DAP Implementation Outline

DAP/Conjur Implementation

A.      Review/finalize architecture

B.      Review and agree upon integrations (HSM/KMS, SysLog, Vault Synchronizer, platforms like k8s/OCP/PCF, etc.)

C.      Review pre-requisites (infrastructure buildout including docker hosts, load balancers, certificates, resources from other teams (if needed), etc)

D.      Deploy DAP Environment

1.       Check Infrastructure - check docker version, hardware requirements, certificates, load balancers...etc

2.       Download conjur-appliance image or spin up shared AMI Instance

3.       Load image into local repository of each host

4.       Create docker containers

5.       Configure Master

6.       Import the Root/CA certificate

7.       Import the master key and server certificate pair

8.       Import the key file and server certificate pair for the Follower load balancer

9.       Configure Master key encryption (if necessary)

10.   Create Standby Seed files

11.   Copy seed files to Standby hosts

12.   Unpack seed files on standby containers

13.   Configure Standby's

14.   Initiate replication

15.   Create Follower seed files

16.   Unpack seed files on Follower containers

17.   Configure Follower containers

18.   Pull CLI image

19.   Load CLI Image into local repo

20.   Create CLI container

21.   Login to CLI

22.   Create root-cluster.yml file

23.   Load root-cluster.yml policy

24.   Enable Auto-Failover

25.   Load Environmental policies

26.   Load User & Group policies

E.       Review Operational considerations (e.g. backup/restore, upgrades)

F.       Hold Policy workshop to review policy best practices and workflows

G.      Configure integrations not configured as part of the DAP environment buildout

H.      Review integration patterns (api calls, Summon, authn-k8s, etc.)