexing	licensing	
Indexing status	Data Indexing	buckets, indexing	
License warnings and violations	Data Indexing	indexing, licensing	
Missing forwarders	Data Indexing	batchreader, forwarding, tailreader	
Saturation of event-processing queues	Data Indexing	indexing, queues	
Search scheduler skip ratio	Data Search	scheduler, searches_skipped	
Excessive physical memory usage	Splunk Miscellaneous	resource_usage	
Integrity check of installed files	Splunk Miscellaneous	configuration, installation	
KV Store status	Splunk Miscellaneous	kv_store	

Most of the health checks, including **THP**, have been passed



Expiring or expired licenses	Data Indexing	licensing	This health check item was successful.
Indexing status	Data Indexing	buckets, indexing	This health check item was successful.
License warnings and violations	Data Indexing	indexing, licensing	This health check item was successful.
Saturation of event-processing queues	Data Indexing	indexing, queues	This health check item was successful.
Search scheduler skip ratio	Data Search	scheduler, searches_skipped	This health check item was successful.
Excessive physical memory usage	Splunk Miscellaneous	resource_usage	This health check item was successful.
KV Store status	Splunk Miscellaneous	kv_store	This health check item was successful.
Orphaned scheduled searches	Splunk Miscellaneous	configuration, search, searches_skipped	This health check item was successful.
Near-critical disk usage	System and Environment	capacity, disk_space, searches_skipped, storage	This health check item was successful.
Linux kernel transparent huge pages	System and Environment	best_practices, operating_system	This health check item was successful.
Assessment of server ulimits	System and Environment	best_practices, operating_system	This health check item was successful.

How to **remove Splunk** Enterprise