Load Balancer Documentation

The implemented solution uses two Amazon elastic load balancers, one mapping to the IdP machines and one mapping to the CPR machines. Backend authentication is not used, but every member of the ELB must be one of the enumerated VM's, and communications between that VM and the ELB are encrypted. Communications between the ELB and the user are encrypted.

- CommITIdPELB
  DNS Name:
  CommITIdPELB-1232715940.us-west-2.elb.amazonaws.com (A Record)
  ipv6.CommITIdPELB-1232715940.us-west-2.elb.amazonaws.com (AAAA Record)
  dualstack.CommITIdPELB-1232715940.us-west-2.elb.amazonaws.com (A or AAAA Record)
  Port Configuration: 443 (HTTPS, Certificate: StarCommonIDTrustOrg) forwarding to 8443 (HTTPS)
  Backend Authentication: Disabled
  Stickiness: LBCookieStickinessPolicy, expirationPeriod='3600'(edit)
  80 (HTTP) forwarding to 8080 (HTTP)
  Stickiness: LBCookieStickinessPolicy, expirationPeriod='3600'(edit)
  8080 (HTTP) forwarding to 8080 (HTTP)
  Stickiness: Disabled(edit)
  us-west-2b

- CPRLoadBalancer
  DNS Name:
  CPRLoadBalancer-1301092763.us-west-2.elb.amazonaws.com (A Record)
  ipv6.CPRLoadBalancer-1301092763.us-west-2.elb.amazonaws.com (AAAA Record)
  dualstack.CPRLoadBalancer-1301092763.us-west-2.elb.amazonaws.com (A or AAAA Record)
  Port Configuration: 443 (HTTPS, Certificate: StarCommonIDTrustOrg) forwarding to 8443 (HTTPS)
  Backend Authentication: Disabled
  Stickiness: LBCookieStickinessPolicy, expirationPeriod='3600'(edit)
  80 (HTTP) forwarding to 8080 (HTTP)
  Stickiness: LBCookieStickinessPolicy, expirationPeriod='3600'(edit)

CNAME DNS records were established mapping common domain names to the dualstack DNS record for each ELB.

Future implementations may consider use of haproxy with multiple proxy IP addresses mapped to by a single DNS entry, and each of those haproxy proxies sitting in front of an array of machines, to avoid making the load balancer a single point of failure and ensuring that all data is transiently present in cleartext only on systems owned by the CommIT operator.