SBA One Architecture Overview – Release 2

AWS

US East Cloud Region

VPC

Production 10.106.0.0/16

Private Subnet AZ1

CACHE
Elasticache Cluster

PostgreSQL
PostgreSQL Primary Instance

Web Servers

Public Subnet AZ1

ELB

NAT Service

IGW

Cloud Front

AWS WAF*

R PostreSQA instance read replica

Talend Administrator Console (TAC), Talend Execution Center (TEC)

Document Scanner Server

Auto Scaling

Document Scanner Server Failover

Auto Scaling

CACHE Elasticache Cluster

Web Servers

PostgreSQL PostgreSQL Secondary Instance

R PostreSQA instance read replica

Manual Failover**

TAC/TEC servers

Public Subnet AZ1

Private Subnet AZ2

S3

S3

VPC Peering

Amazon Route 53

S3

NAT Service

IGW

Max.gov

WWW

End Users

DevOps (Developer Workstations)

System Administrators

Management 10.104.0.0/16

VPC

PAM Server1

Splunk Server1

Jenkins Master1

Chef Server1

Jenkins Build Server1

SIEM Server1

Public Subnet AZ1

Private Subnet AZ1

Manual Failover

PAM Server2

Public Subnet AZ2

Maintenance Servers from AZ1private subnet restored from snapshot

Private Subnet AZ2

VPC Peering

VPC

IGW

Staging 10.105.0.0/16

- Set-up similar to that of Production (minus Data Migration Server)
- Staging used for Initial PROD testing, hot-fixes thereafter
- Staging & Prod use same CFT – parameterized for VPC and other environment-specific differences

SaaS Tools:
- **Rally**
- **Confluenc**
- **GitHub**

Network flows
—— ingress
—— egress

*Firewalls will be configured at each instance of a subnet via AWS security groups. By default, all inbound traffic will be denied. Ports & source must be explicitly opened. New AWS WAF firewall will secure traffic outside CloudFront.
Blacklisting at the subnet level will be configured via Network Access Control Lists.
**Manual Failover of maintenance servers and Data Migration Servers for Release2, HA implemented later. SNS will be set-up for notification of failure.

Release 2: For Q4-2016 - Version 0.1-Iteration 17 Status:Draft

SBA One Architecture Detailed View – Release 2

AWS

VPC

Production 10.106.0.0/16

US East Cloud Region

Web Servers
- *Ruby on Rails / app s/w*
- *nginx*
- *AWS CodeDeploy agent*
- *tcpdump-to-log cron job*

CACHE
Elasticache Cluster

PostgreSQL
PostgreSQL Primary Instance

Document Scanning Server
- *Ruby on Rails / app s/w*
- *AWS CodeDeploy agent*
- *tcpdump-to-log cron job*
- *doc scanner cron job*
- *clamd daemon*

Data MigrationServers
- *TAC Server*
- *Talend ETL*
- *postgresql client*
- *apache, git*
TEC Server:
- *Talend TEC*
- *apache*

R PostreSQL read replica

ELB

NAT Service

IGW

Public Subnet AZ1

Public Subnet AZ1

Private Subnet AZ3

Auto Scaling

Auto Scaling

Manual Failover

Web Servers

CACHE Elasticache Cluster

R PostgreSQL read replica

PostgreSQL PostgreSQL Secondary Instance

Document Scanning Server

Data Migration Server

Private Subnet AZ2

S3
- *sba-build-repo*
- *sbaone-cloudtrail-logs*
- *sba-prod-backups*
- *sba-maintenance*

S3
- *sba-docs-prod*

VPC

Management 10.104.0.0/16

Base Image

Included on all servers (except PAM):
- *CentOS 6.7 hardened*
- *ClamAV / freshclams*
- *OSSEC client/agent*
- *OpenScap utils (client)*
- *Additional tools (e.g. bind-utils)*
- *Splunk forwarder (client)**
- ***Added after instance lauch via Chef***

NAT Service

IGW

PAM Server

Public Subnet AZ1

Jenkins Build Server

Jenkins Master

Chef Server1

Splunk Enterprise Server

SIEM Server
- *ossec server*
- *bro log analysis*
- *knife workstation*
- *OpenSCAP*

Private Subnet AZ1

Manual Failovers

PAM Server2

Public Subnet AZ2

Maintenance Servers from AZ1private subnet restored from snapshot

Private Subnet AZ2

Release 2: For Q4-2016 Iteration 17 - Version 0.1 Status:Draft

SBA One Architecture Overview – Release 2

US East Cloud Region

AWS

VPC — Production 10.106.0.0/16

Private Subnet AZ1

PostgreSQL
PostgreSQL Primary Instance

PostgreSQL read replica

TAC Server   TEC Server

Document Scanner Server

Web Servers

ELB

NAT Service

IGW

Public Subnet AZ1

Auto Scaling
Web Servers

PostgreSQL read replica

PostgreSQL
PostgreSQL Secondary Instance

Manual Failover**

TAC/TEC servers

Auto Scaling
Document Scanner Server Failover

Public Subnet AZ1

Private Subnet AZ2

S3

S3

VPC Peering

VPC — Management 10.104.0.0/16

NAT Service

IGW

PAM Server1

Public Subnet AZ1

Splunk Server1

Jenkins Master1

Chef Server1

Jenkins Build Server1

SIEM Server1

Manual Failover**

PAM Server2

Public Subnet AZ2

Maintenance Servers from AZ1private subnet restored from snapshot

Private Subnet AZ2

Private Subnet AZ1

VPC Peering

VPC — Staging 10.105.0.0/16

IGW

- Set-up similar to that of Production (minus Data Migration Server)
- Staging used for Initial PROD testing, hot-fixes thereafter
- Staging & Prod use same CFT – parameterized for VPC and other environment-specific differences

Instance Key
- Reserved (green)
- Planned-Reserved (blue)
- On-Demand (orange)

*Firewalls will be configured at each instance of a subnet via AWS security groups. By default, all inbound traffic will be denied. Ports & source must be explicitly opened. New AWS WAF firewall will secure traffic outside CloudFront.
Blacklisting at the subnet level will be configured via Network Access Control Lists.
**Manual Failover of maintenance servers and Data Migration Servers for Release2, HA implemented later. SNS will be set-up for notification of failure.

Release 2: For Q4-2016 - Version 0.1-Iteration 17 Status:Draft