Please create a CFT in a new repo on GitHub with the following information. Ensure successful deployment in EVAL only, but create the resource file for SS PROD as part of this process Repo Name: splunk-search-nonprod
Resources needed:
ALB
Target Groups point to port 8000 with TLS enabled on each EC2
TLS with http redirect to https enabled
Should be listening on 1a, 1b, and 1c AZS in PROD
EC2
Number of Hosts: 1
Instance Types:
Eval: t3a.medium
SS Non-Prod: c7i.4xlarge
Amazon Linux 2023
Use AWS AMI from SSM: /aws/service/ecs/optimized-ami/amazon-linux-2023/recommended/image_id Hosts should be non-auto-scaling
Hosts should be placed in 1a with 1b and 1c as available AZS in the default CFT config
EC2s should use the standard naming pattern and script that we currently use in userdata, but should be used in cfn-init instead. This will ensure our naming standard is used. EC2 Naming Standard: [env]-[os]-[Tag:: Pod]-[Tag:: Technology]-[ident]
Tag::Pod = splunk
Tag:: Technology: search
DNS
ALB should have DNS set for each of the deployable environments:
EVAL np.splunk.eval.aamc.org
SS NON-PROD: splunk.ent-np.aamc.org
Use cfn-init
Do not use userdata, instead use cfn-init
Ensure the splunk user exists as UID/GID: 1250/1250
User should not be able to ssh (no password)
Ensure all other standard tagging is done for all resources
Do NOT install the splunk agent, these steps will be done after the base template is built, deployed, and tested in eval with success.