

Capital Goods: Ventura Developer's Sandbox Environment Build Requirement Definition Document (RDD)

Hello Boris,

As discussed today on the 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.
- Ventura is a 3-tier E-commerce application and the following infrastructure would need to be stood up for the sandbox environment for all the application developers that'll be part of this project (sandbox), however there are 5 environments in total that makes up the entire environment build and that'll be developers Sandboxes, Dev, UAT, Prod and DR.
- For the developers sandboxes please use the below requirements and resource inclusions for the infrastructure build. This RDD is strictly meant for standing up the individual sandbox environments for each developer. Please refer to the other RDDs of the other environments for their own specific requirements.
- At this point there are two developers in the environment and their names are James and George.
- For the Sandbox VPC Network, please assign different subnet resources to the individual developers (EC2 VM/Instance and SQL Database subnets). Also implement all necessary governance practices and security guidelines to avoid resource/environment compromise.
 - 1 EC2 instance for the developer
 - 1 RDS instance using MySQL-engine
 - S3 bucket to host all application related logs for more scrutoning and scrubbing.
 - Region: us-east-1

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

Confluence Pages:

a. Developer's VM Instance (Sandbox)

Number of instances	OS	Instance Type	Primary Volume Size	Installations + Configurations	Comments
1	CentOS 7	t2-micro	General Purpose (Balanced PD) 50GB	Apache (httpd) Tenable Shorewall Crowdstrike Cloud Watch Agent AD Join SELinux Disabled	1. Follow our resource naming standards which will be "ventura-sandbox"-resourcename" <ul style="list-style-type: none">- application id: dmt468- owner: developers-name- environment: sandbox- budget code: cost-sandbox- patch group: pg-sandbox- compliance classification: nist- data classification: pii- LOB: e-commerce- project manager: alexander-dirus- project name: ventura-project- region: us-us-east-1

b. RDS(MySQL) Instance (Sandbox)

Number of instances	Engine	Instance Type (MT)	Multi AZ (Y/N)	Storage Size (PD)	Template	Comments
1	MySQL	db.m5d.large (2vCPU, 8Mem)	N	General Purpose: 100GB	As per environment	1. Following our resource naming standards which will be "ventura-sandbox"-resourcename"

c. All resources within the Individual Developer's Sandbox Project/Environment must have the below mandatory labels

						2. Add all our mandatory and strongly recommended labels (<ul style="list-style-type: none"> - application id: dmt468 - owner: developers-name - environment: sandbox - budget code: cost-sandbox - patch group: pg-sandbox - compliance classification: nist - data classification: pii - LOB: e-commerce - project manager: alexander-dirus - project name: ventura-project - region: us-east-1
--	--	--	--	--	--	---

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
 - Object Lifecycle

Additional Notes:

- As shown on the architecture, application availability will be achieved by having 2 availability zone (A & B) at every time.
- On security:
 - In the application, only the web hosts could be publicly facing. The application and RDS(MySQL) instances must be Private
 - Firewall(SG) rules should be configured with the following rules
 - The “developer vm instance” will allow internet traffic on port 80 and 443 for web requests with source 0.0.0.0/0. And SSH/22 access through developer’s network(IP)
 - The RDS(MySQL) instances will only allow database connections from port 3306 from the application hosts

d) Network Environment (Sandbox)

Below one shows the CIDR details and IP Subnets for non-prod environment (Sandbox)

Proposed Sandbox VPC/Subnet environment - VPC IP address/CIDR 10.10.0.0/16						
Subnet Name	Type	AZs	Usage	CIDR	Total Ips	Network IP's
Ventura-Sandbox-Subnet1	Public	us-east-1a	James EC2 VM	/28	11	10.10.1.0
Ventura-Sandbox-Subnet2	Private	us-east-1a	James RDS DB	/28	11	10.10.5.0
Ventura-Sandbox-Subnet3	Public	us-east-1a	George EC2 VM	/28	11	10.10.10.0
Ventura-Sandbox-Subnet4	Private	us-east-1a	George RDS DB	/28	11	10.10.15.0
Ventura-Sandbox-Subnet5	Private	us-east-1a	Free	/28	11	10.10.20.0
Ventura-Sandbox-Subnet6	Private	us-east-1a	Free	/28	11	10.10.25.0
Total IPs					66	