

Steps for ThreatAlert-gss parent CloudFormation

1. Create S3 bucket and name it “[customername]-threatalertgss”
2. Put the 4 files in there based on if it is govcloud or commercial cloud
   1. <https://github.com/stackArmor/Threat-Alert>
   2. ThreatAlert-gss is the parent stack and is the same file regardless if it is commercial or Gov Cloud
   3. ThreatSplunknSG, PaloAlto, and RestofApps are the three child stacks for commercial
   4. ThreatSplunknSGGov, PaloAltoGov, and RestofAppsGov are the three child stacks for Gov Cloud
3. Create S3 bucket and name it “[customername]-paloaltoconfig-bucket”
4. Run the stack using ThreatAlert-gss (the parent stack)
5. Determine VPC (the default is 10.0.0.0/24)
6. Determine FedRAMP (the default is FedRamp-Moderate)
   1. This currently just tag server that the level of FedRamp based on this parameter
7. Select the TypeOfCloud based on if it is either commercial cloud or gov cloud
8. Put in the CIDR block for external access to the Remote Desktop Gateways
9. Select keypair
10. Change either TAS3BucketName (commercial) or GTAS3BucketName (GovCloud) based on step 1
11. Put in the password for the DomainAdmin (needs symbol) and MicrosoftADPW
12. Change the DomainDNSName to the desired DNS. It is currently “threatalert.stackarmor.com”
13. Change the instance types if desired
14. Change S3BucketNameP based on step 3
15. Enter DSMAdminPass and the number of DSM Protected Instances

