**CareGem Infrastructure Deployment Guide**

# Document Purpose

The purpose of this document is to provide detail instructions to setup CareGem healthcare application onto the AWS Cloud.

# Prerequisite

The following are the prerequisites for the setup

1. Admin access to the AWS account where setup needs to be completed.
2. Access to the below Cloud Formations:
   1. admin-portal-s3.yml
   2. cloudfront-distribution-admin-portal.yml
   3. cloudfront-distribution-org-portal.yml
   4. cloudfront-distribution-patient-portal.yml
   5. cloudfront-origin-access-identity.yml
   6. cognito-identity-pool.yaml
   7. cognito-user-pool.yaml
   8. lambda-role.yml
   9. org-portal-s3.yml
   10. paitent-portal-s3.yml
   11. policy-dynamodb-table.yaml
   12. rds.yaml
   13. s3-for-logs.yml
   14. user-dynamodb-table.yaml
   15. vpc-setup.yml

# Setup Instructions

The CareGem application requires the below AWS services. The services must be configured in the given sequence only.

## Register Domain

The 1st step in the setup is to acquire a new domain. Here are steps to request new domain using AWS Route 53 service.

1. Sign in to the AWS Management Console and open the Route 53 console at <https://console.aws.amazon.com/route53/>.
2. If you're new to Route 53, choose **Get started**.

If you're already using Route 53, in the navigation pane, choose **Registered domains**.

1. Choose **Register domain**, and specify the domain that you want to register:
   1. Enter the domain name that you want to register, and choose **Check** to find out whether the domain name is available.
   2. If the domain is available, choose **Add to cart**. The domain name appears in your shopping cart.

The **Related domain suggestions** list shows other domains that you might want to register instead of your first choice (if it's not available) or in addition to your first choice. Choose **Add to cart** for each additional domain that you want to register, up to a maximum of five domains.

* 1. In the shopping cart, choose the number of years that you want to register the domain for.
  2. To register more domains, repeat steps 3a through 3c.

1. Choose **Continue**.
2. On the **Contact Details for Your** *n* **Domains** page, enter contact information for the domain registrant, administrator, and technical contacts.

Note: Once the domain is validated in will appear in registered domain tab. The domain registration sometime requires 24 hours to validate your domain.

Graphical user interface, text, application, email

Description automatically generated

## Create Sub Domains

We also need to create subdomains for the **Admin** and **Org Portal** applications.

Sub Domains to be added: (the given domain(s) name is for staging environment. Update production domain accordingly during the production deployment)

1. caregemstg.com -> primary domain
2. admin.caregemstg.com -> subdomain for ‘admin portal’
3. org.caregemstg.com -> subdomain for ‘org portal’

Steps to add Sub Domain **admin.caregemstg.com**:

1. Create a hosted zone for admin.caregemstg.com
   1. Open the [Route 53 console](https://console.aws.amazon.com/route53/).
   2. In the navigation pane, choose Hosted zones.
   3. Choose Create hosted zone.
   4. In the right pane, enter the name of the subdomain: **admin.caregemstg.com**
   5. For Type, accept the default value of Public hosted zone.
   6. Choose Create hosted zone.
2. Expand the Hosted zone details dropdown list for the subdomain in the hosted zone (admin.caregemstg.com). In the right pane, copy the names of the four servers listed as the Name servers under Hosted zone details.
3. Add NS record to in primary domain (caregemstg.com) to route traffic to the subdomain (admin.caregemstg.com)
   1. Select the hosted zone for the domain (caregemstg.com). Be sure not to select the name of the subdomain (admin.caregem.com).
   2. In the hosted zone for the domain, choose Create record.
   3. For Name, enter the name of the subdomain (admin.caregemstg.com) .
   4. For Value, enter the names of the name servers.
   5. For Record type, choose NS - Name servers for a hosted zone.
   6. For TTL (Seconds), select a more common value for an NS record, such as 172,800 seconds.
   7. For Route Policy, choose Simple routing.
   8. Choose Create Records.

Steps to add Sub Domain **org.caregemstg.com**:

1. Create a hosted zone for admin.caregemstg.com
   1. Open the [Route 53 console](https://console.aws.amazon.com/route53/).
   2. In the navigation pane, choose Hosted zones.
   3. Choose Create hosted zone.
   4. In the right pane, enter the name of the subdomain: **org.caregemstg.com**
   5. For Type, accept the default value of Public hosted zone.
   6. Choose Create hosted zone.
2. Expand the Hosted zone details dropdown list for the subdomain in the hosted zone (admin.caregemstg.com). In the right pane, copy the names of the four servers listed as the Name servers under Hosted zone details.
3. Add NS record to in primary domain (caregemstg.com) to route traffic to the subdomain (admin.caregemstg.com)
   1. Select the hosted zone for the domain (caregemstg.com). Be sure not to select the name of the subdomain (org.caregem.com).
   2. In the hosted zone for the domain, choose Create record.
   3. For Name, enter the name of the subdomain (org.caregemstg.com) .
   4. For Value, enter the names of the name servers.
   5. For Record type, choose NS - Name servers for a hosted zone.
   6. For TTL (Seconds), select a more common value for an NS record, such as 172,800 seconds.
   7. For Route Policy, choose Simple routing.
   8. Choose Create Records.

Graphical user interface, text, application

Description automatically generated

## Acquire New Certificate

The next step is to get certificate for the newly created domain. We also need to add subdomains to the below subdomains to the certificate that we will be using in the later stage of the deployment.

Domains to be added: (the given domain(s) name is for staging environment. Update production domain accordingly during the production deployment)

1. caregemstg.com -> primary domain
2. admin.caregemstg.com -> subdomain for ‘admin portal’
3. org.caregemstg.com -> subdomain for ‘org portal’

Steps to request new SSL certificate:

1. Go to **AWS Certificate Manager** and click on **Request a certificate** button
2. Click **Next**
3. Add below domains:
   1. caregemstg.com
   2. admin.caregemstg.com
   3. org.caregemstg.com
4. Note: - Kindly note, sometimes it takes a couple of hours to update certificate status to **Issued**. The certificate can only be used when status changes to **Issued**. Amazon verifies your claim on the domain that was provided while requesting the certificate.

## VPC Setup

Execute the below cloud formation to create VPC and the corresponding subnets. The CFT will primarily create following resources

1. Two (2) Public Subnets – Hosts jumpbnox
2. Two (2) Private Subnets – Hosts Lambda Functions
3. Two (2) DB Subnets – Hosts Database Instance
4. NAT Gateway – Attached to private subnets
5. Internet Gateway – Attached to public subnets

Once the cloud formation successfully executed. Go to the **Outputs** section of the template to verify if all the above-mentioned resources are provisioned.

Graphical user interface, application, email

Description automatically generated

## Setup RDS

1. Edit rds.yaml and update the following parameters before running the CloudFormation
   1. **DatabaseName:** CareGemDB
   2. **DatabaseUser:** dbadmin
   3. **DatabasePassword:**
   4. **DatabaseSize:** 10 (change as needed for production deployment)
   5. **DatabaseInstanceClass:** db.t2.small (change as needed for production deployment)
   6. **VPC:** <<VPC ID that was created in the previous step)
   7. **DBSubnets:** <<List of DB Subnets that was created in the previous step)
   8. **EnvironmentName:** qa / prd

Graphical user interface, text, application, email

Description automatically generated

## Setup jumpbox

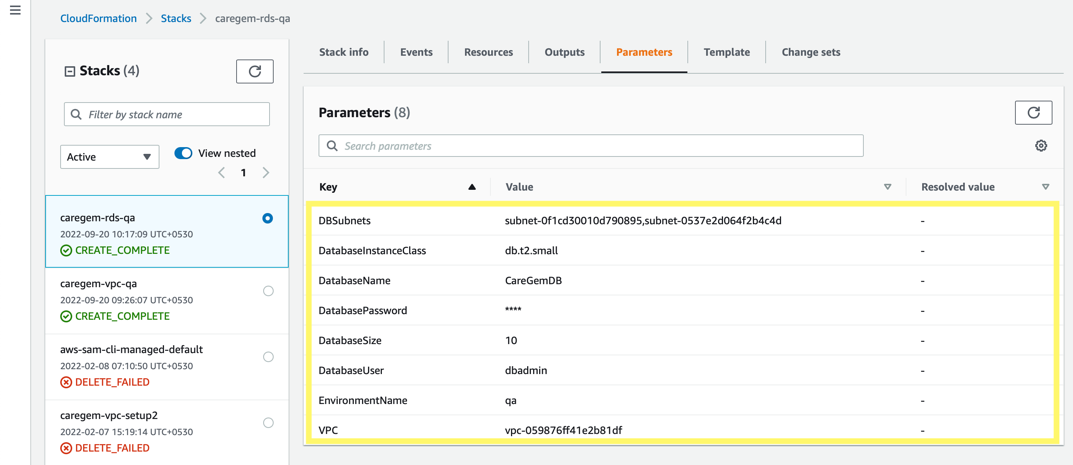
1. Go to EC2 dashboard and click on Launch Instances
2. On **Quick Start** tab click on **Windows**
3. For **Instance Type** select Image with AMI ID **ami-09893189de3a034b4**
4. In **Key Pair** section click on **Create new key pair**
5. Enter key name as ‘caregem-qa-ec2-key’ and click **Create key pair**
6. Store created key-pair in some secure place.
7. For Windows instances, this key pair will be used to decrypt the administrator password which can be used to connect to the instance.
8. Edit **Network Settings** sectionas below

* VPC -> VPC Id, created in section #3.4
* Subnet -> Public Subnet-1, created in section 3.4
* Auto-assign public ip ->Enable
* Security Group -> Existing security group i.e. EC2 Security Group created in section #3.5

**Graphical user interface, text, application, email

Description automatically generated**

1. For **Configure storage**, update below configuration and then click **Launch instance**



## Dynamo DB Setup

## Execute the below cloud formation to create DynamoDB tables.

## policy-dynamodb-table.yaml -> creates Policy table

## user-dynamodb-table.yaml -> creates User table

1. user-connections-table.yaml -> creates user\_connections table
2. user-exceptions-dynamodb-table.yaml -> create user\_exceptions table
3. user-changelog-dynamodb-table.yaml -> create user\_pii\_hist table

## Systems Manager Parameter Store Setup

Execute the below cloud formation to create systems manager parameters

* ssm-parameter-store.yml

## Secret Manager Setup

Execute the below cloud formation to create secrets manager secrets

* secrets-manager.yml

Secret value for SFTP & CDS billing secret value must be updated

## API Gateway CloudWatch log group and role

Execute the below cloudformation to create API Gateway CloudWatch log group and role

* api-gateway-access-logs.yml

## Amazon Chime setup

1. Create an Amazon Chime Voice Connector
2. Open the Amazon Chime console at <https://chime.aws.amazon.com/>.
3. For **Calling**, choose **Voice connectors**.
4. Choose **Create new voice connector**.
5. For **Voice connector name**, enter a name for the Amazon Chime Voice Connector.
6. (Optional) For **AWS Region**, choose an AWS Region for your Amazon Chime Voice Connector. The default Region is US East (N. Virginia) (**us-east-1**). Regions cannot be changed after your Amazon Chime Voice Connector is created.
7. For **Encryption**, select **Enabled**.
8. Choose **Create**.
9. Provision phone number
10. Open the Amazon Chime console at <https://chime.aws.amazon.com/>.
11. For **Calling**, choose **Phone number management**.
12. Choose **Orders**, **Provision phone numbers**.
13. Select **Voice Connector**
14. Search for available phone numbers by country and other location options. Select the phone numbers that you want, then choose **Provision**.
15. The phone numbers appear in your **Orders** and **Pending** lists while the provisioning occurs.
16. When provisioning completes, the phone numbers appear in your **Inventory**, and you can assign them to individual users.
17. Update the parameter value of /caregem/ChimePSTNNumber with newly provisioned phone number.

## Deploy IAM Policies

Execute below cloudformation to create IAM Role for Lambda

* lambda-role.yml

## SES Setup

Create domain identity

1. Sign in to the AWS Management Console and open the Amazon SES console at <https://console.aws.amazon.com/ses/>.
2. In the navigation pane, under **Configuration**, choose **Verified identities**.
3. Choose **Create identity**.
4. Under **Identity details**, select **Domain** as the type of identity you want to create. You must have access to the domain’s DNS settings to complete the domain verification process.
5. Enter the name of the domain or subdomain in the **Domain** field.
6. Under **Verifying your domain**, expand **Advanced DKIM settings** and choose **Easy DKIM**
7. In the **DKIM signing key length** field, choose RSA\_2048\_BIT
8. Check the checkbox for **Publish DNS records to Route53**
9. Ensure that the **Enabled** box is checked in the **DKIM signatures** field.
10. Choose **Create identity**.

Create email identity

1. Sign in to the AWS Management Console and open the Amazon SES console at <https://console.aws.amazon.com/ses/>.
2. In the navigation pane, under **Configuration**, choose **Verified identities**.
3. Choose **Create identity**.
4. Under **Identity details**, choose **Email address** as the identity type you want to create.
5. For **Email address**, enter the email address that you want to use. The email address must be an address that’s able to receive mail and that you have access to.
6. To create your email address identity, choose **Create identity**. After it's created, you should receive a verification email within five minutes. The next step is to verify your email address by following the verification procedure in the next section.

Method to verify email identity

1. Publish an MX record to Route53 Hosted Zone for caregemstg.com
   1. Set Record name: caregemstg.com
   2. Set Record type: MX – Specifies mail servers
   3. Set Routing policy: Simple routing
   4. Set Value: 10 inbound-smtp.us-east-1.amazonaws.com
   5. Set TTL : 1800 seconds
2. Follow this [blog](https://levelup.gitconnected.com/easily-create-email-addresses-for-your-route53-custom-domain-589d099dd0f2#:~:text=New%20Email%20Address-,In%20the%20AWS%20console%2C%20navigate%20to%20SES%20%3E%20Identity%20Management%20%3E,%2Dreply%40example.com).

## AWS Cognito User Pool Setup

## Execute the below cloud formation to create AWS Cognito User Pool.

## **CFT Name:** cognito-user-pool.yaml

Execute SAM template for cognito-trigger to create lambda triggers

* Pre-authentication lambda trigger: Pre-Auth-Lambda
* Post-authentication lambda trigger: Post-Auth-Lambda
* Custom message lambda trigger: Cognito-Triggered-Email-Lambda

## AWS Cognito Identity Pool Setup

## Execute the below cloud formation to create AWS Cognito Identity Pool.

## **CFT Name:** cognito-identity-pool.yaml

## Deploy Custom Authorizer

## This deployment is separately done by the development team. Raj to update deployment steps for this section.

1. Execute SAM template for auth-service to create API Gateway custom authorizer
2. Update /caregem/AuthorizerLambdaArn SSM Parameter

## 

## Deploy APIs

This deployment is separately done by the development team. Raj to update deployment steps for this section.

* Open build\_deploy.sh
* For sam deploy command Replace SAM\_CLI\_SOURCE\_BUCKET variable with bucket name
* For sam deploy add aws profile for environment (dev/staging/prod)
* Execute build\_deploy.sh to deploy APIs

## CloudFront Origin Access Identity Setup

Execute the below CFT to create the CloudFront Origin Access Identity. The same identity will be used by CloudFront(s) to access the Origin S3 buckets.

## **CFT Name:** cloudfront-origin-access-identity.yml

## S3 Setup

Execute the below CFTs in given order

## s3-for-logs.yml

## paitent-portal-s3.yml

## admin-portal-s3.yml

## org-portal-s3.yml

## 

## CloudFront Setup

Execute the below CFTs in given order

1. cloudfront-distribution-patient-portal.yml
2. cloudfront-distribution-org-portal.yml
3. cloudfront-distribution-admin-portal.yml

## Update SSM Parameter Store and Secrets Manager Secrets

**SSM Parameter Store**

Run update Cloudformation stack and update values of all the parameters

1. /caregem/AccessLogArn -> StackOutput from 3.10
2. /caregem/ApiKeys -> path to secret
3. /caregem/BillingCDSSecret -> path to secret
4. /caregem/CaregemS3Config -> caregem-config prod s3 bucket
5. /caregem/ChimeInstanceArn -> Chime Instance ARN
6. /caregem/VpcSg -> VPC Security Group. Stack Output from 3.4
7. /caregem/VpcSubnet -> Private Subnets. Stack Output from 3.5
8. /caregem/WebSocketURL -> Web Socket URL.

**Secrets Manager**

Run update Cloudformation stack and update values of all the key-value secrets

## DNS Update

### New DNS record for **caregemstg.com** domain

1. Go to Route 53 Dashboard
2. Click on **Hosted zones**
3. Click on **caregemstg.com**
4. Click on **Create record** and update below parameters
   1. **Record name:** ->keep empty
   2. **Record Type** -> A
   3. **Alias –** Toggle Yes
   4. **Route traffic to** -> Route traffic to CloudFront distribution
   5. **Routing policy** - > Simple routing

### New DNS record for **admin.caregemstg.com** domain

1. Go to Route 53 Dashboard
2. Click on **Hosted zones**
3. Click on **admin.caregemstg.com**
4. Click on **Create record** and update below parameters
   1. **Record name:** ->keep empty
   2. **Record Type** -> A
   3. **Alias –** Toggle Yes
   4. **Route traffic to** -> Route traffic to CloudFront distribution
   5. **Routing policy** - > Simple routing

### New DNS record for **org.caregemstg.com** domain

1. Go to Route 53 Dashboard
2. Click on Hosted zones
3. Click on org.caregemstg.com
4. Click on Create record and update below parameters
   * 1. **Record name:** ->keep empty
     2. **Record Type** -> A
     3. **Alias –** Toggle Yes
     4. **Route traffic to** -> Route traffic to CloudFront distribution
     5. **Routing policy - > Simple routing**

**Caregem migrations**

# Prerequisite

# Migration instructions

## Export MySQL databases to self-contained files

* 1. Connect to GCP prod RDP client using Microsoft Remote Desktop (or similar software)
  2. Connect to Carex VPN using OpenVPN
  3. Create a database connection to Carex DB on MySQL workbench
  4. Go to Administration > Data export.
  5. Select schema to export.
  6. Under Export Options select Export to Self-Contained File
  7. Click Start Export
  8. Do steps 5-7 for all 3 DB schemas – mlprep-uat, mlprep\_qa and carex-uat

## Cleanup MySQL dump files

* 1. Remove following lines
     1. Line 17 - SET @MYSQLDUMP\_TEMP\_LOG\_BIN = @@SESSION.SQL\_LOG\_BIN;
     2. Line 18 - SET @@SESSION.SQL\_LOG\_BIN= 0;
     3. Line 24 - SET @@GLOBAL.GTID\_PURGED=/\*!80000 '+'\*/ '51f2bc8e-f46e-11e6-a24e-42010a800557:1-110026663';
     4. SET @@SESSION.SQL\_LOG\_BIN = @MYSQLDUMP\_TEMP\_LOG\_BIN;
  2. Run sed -i -e 's/DEFINER=`sachin`@`%`/DEFINER=`dbadmin`@`%`/g' Dump20221121\_carex\_uat.sql

## Create MySQL DB schemas

* 1. Download AWS prod jumpbox remote desktop file
  2. Retrieve jumpbox password using EC2 key-pair obtained from deployment setup step 3.6.6
  3. Connect to jumpbox RDS client
  4. Open Server Manager > Local Server
  5. Under Properties. Set IE Enhanced Security Configuration Off
  6. Download Chrome and MySQL Workbench
  7. Create a database connection to Prod Caregem using MySQL Workbench
  8. Go to Administration > Data Import/Restore
  9. Under Import Options > Select Import from Self-Contained File
  10. Under Default Schema to be Imported To > Select Default Target Schema with DB schema name corresponding to .sql dump file
  11. Do steps 8-10 for all 3 DB mlprep-uat, mlprep\_qa and carex-uat

## Migrate users from TrueVault to Cognito User Pool and DynamoDB tables

* 1. Set .env file for migration\_scripts with correct environment variables
  2. Execute python -i .\migrate\_user.py → main() method
  3. Execute db\_scripts.sql from migration scripts
     1. From Line 1 – 147 for carex\_uat database
     2. From Line 148 – 244 for mlprep-uat database
  4. Set database trigger for survey\_vital table in mlprep DB
  5. Validate device\_pairing view set correctly else copy it from migration\_scripts/views.sql
  6. Add below line to all analytics and normalized views

`s`.`patient\_internal\_id` AS `internal\_id`. For view named analytics\_lightheadness add this instead

`mlprep-uat`.`analytics\_lightheadedness`.`internal\_id` AS `internal\_id`

* 1. Execute python -i .\deleted\_user\_with\_internal\_id.py
  2. Execute python -i .\networks\_with\_internal\_id.py
  3. Execute python -i .\survey.py
  4. Execute python -i .\update\_hash\_patient.py
  5. Execute python - .\create\_user\_cognito.py
  6. Execute python -i .\change\_log\_back\_up.py