Capital Goods: Ventura Application Prod Environment Build Requirement Definition Document (RDD)

Hello Boris,

As concluded today in our call:

- Capital Goods is a company that deals with a variety of products across different manufacturing lines (Grocery, Machineries, Electronics and Clothing). However we only offer our services instore today across the different business domains and units mentioned. The demand for machinery and electronics in recent days has grown tremendously and the majority of the Global sales are all driven by online shoppers. Our customer requests for online services for our mechineeries and electronic products have grown by 300% in the last 6 months and the growth continues. This is the reason why Capital Goods is embarking on this project to develop and host **Ventura** applications which will provide our customers across the United States, Canada, Africa, Europe and Asia the opportunity to make purchases from anywhere and anytime.

- The following resource build requirements are strictly for the "Dev" environment only and related questions about this requirement and environment specifications should be targeted to the Senior Solutions Architect Brian Moderate.

    - 1 RDS instance using MySQL-engine, with high availability configured
    - Bastion hosts to provide a single point of management of all instances
    - 2 load balancers 1 for the web tier and 1 for the application tier
    - 6 instances for the web tier
    - 6 instances for the app tier
    - S3 bucket to host static content, which will be served via CloudFront for a more robust customer experience across geographical locations.
    - Region: us-east-1

Additional details have been provided in confluence. Please find below the confluence URL for your reference

Confluence Pages:

a. **Web Servers (Prod)**

Number of instances	OS	Instance Type	Installations + Configurations	Comments

6	CentOS 7	t2-medium	Apache (httpd) Tenable Shorewall Crowdstrike Cloud Watch Agent AD Join SELinux Disabled	1. Follow our resource naming standards which will be "ventura-prod"-resourcename" 2. Add all our mandatory and strongly recommended labels (- application id: dmt468 - owner: developers-name - environment: prod - budget code: cost-prod - patch group: pg-prod - compliance classification: nist - data classification: pii - LOB: e-commerce - project manager: alexander-dirus - project name: ventura-project - region: us-central1

a. App Servers (Prod)

Number of instances	**OS**	**Instance Type**	**Primary Volume Size**	**Installations + Configurations**	**Comments**
6	CentOS 7	t2-medium	250GB	Apache Tomcat Tenable Shorewall Crowdstrike Cloud Watch Agent AD (MS Active Directory) Join SELinux Disabled	1. Following our resource naming standards which will be "ventura-prod"-resourcename" 2. Add all our mandatory and strongly recommended labels (- application id: dmt468 - owner: developers-name - environment: prod - budget code: cost-prod - patch group: pg-prod - compliance classification: nist - data classification: pii - LOB: e-commerce - project manager: alexander-dirus - project name: ventura-project - region: us-central1

b. RDS(MySQL) Instance (Prod)

Number of instances	Engine	Instance Type (MT)	Multi AZ (Y/N)	Storage Size (PD)	Template	Comments
1	MySQL	db.m5d.large (2vCPU, 8Mem)	Y	General Purpose: 500GB	As per environment	1. Following our resource naming standards which will be “ventura-prod”-resourcename” 2. Add all our mandatory and strongly recommended labels (- application id: dmt468 - owner: developers-name - environment: prod - budget code: cost-prod - patch group: pg-prod - compliance classification: nist - data classification: pii - LOB: e-commerce - project manager: alexander-dirus - project name: ventura-project - region: us-central1

c. Amazon Simple Storage Service

- S3 buckets will be implemented with all mandatory security features enabled (refer to the confluence of S3 security standards).
  - Enable encryption
  - Bucket/Object ACLs
  - Enable Bucket Logging
  - Enable Versioning
  - Define Object Lifecycle (Standard 120 days…..)

2) Network Environment (Prod)

Proposed **Prod** VPC/Subnet environment - VPC IP address/CIDR 10.0.0.0/16						
Subnet Name	Type	AZs	Usage	CIDR	Total Ips	Remark
Ventura-Prod-NAT-ALB-Subnet-1	Public	us-east-1a	NAT Gateways and ELB(ALB)	/28	11	10.0.1.0
Ventura-Prod-ALB-Subnet-2	Public	us-east-1b	ELB (ALB)	/28	11	10.0.3.0
Ventura-Prod-Web-Subnet-1	Private	us-east-1a	Web/Agent Servers	/23	507	10.0.5.0
Ventura-Prod-Web-Subnet-2	Private	us-east-1b	Web/Agent Servers	/23	507	10.0.10.0
Ventura-Prod-App-Subnet-1	Private	us-east-1a	App/Agent Servers	/23	507	10.0.15.0
Ventura-Prod-App-Subnet-2	Private	us-east-1b	App/Agent Servers	/23	507	10.0.20.0
Ventura-Prod-DB-Subnet-1	Private	us-east-1a	RDS(MySQL) DB (Primary DB)	/27	27	10.0.25.0
Ventura-Prod-DB-Subnet-2	Private	us-east-1b	RDS(MySQL) DB (Secondary DB)	/27	27	10.0.30.0
Total IPs					2,104	

Additional Notes:

- As shown on the architecture, application availability will be achieved by having 2 availability zones at every time.
- On security:
  - In the application, only the web hosts could/may not be publicly facing. But the application and RDS(MySQL) instances must be Private
  - Firewall(Security Group) rules should be configured with the following rules
    - Bastion hosts will allow management connection only from Capital Goods internal network. And all of the other hosts will only allow management connections from the bastion host.
    - The web hosts will allow traffic only from the ELB(ALB) on port 80 and 443 for web requests from source being the ALB Security Group ID. And SSH/22 access through the Bastion Host (IP)
    - Application hosts will only allow application port 80 and 443 traffic connections from the Internal Proxy/Load Balancer **Static Internal IP** or you could make use of Security Group referencial. (Check with the developers if in doubt) and SSH/22 access through the Bastion Host (IP)

        - The RDS(MySQL) instance will only allow database connections from port 3306 from the application hosts
    - In addition, monitoring and logging; alerts and notifications for critical events should be configured. Please refer to our security standard document for more details.
- Application Security
    - Implement AWS WAF
    - Secret Manager
    - And AWS Shield
    - AWS Trusted Adviser
    - AWS Service Catalog for the developers (create products)
    - CloudWatch
    - AWS Lambda (Automation)