亚马逊云科技
快速部署电商独立站解决方案
指导手册

2022 年 06 月

声明

本手册的目的在于帮助用户快速了解如何使用 快速部署电商独立站 解决方案， 完成解决方案的配置、部署、验证、使用。解决方案基于亚马逊云科技云服务，使用开源项目社区版 Odoo

(Odoo 致力于为企业管理提供高效智能的开源解决方案，是全球业内高速成长的软件服务商之一，逾七百五十万用户选择 Odoo 进行数字化升级。通过一系列全业务链覆盖、高度集成、简单易用的商业应用，助力企业实现信息化改革、降本增效并释放公司增长潜力)。

使用区域

您可以使用该解决方案的亚马逊云科技区域为：
ap-northeast-1 / ap-northeast-2 / ap-southeast-1 / ap-southeast-2 / eu-central-1 / sa-east-1 / us-east-1 / us-east-2 / us-west-1 / us-west-2

预期费用

您需要在您的 AWS 账户中运行此解决方案时所使用的 AWS 服务的成本支付费用。截至发布之日，按计划中的完成部署单日基准成本应为：

- S3 ： < 0.1 $
- EC2： < 5 $
- EKS： < 1 $
- RDS < 3 $
- ElasticCache < 2 $
- EFS < 0.1 $
- ELB < 1 $
- VPC < 1 $

部署建议

使用成本管理标签：我们建议您无论何时创建云资源，都对其进行标记。请您尝试在实验期间为实验资源设置统一的标记字段，例如项目：OdooSolution

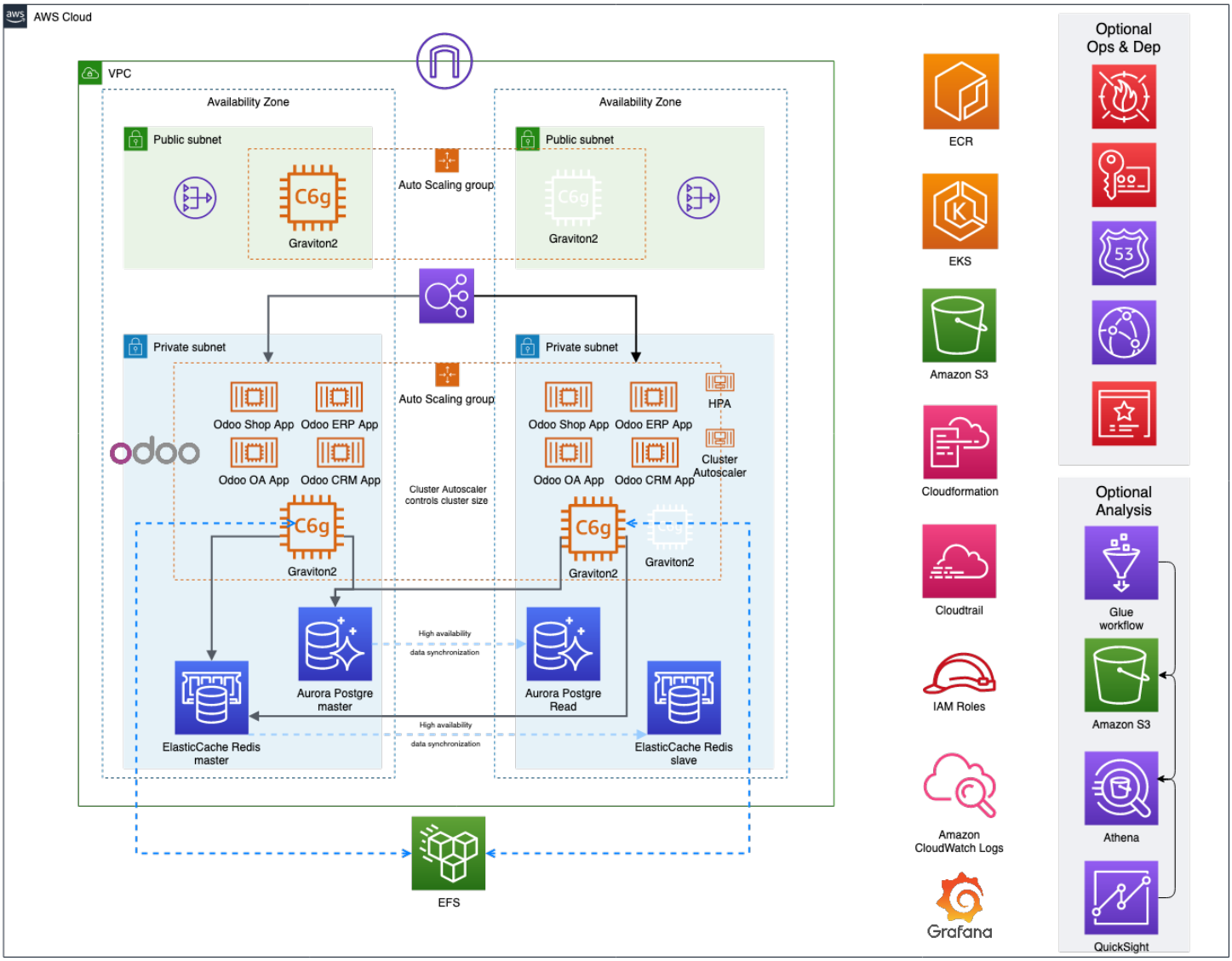
目录

解决方案介绍

部署架构图

- 我们已将一些流行技术运用到解决方案中，包括容器编排技术、缓存技术、数据库高可用技术、压力测试技术等。
- 我们将通过 cloudformation 部署解决方案，解决方案将使用流行的开源 ERP 软件 Odoo 作为端到端电商独立站应用示范，她将运行在 AWS EKS 环境中，RDS postgreSQL 作为默认的数据库层，ElasticCache Redis 存储 session 和缓存,EFS 和 S3 实现共享存储。以上架构在企业实际应用中常常被作为典型的应用负载框架广泛部署。兼顾弹性，稳定性，易用性，易维护性，并且所有实例节点基于 Graviton2 提供超高性价比

Graviton2 based Ecommerence Solution



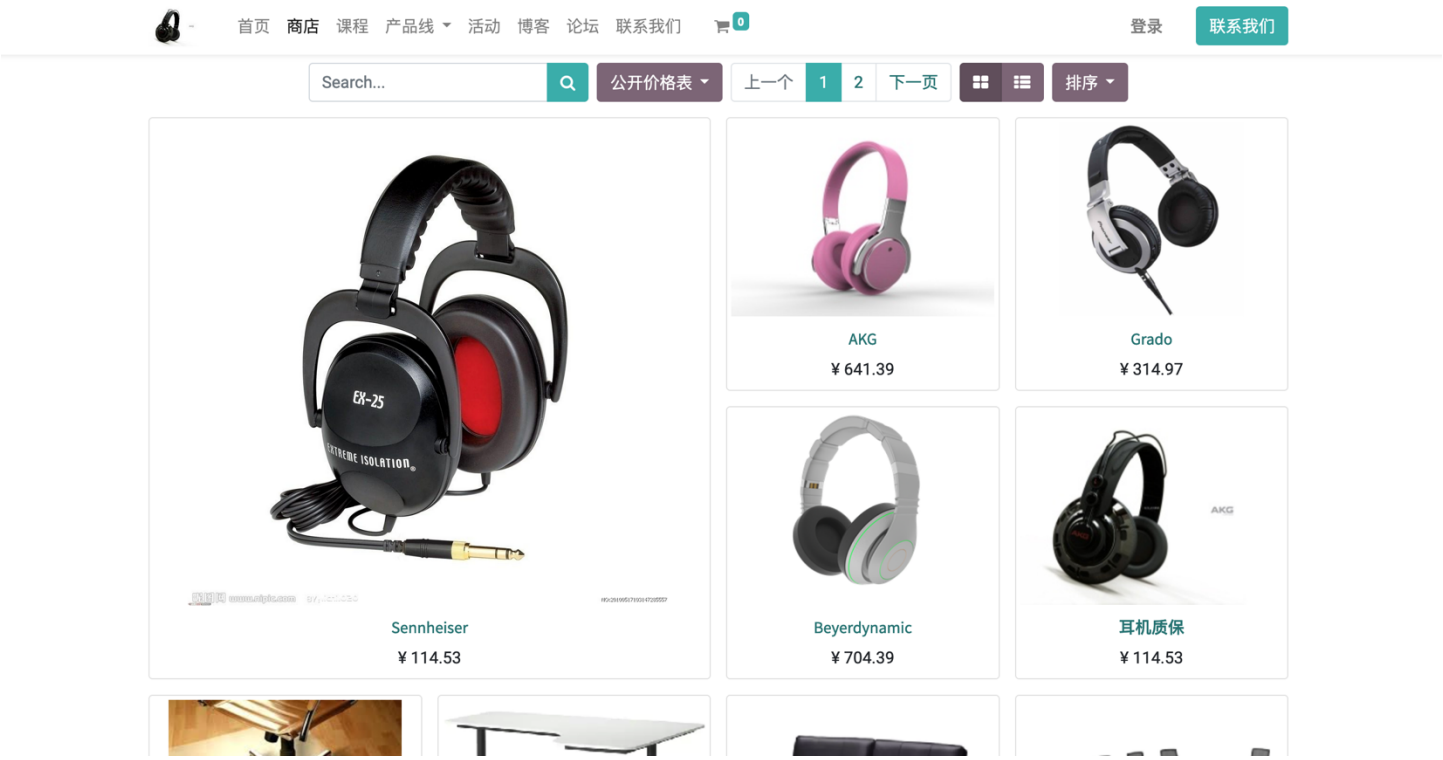
架构特点

在实验动手环节，我们将电商独立站工作负载的典型场景。逐步指导如何使用该解决方案建立电商独立站端到端的交付。解决方案已稳定、可靠、弹性、低成本的优良架构准生产系统为交付目标。

- 所有实例节点基于 Graviton2 提供超高性价比
- EKS+HAP+CA+ELB 作为弹性应用层
- Aurora postgreSQL 多副本的数据库层
- ElasticCache Redis 存储 session 和缓存
- EFS 和 S3 实现共享存储
- 使用 Cloudformation 传参 configmap 一键部署
- 可选 Glue Athena 等数据分析 workload 连接
- 可选 ACM ELB ssl 加密和卸载
- 可选使用 Spot 实例运行 EKS WorkNode

效果演示

[demo website]



资源清单

我们将使用 cloudformation 模板配置以下资源：

1. Amazon S3 存储桶，用于保存 ERP 或电商独立站静态数据数据。
2. IAM 角色，用于管理整套环境服务权限的 IAM 角色，以访问和供应其他 AWS 资源
3. 新建 VPC，包含两个公有子网、两个私有子网，Internet 网关和安全组以对外提供服务并支持安全访问控制。
4. 一台堡垒机 EC2 实例，创建将被放置在公有子网，对下游组件它将向架构前后端进行配置管理，对公网您可以配置只有您的本地 IP 地址可以与之通讯
5. EKS 集群和工作组，工作组将被放置在私有子网，运行 Odoo 模块化容器应用
6. 您可以自定义 Aurora postgreSQL 或 RDS postgreSQL 的多副本不同高可用级别和性能级别数据库层
7. 您可以自定义不同高可用级别和性能级别的 ElasticCache Redis 存储会话和缓存数据
8. 新建 EFS 共享存储，将共享存储 Odoo 应用中的静态文件。

部署前置条件

创建亚马逊云科技账号

我们建议您使用自己的 AWS 账户，但如果您目前没有 AWS 账户建议您联系专员开通一个国内实验账号，或是: 点击此处立即创建个人海外区账户

创建 IAM 用户或角色

- 拥有 AWS 账户后，创建一个具有以下权限的 IAM 用户或角色用于 Cloudformation 环境部署，他应该具备以下权限：
    - 增删改查 VPC
    - 增删改查 Amazon EC2, AWS ELB, AWS EFS
    - 增删改查 Amazon EKS 集群
    - 创建，读，写，删 Amazon S3 桶和对象
    - 创建，读，写，删 Amazon RDS
    - 创建，读，写，删 Amazon ElasticCache
    - 创建, 启动，删除 Amazon Cloudformation
    - Amazon CloudWatch

作为一般的安全最佳实践，您应该最小化小对上述服务的 IAM 权限，在实验过程中您也可以使用默认的管理员权限进行测试

- 实验将涉及启动 Cloudformation，在启动 cloudformation 模板之前，请确保您拥有一个 EC2 秘钥 在将运行模板的 AWS 区域中进行准备，以便模板中的资源与您的秘钥配对。（为方便后续实验的示范对应，在 workshop 中我们建议您将名字命名为 workshop）

如果您刚刚拿到 AWS Event Engine 账号，您可以通过 AWS Event Engine 控制台下载和使用 SSH Key。如果您使用新注册或自己的账号没有 SSH Key，您可以按照以下操作创建并下载一个

创建密钥对

打开 Amazon EC2 控制台 https://console.aws.amazon.com/ec2/

1，在导航窗格中的 NETWORK & SECURITY 下，选择 Key Pairs。

2，选择 Create key pair (创建密钥对)。

3，对于 Name (名称)，输入密钥对的描述性名称。为方便后续实验的示范对应，在 workshop 中我们建议您将名字命名为 workshop 。Amazon EC2 将公有密钥与您指定作为密钥名称的名称相关联。密钥名称最多可包含 255 个 ASCII 字符。它不能包含前导空格或尾随空格。

4，对于 File format (文件格式)，选择要保存私有密钥的格式。要以可与 OpenSSH 一起使用的格式保存私有密钥，请选择 pem。要以可与 PuTTY 一起使用的格式保存私有密钥，请选择 ppk。

5，选择 Create key pair (创建密钥对)。

6，您的浏览器会自动下载私有密钥文件。基本文件名是指定为密钥对名称的名称，文件扩展名由您选择的文件格式确定。将私有密钥文件保存在安全位置。 重要

ps：这是您保存私有密钥文件的唯一机会。

7，如果您将在 macOS 或 Linux 计算机上使用 SSH 客户端连接到您的 Linux 实例，请使用以下命令设置您私有密钥文件的权限，以确保只有您可以读取它。

chmod 400 workshop.pem

部署手册

使用 Cloudformation 部署电商独立站

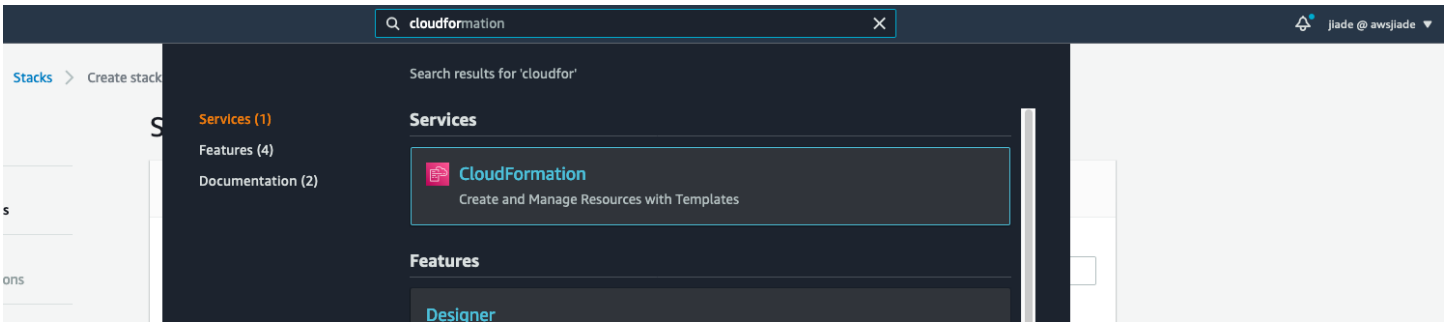
1.使用有效凭证登录 AWS 控制台

2.选择 AWS 区域。 此实验室的首选区域是 us-east-1。

- 您可以点击以下的 Launch Stack，这样将直接跳转到首选区域的堆栈创建页面

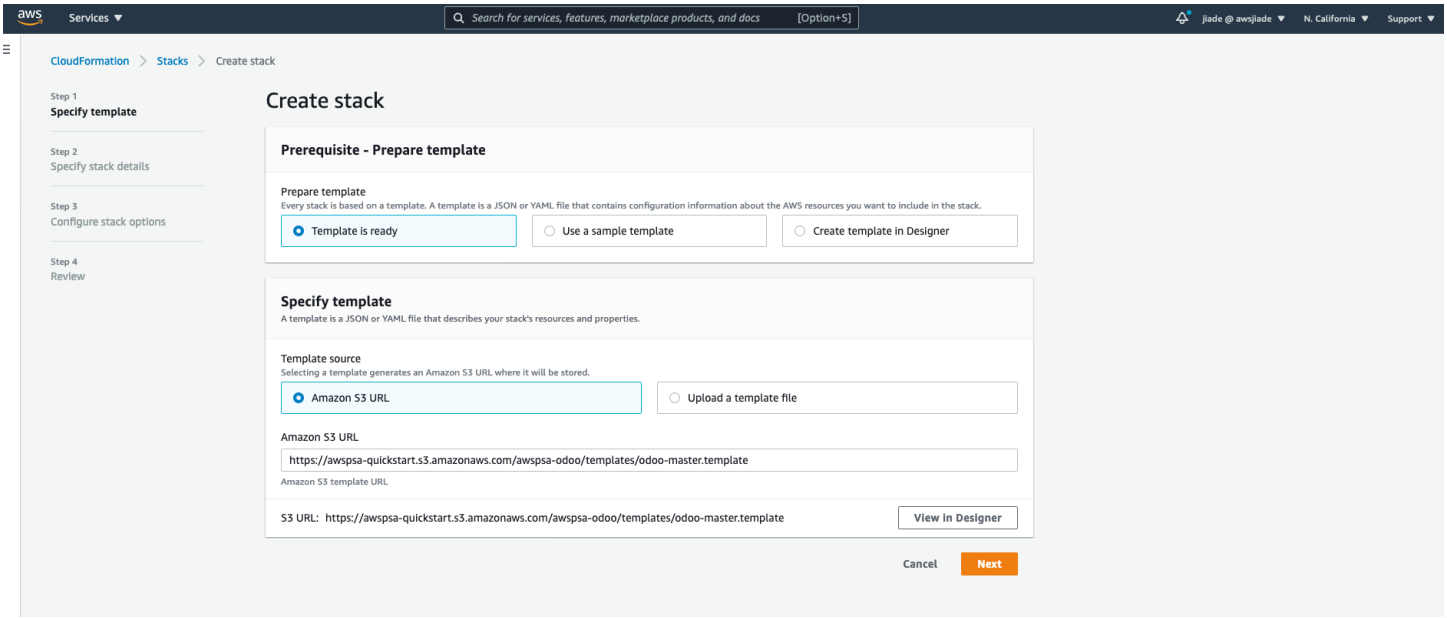
账户所属	实验模板
海外区域账户	Launch Stack

3.若您选择自定义的区域后，请导航到 cloudformation 服务控制台。

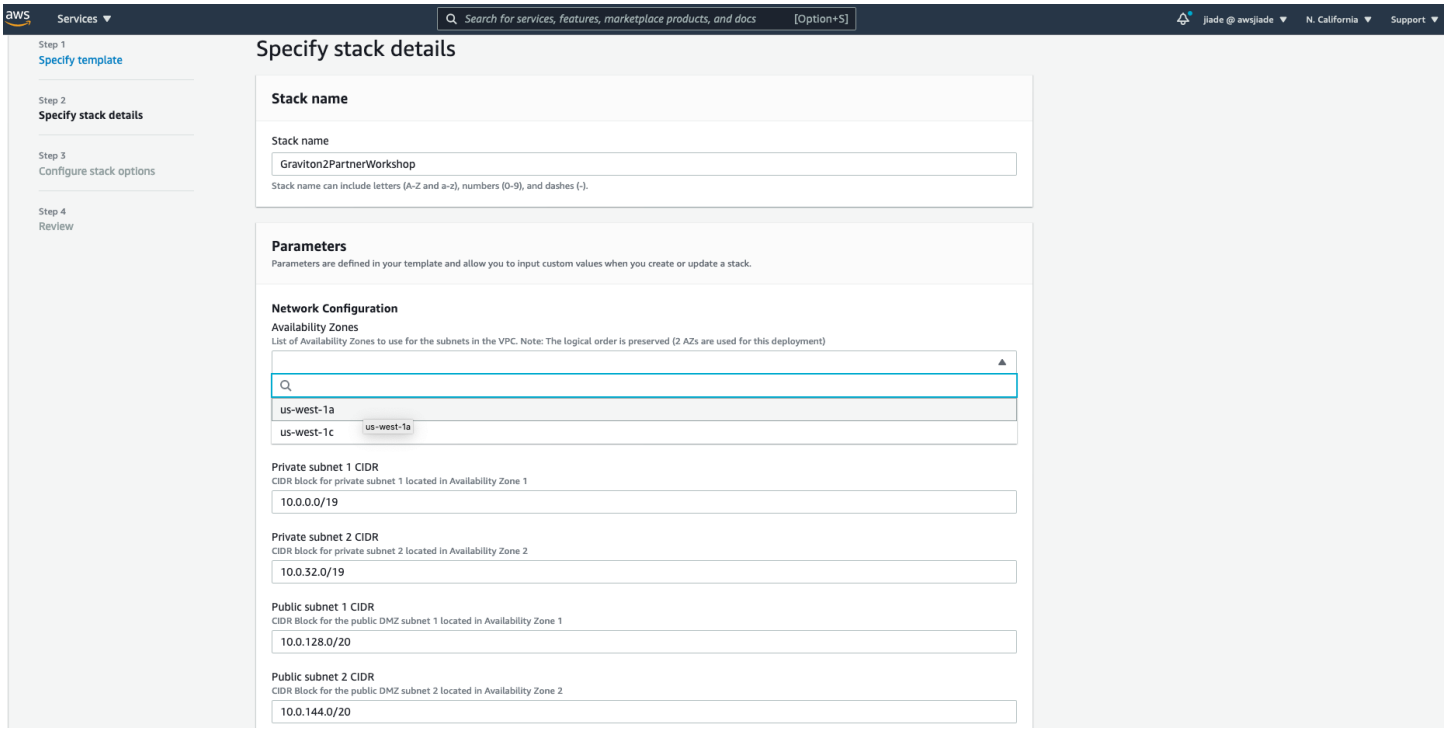


4.填写对应的堆栈 URL，单击“创建堆栈”。

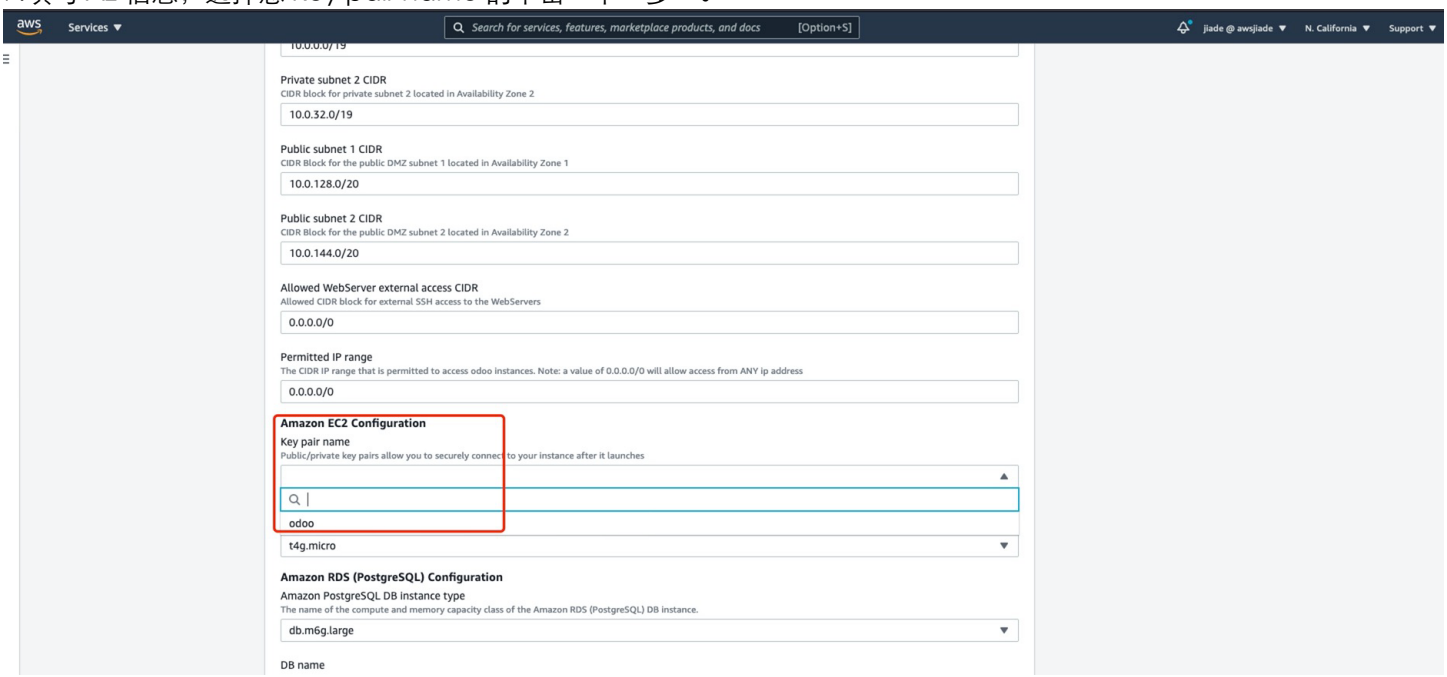
5.单击“启动堆栈”按钮以启动堆栈，然后单击“下一步”：



6.你可以自定义指定为 StackName，然后单击“下一步”。

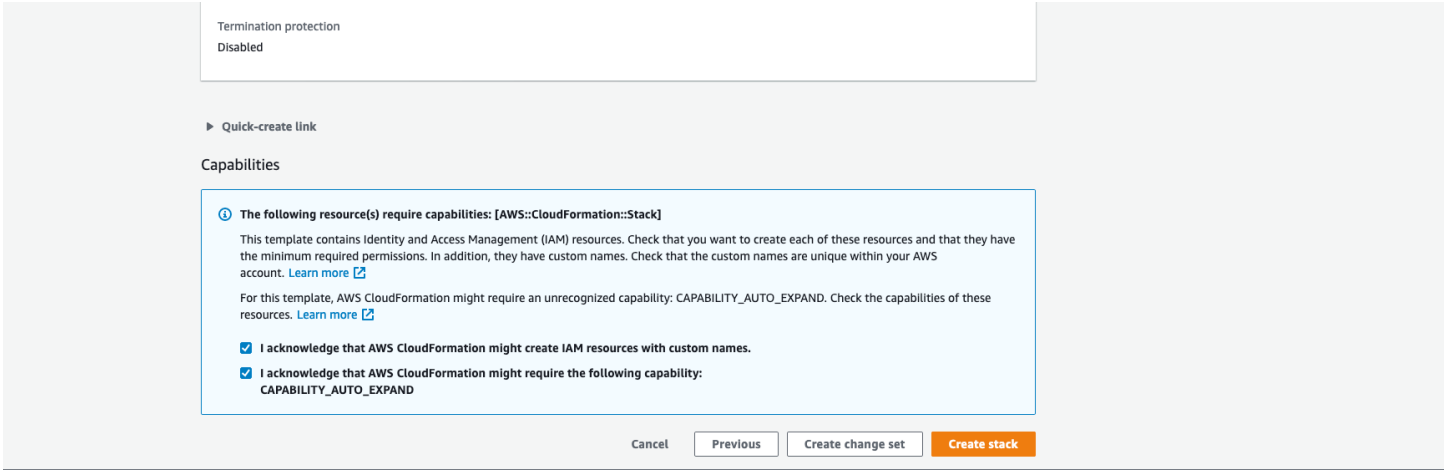


7.填写 AZ 信息，选择您 Key pair name 的单击“下一步”。



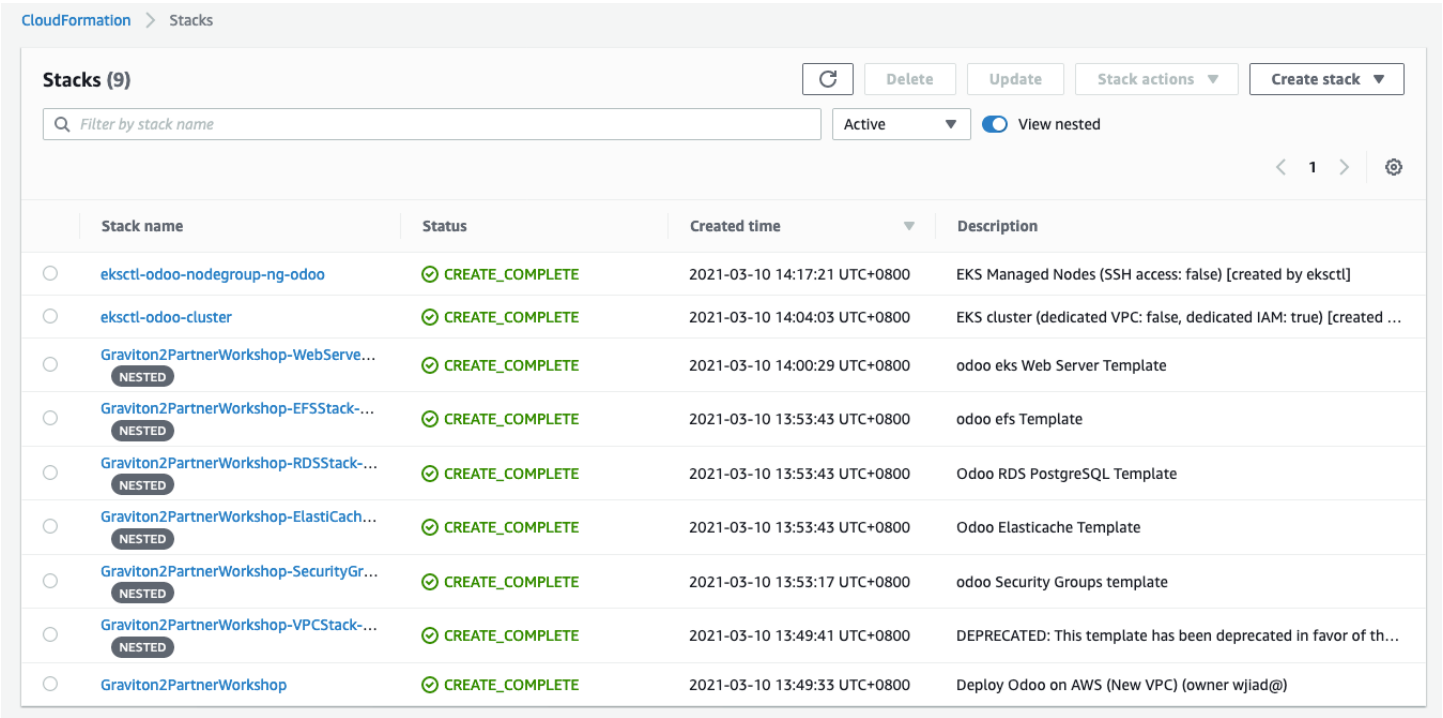
您也可以在其他的选项中配置您需要的架构，例如：postgreSQL、redis、堡垒机、EKS 的实例类型。RDS 的自动备份策略、是否多 AZ 部署、EKS 集群的节点数量，Odoo 的管理员密码，等等。

8.确认使用自定义名称创建 IAM 资源的权限，然后单击“创建”。

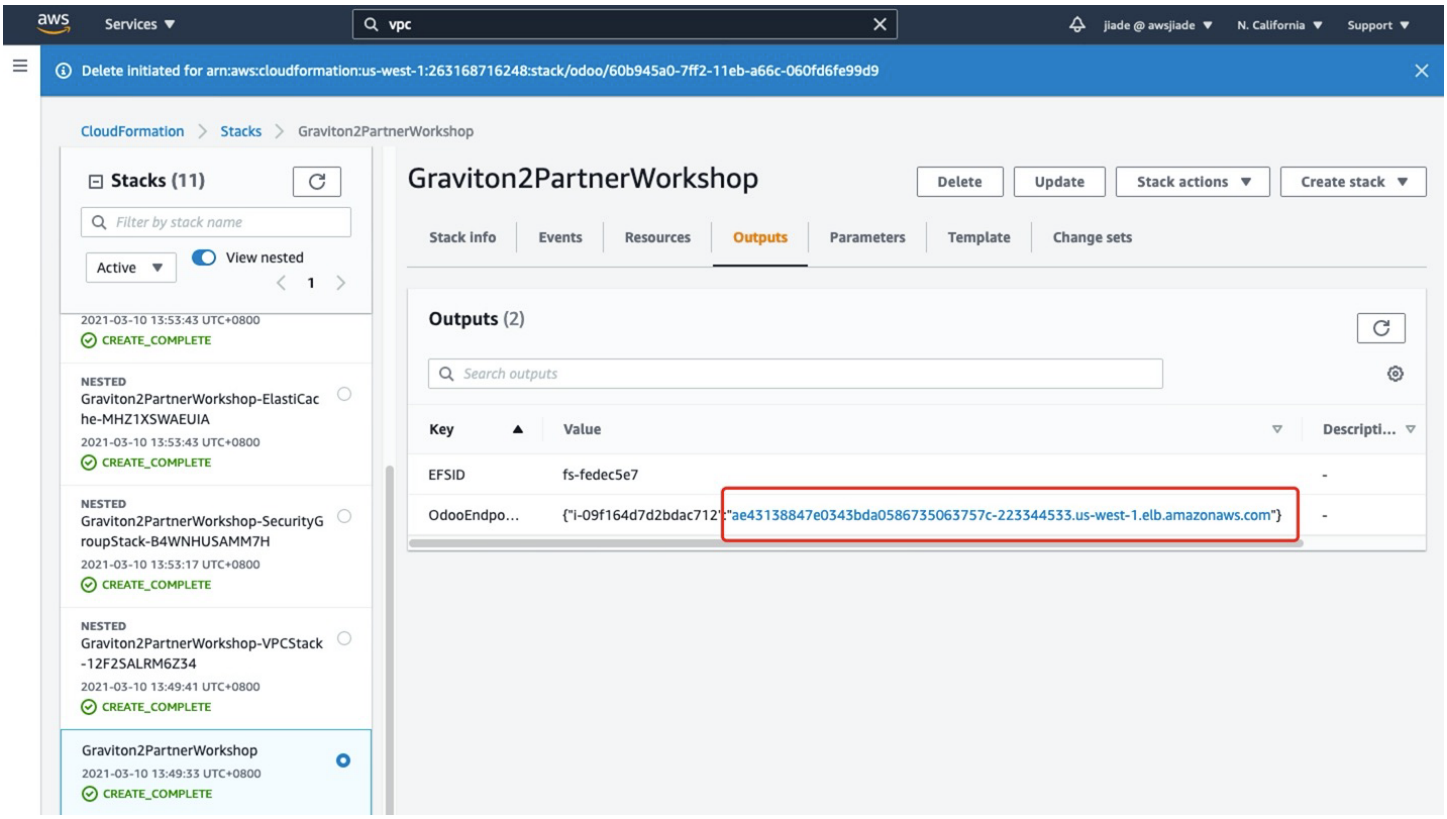


9.等待 cloudformation 供应所有资源。 大约需要 35 分钟才能完成执行

10.cloudformation 部署成功，包含 8 个内嵌 stack，主 stack 为 Graviton2PartnerWorkshop



11.点击 Graviton2PartnerWorkshop 进入 output，即可查看您 Odoo 应用的 URL。

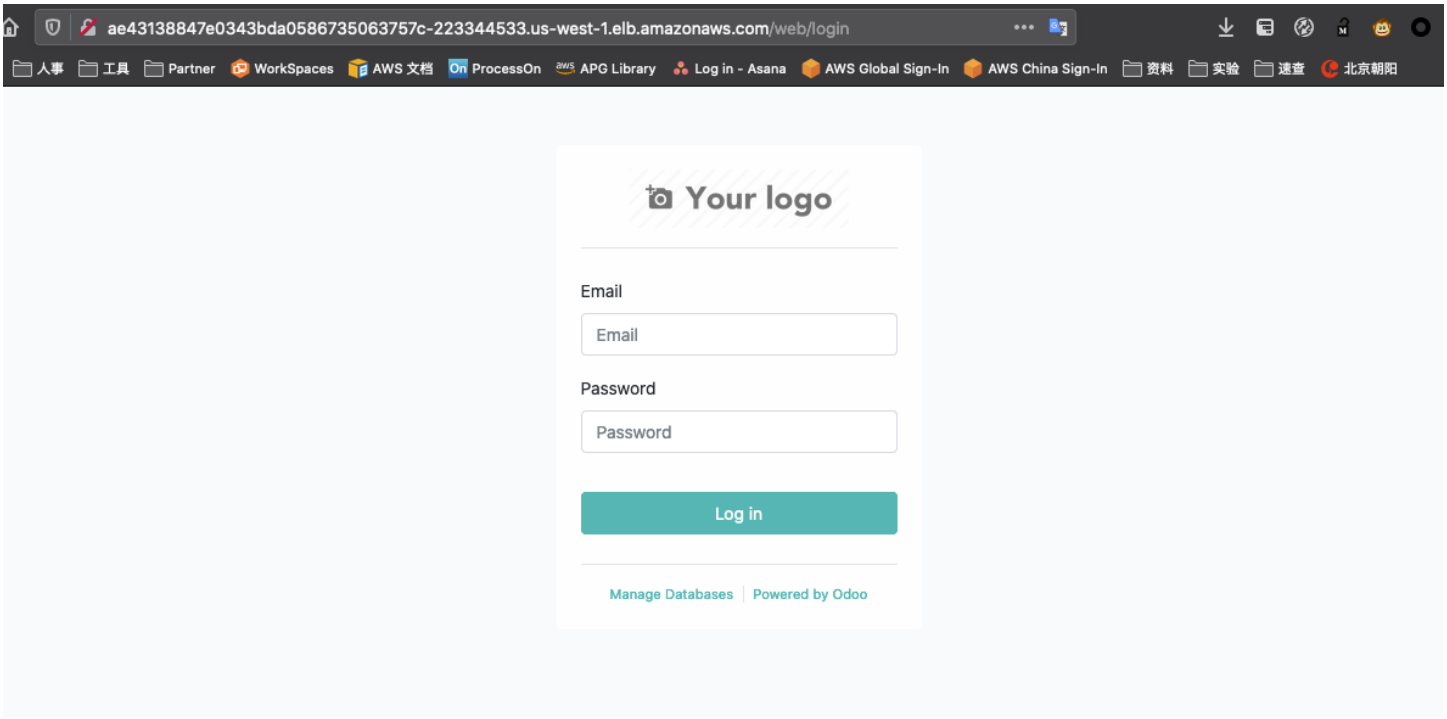


如果您遇到 Graviton2PartnerWorkshop 已存在的报错，可能是您在之前的使用中已经自动创建了这个模板并且未完成删除，请您替换模板名称或是导航至 cloudformation 控制台完成删除并重新创建。

登录 Odoo 社区版后台管理系统

在您的任意浏览器输出访问 output 的 URL，这是一个 ELB 负载均衡器，后面连接至 EKS 集群内的各个 odoo Pod 的地址，例如 http://ae43138847e0343bda0586735063757c-223344533.us-east-1.elb.amazonaws.com/

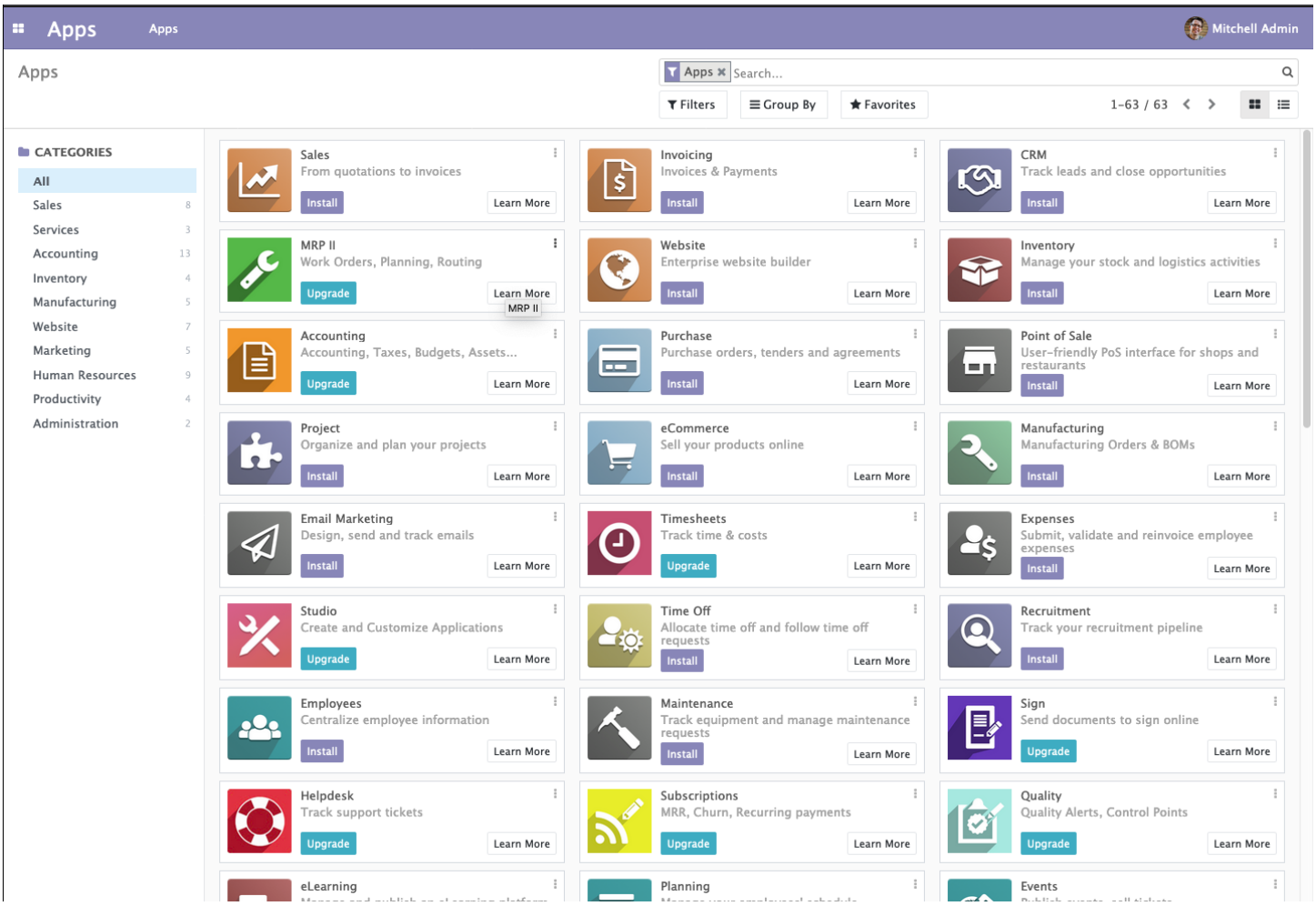
输入您的自定义密码，如果 cloudformation 填写参数页面您没有进行改动，默认用户名密码为 admin/admin



ps.初次登陆时会触发应用在数据库建表，这个过程大概需要 30 秒等待

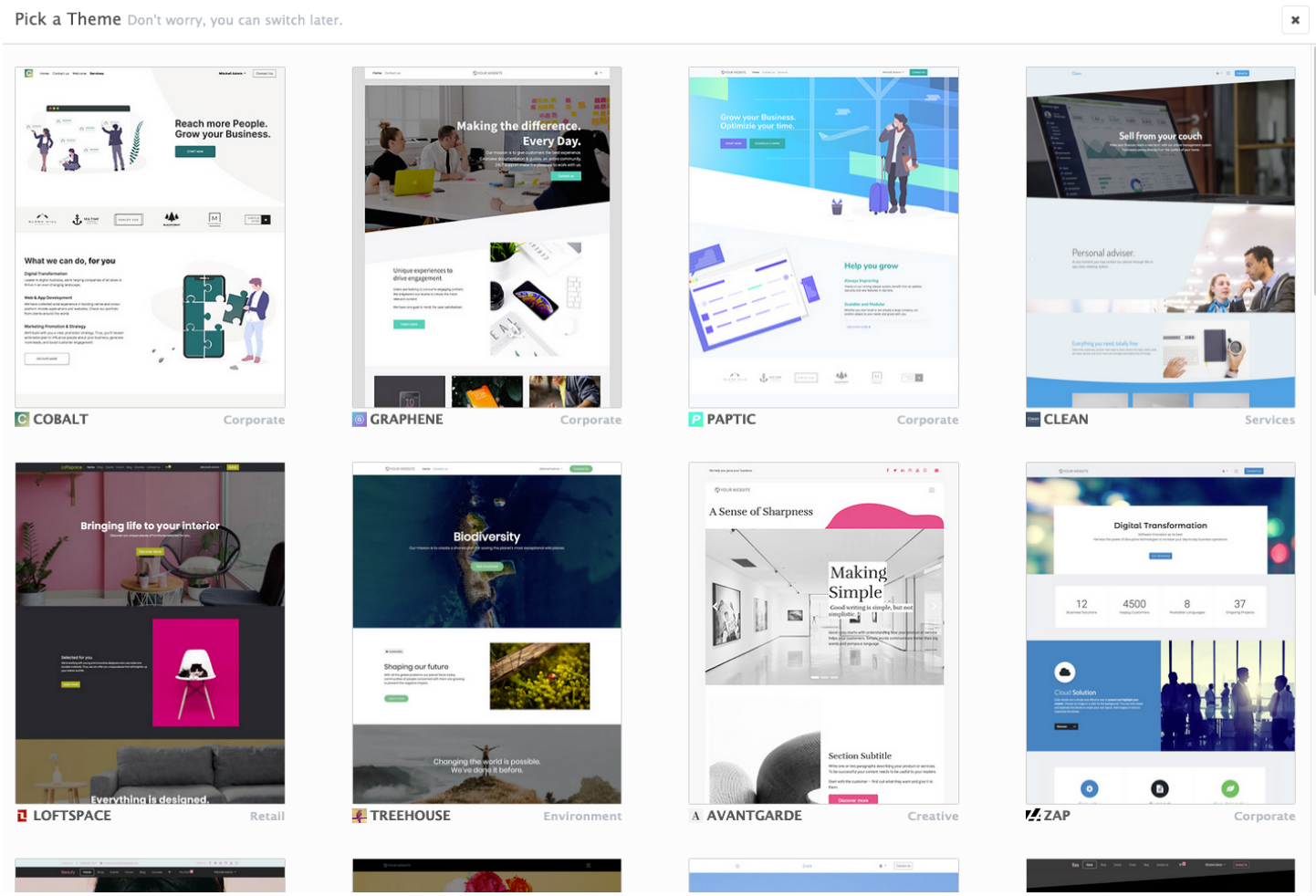
登录后您可以看见 odoo 流行的企业应用列表。除了这些，odoo 拥有活跃的开源社区，提供上千个成熟的企业级应用，并将这些应用封装为模块化插件，您只需点击任意模块的 install 即可进行模块安装，并主动跳转到您登陆权限对应的该应用后台管理界面。有关更多关于 Odoo 的信息，请您查阅 odoo_user_doc

Odoo is a suite of web based open source business apps. The main Odoo Apps include an Open Source CRM, Website Builder, eCommerce, Warehouse Management, Project Management, Billing & Accounting, Point of Sale, Human Resources, Marketing, Manufacturing, … Odoo Apps can be used as stand-alone applications, but they also integrate seamlessly so you get a full-featured Open Source ERP when you install several Apps.

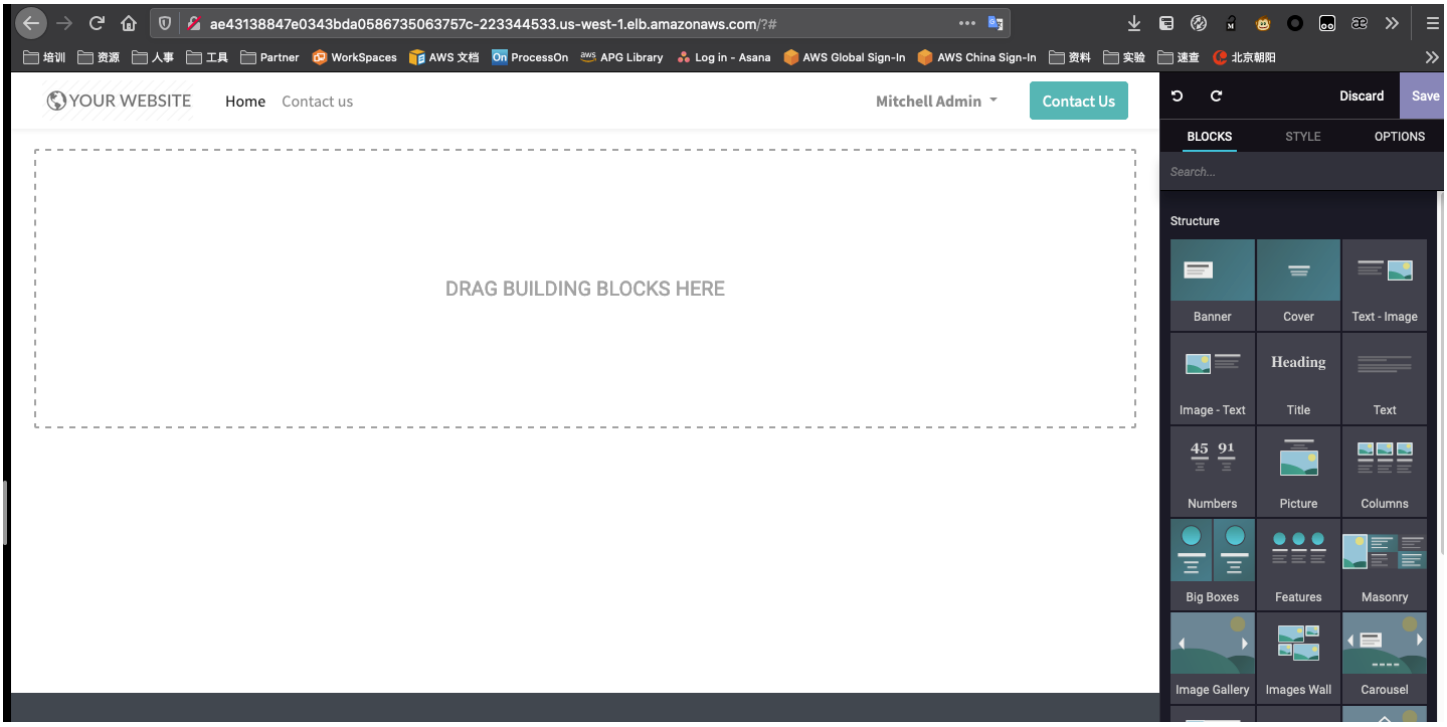


部署电商和 ERP 模块

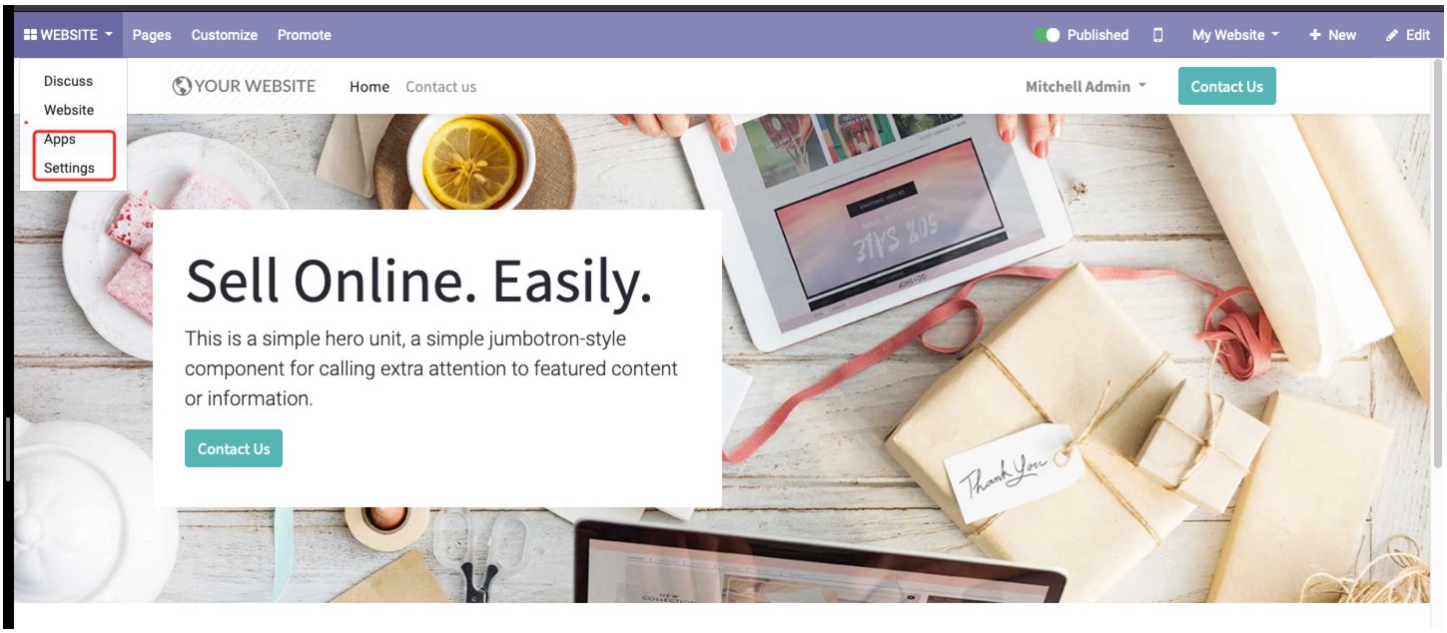
现在我们点击 website—》install，稍等 30 秒左右将会完成模块安装，并跳转到主题选择页面



进入到 website 编辑页面，您可以通过简单的拉拽完成自定义门户网站搭建，使用体验类似日常的办公文档编辑软件，包括双击替换图片、调整字体、替换视频 URL 等。当然同时您也可以直接在这个控制台浏览器窗口修改或编写 html 代码，以完成您需要的其他功能



点击左上角的主图标，您可以选择其他项目，例如点击 settings 设置系统为中文，点击 apps 安装其他应用，或许您现在就可以在 10 分钟内完成一个在线教育平台的 demo。



配置 Amazon EKS 堡垒机之外的 Role 获得 EKS 集群控制权

Cloudformation 帮助我们创建了 EKS 集群等资源，这些资源默认只能在内网进行通讯。我们仅能通过 ssh 至堡垒机从而对这些资源进行后台管理。这也是我们安全性最佳实践的原则。

如果您出于对实验便利的需要，想从控制台界面操作 EKS 集群。你需要为 EKS 集群的 configmap 进行编辑，以添加您当前使用的除了堡垒机 role 之外的用户访问 EKS 的授权。要完成这个操作您可以进行如下配置：

1，ssh 至您的堡垒机,例如（请把 c2-54-176-92-104.us-east-1.compute.amazonaws.com 替换成你自己的堡垒机地址，ee-default-keypair.pem 是你在创建 Cloudformation 时选择的的 Key,如果你不是使用默认模板做的选择，请替换为你自己的 Key name。通过 eventengine 做实验的同事请在 https://dashboard.eventengine.run/dashboard 页面下载 ee-default-keypair.pem）

ssh -i "ee-default-keypair.pem" ec2-user@ec2-54-176-92-104.us-east-1.compute.amazonaws.com

若您成功登录，您应该是第一次登陆到堡垒机，现在我们需要通过 aws eks 命令将堡垒机的 kubeconfig 文件进行更新，使得堡垒机可以管控 EKS 集群

aws eks --region us-east-1 update-kubeconfig --name odoo

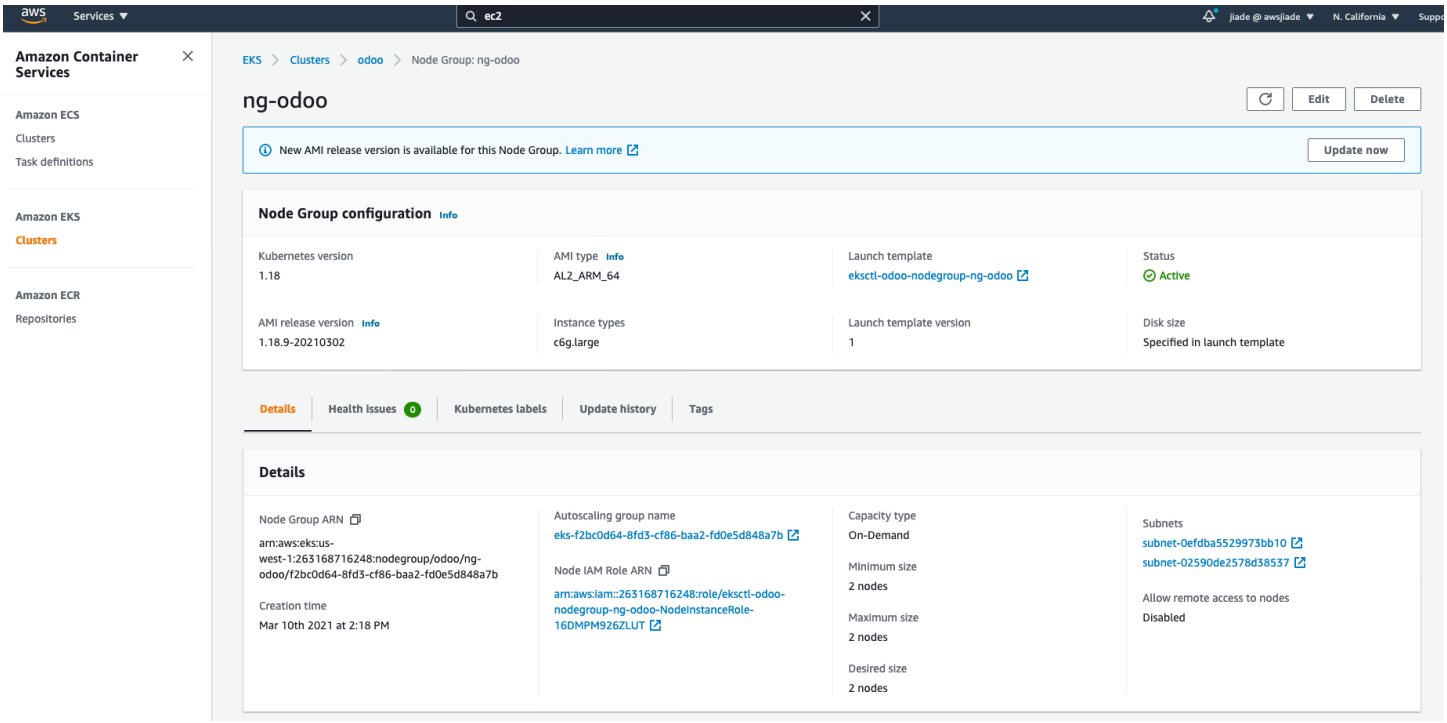
由于 EKS 集群由堡垒机创建，堡垒机默认就有 EKS 集群的管理权限，您可以通过 kubectl get pods -n odoo 命令，查看我们已经通过脚本部署的 2 个 odoo 应用。

```
kubectl get pods -n odoo
NAME                READY   STATUS    RESTARTS   AGE
odoo-arm-85b78fbb5d-62bw6   1/1     Running   0          9d
odoo-arm-85b78fbb5d-6wzq6   1/1     Running   0          9d
```

2，在堡垒机运行以下命令，编辑 configmap 以为用户添加权限，请将${ACCOUNT_ID}替换为您的账号，将${AWS_REGION}替换为您实验的 region

```
eksctl create iamidentitymapping --cluster odoo \
--arn arn:aws:iam::${ACCOUNT_ID}:role/TeamRole \
--group system:masters \
--username admin \
--region ${AWS_REGION}
```

编辑完成后您可以通过控制台查看您的集群



如果您还需要通过你自己的笔记本管理集群，你需要在本地配置了相应的 aksk，完成后可以在本地运行 kubectl get nodes，进行测试

1，在您的本地终端安装 AWS CLI，配置用户的 AKSK 和默认 region，如果您没有配置过 AWS CLI 您可以参考 AWS CLI 安装完成安装和配置 CLI 工作。如果您之前安装过 CLI，您只需要更换 AKSK 为您实验的 AKSK 即可

2，运行以下命令，请将 region 和 name 字段替换为您的环境,例如下面示范的，us-east-1 和 odoo(如何您使用默认参数)

```
aws eks --region us-east-1 update-kubeconfig --name odoo
```

3，运行以下命令以获取并记录您的 IAM ARN 和 username

```
aws sts get-caller-identity
```

```
{
  "UserId": "AIDAT2RQT5XMFX7535ZCV",
  "Account": "xxxxxxxx",
  "Arn": "arn:aws:iam::xxxxxxxxx:user/jiade"
}
(END)
```

4，在您的本地执行以下命令测试您配置的本地管理

kubectl get nodes

```
NAME                                          STATUS   ROLES    AGE   VERSION
ip-10-0-28-210.us-east-1.compute.internal   Ready    <none>   9d    v1.18.9-eks-d1db3c
ip-10-0-45-169.us-east-1.compute.internal   Ready    <none>   9d    v1.18.9-eks-d1db3c
```