Upgrading Splunk deployment

Order of upgrading customers on-prem

1. Master Node
2. Search Heads
3. Enable maintenance Mode on Master Node
   1. https://docs.splunk.com/Documentation/Splunk/9.0.4/Indexer/Usemaintenancemode
4. Indexers
5. Disable maintenance Mode on Master Node
6. Deployment Server
7. Heavy Forwarder & UFs

**Pre-checks for Splunk Upgrade**

1. Verify if all servers required for upgrade are accessible
2. App compatibility check
   1. Verify if the apps are compatible with the version you are upgrading to
3. Use the script to perform the check
   1. Prepare RFC and make a note of below things
4. Verify the splunk version compatibility
   1. Windows
5. Verify that windows/server version is supported
6. Verify the disk space on each splunk server that requires the Splunk upgrade. It should be less than 80%
7. Make sure KV store status looks good
   1. Splunk show kvstore-status –verbose
8. Verify the indexer and forwarder compatibility
   1. <https://docs.splunk.com/Documentation/VersionCompatibility/current/Matrix/Compatibilitybetweenforwardersandindexers>
   2. Check versions of HF/UF/DS sending data to splunk cloud instance

Index = \_internal sourcetype=splunkd source=\*”/var/log/splunk/metric.log” Metrics group=tcpin\_connections

| dedup hostname

| rex field =version \* "(?<fwdV>\d+.\d+)"

| eval splV=8.2

| eval Recommendation=if((splV-fwdV)>0.1, “Upgrade”, “No Upgrade Needed”)

| eval “Forwarder Type” = case(fwdType==”uf”, “Universal” , fwdType==”lvf”, “Light”, fwdType=="full", "Heavy")

| eval \_time=strftime(\_time, “%c”)

| rename \_time as “Last Log” , hostname as “Forwarder Name”, version as “Forwarder Version”

| table “Forwarder Name” , “Forwarder Version”, “Forwarder Type”, “Last Log”, Recommendation

| sort -Recommendation “Forwarder Type” “Forwarder Version”

Upgrade steps when using tarball (tgz file)

1. Download tarball using wget command
2. Stop the Splunk Enterprise service: Stop Splunk via splunk user
3. If you are using a .tar file expand it into the same directory with the same ownership as your existing Splunk Enterprise instance. This overwrites the -C /opt
4. Start the Splunk Enterprise services by running /$SPLUNK\_HOME/bin/splunk restart

**Upgrade steps for rpm is listed in RFC**

Once RFC is Approved: Steps to perform before Splunk Upgrade

1. Before implementing your change:
   1. Email SOC about the upgrade
      1. Make sure the devices are added in Maintenance
   2. Notify Client about the upgrade and cc CSM on that email as well
2. Verify the disk space on each Splunk server that requires Splunk Upgrade. It should be less than 80%
3. Add your changes to Calendar
4. Take backup of etc folder on server. Place it in the home folder
   1. Linux
      1. Cd /home/<user>
      2. Mkdir backup
      3. Cd backup
      4. Tar -czf splunk\_etc\_backup\_$(uname -n)\_$(data + “%Y\_%m\_%d”).tgz /opt/splunk/etc
5. Verify the sourcetype and index thruput on the (Last 30 days)
   1. Index= \_internal source=metrics.log per\_sourcetype\_thruput |evel MB=kb/1024 | timechart span=1d limit=20 sum(MB) by series
   2. Index= \_internal source=metrics.log per\_index\_thruput |evel MB=kb/1024 | timechart span=1d limit=20 sum(MB) by series
   3. Index= \_internal source=metrics.log per\_source\_thruput |evel MB=kb/1024 | timechart span=1d limit=20 sum(MB) by series
6. Verify the deployment clients (if Applicable)
7. Follow the Step from your RFC to complete the Splunk Upgrade

**Post-Checks for Splunk Upgrade:**

1. Verify that all instances are upgraded to the requested version successfully
2. Run Health Check on all servers from the monitoring console and fix the errors if any
3. Ensure there are no alerts on Barracuda for the servers. Ensure SNMP monitoring is enabled
4. Validate the apps on the servers on the servers are not throwing any errors and the configured inputs are collecting data post upgrade.
5. Verify the sourcetype and index thruput on the server (Last 30 days)
   1. Index= \_internal source=metrics.log per\_sourcetype\_thruput |evel MB=kb/1024 | timechart span=1d limit=20 sum(MB) by series
   2. Index= \_internal source=metrics.log per\_index\_thruput |evel MB=kb/1024 | timechart span=1d limit=20 sum(MB) by series
   3. Index= \_internal source=metrics.log per\_source\_thruput |evel MB=kb/1024 | timechart span=1d limit=20 sum(MB) by series
6. Check KVStore status post upgrade
   1. Splunk show kvstore-status –verbose
7. Verify the Deployment clients (if Applicable)
8. Verify Phone home to DS (if Applicable)

| rest splunk\_server=local /services/deployment/server/clients

| table hostname ip utsname \*.restartSplunkd package lastPhoneHomeTime

| eval temp=hostname. “#”.ip.”#”.utsname.”#”.package.”#”.lastPhoneHomeTie

| table temp \*. RestartSplunkd

| untable temp apps count

| evel Apps = if (like (apps, “apps%”), mvindex (split(apps, “.”), 1), null())

| eval serverclass=