**基于Tag驱动的EBS类型优化模板**

关键词：AWS CloudFormation, AWS Lambda, Tag, CloudTrail, CloudWatch

作者：刘育新，AWS专业服务咨询顾问

时间：2018年10

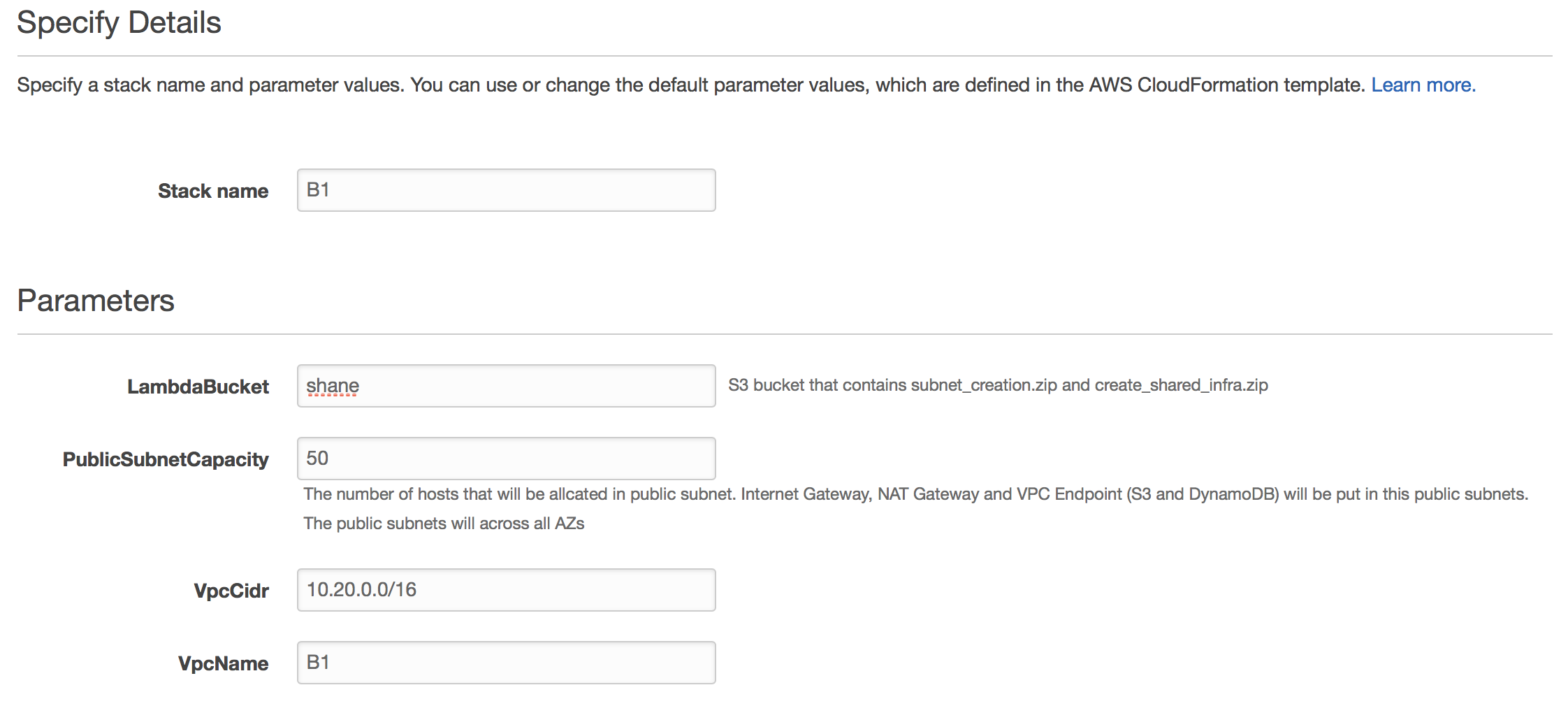
## 需求背景

企业中用于做报表的数据库服务器只是在每天的某个时间点需要大规模的磁盘IO操作，持续时间大约3个小时，如果按照高峰时期的磁盘IO需求来设定EBS卷的类型，需要IOPS为10000的io1卷。而按照平时大多数时候的磁盘IO水平来看，gp2类型的磁盘已经可以满足要求。为了能够做到物尽其用，节省成本，在IO高峰时候使用io1卷，而平时使用gp2卷会是一个理想的安排。

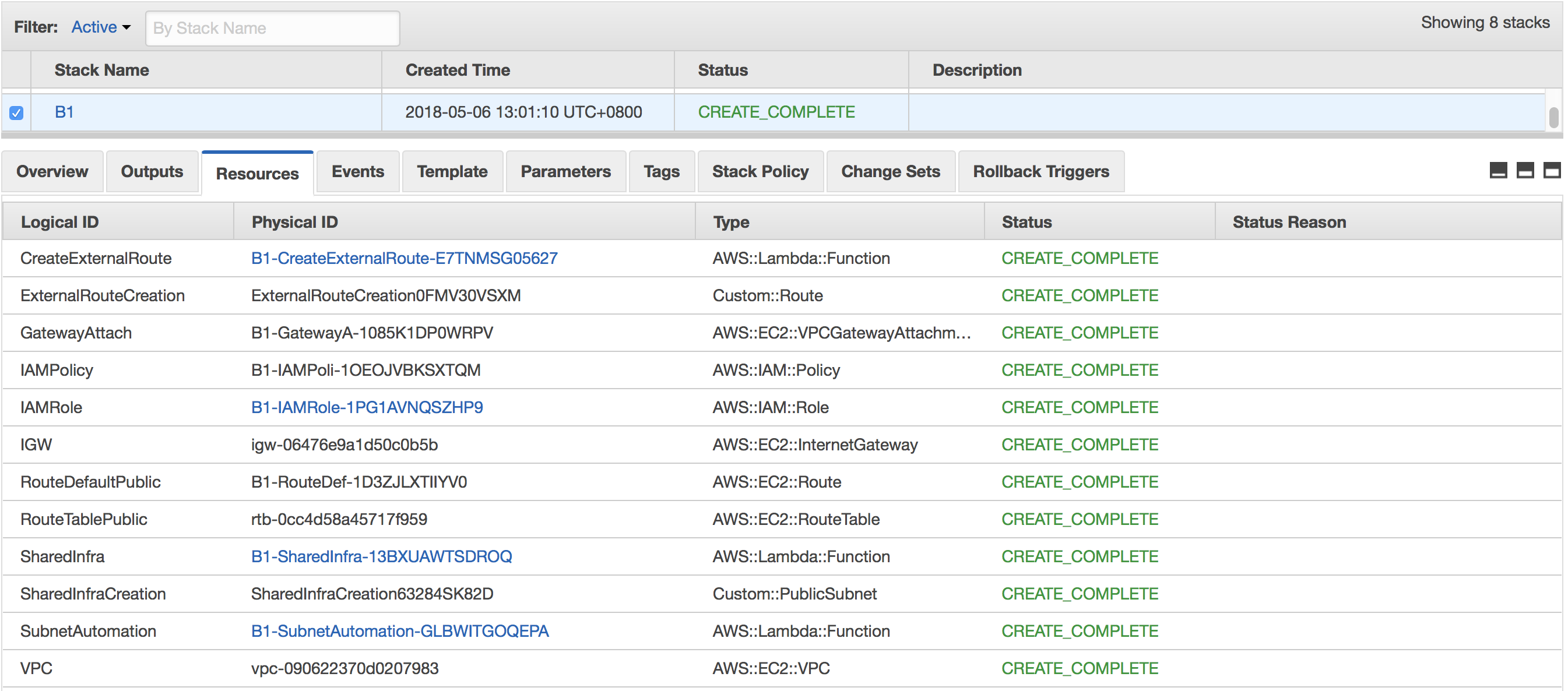
## 方案概述

## ，安装和运行

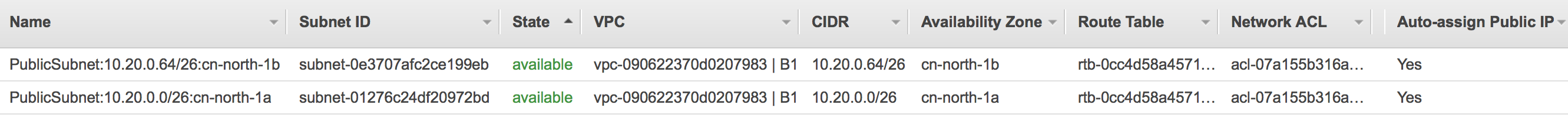
1. 在浏览器中输入：<https://github.com/shaneliuyx/autosubnet_creation>， 下载2个json文件和3个zip文件。将3个zip文件上传到一个S3存储桶中。
2. 打开AWS控制台，并选择CloudFormation，选择存储在本地的json文件CreateBaseVpc.json，运行CloudFormation模板。
3. 假设输入缺省的PublicSubnetCapacity和VpcCidr如下：



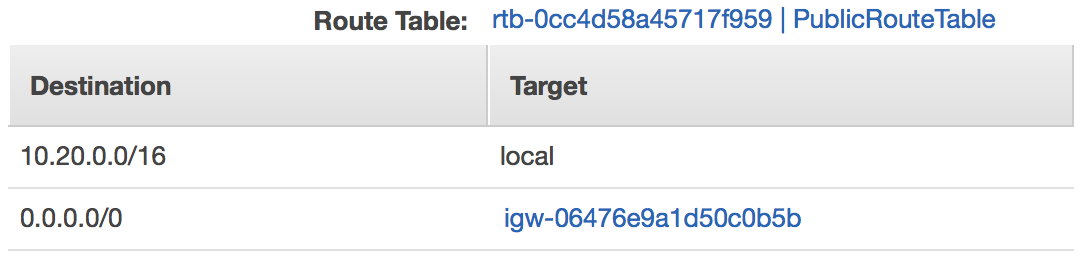
1. 选择Next，直至AWS资源开始创建
2. 最终运行结果如下



创建的Subnet如下：

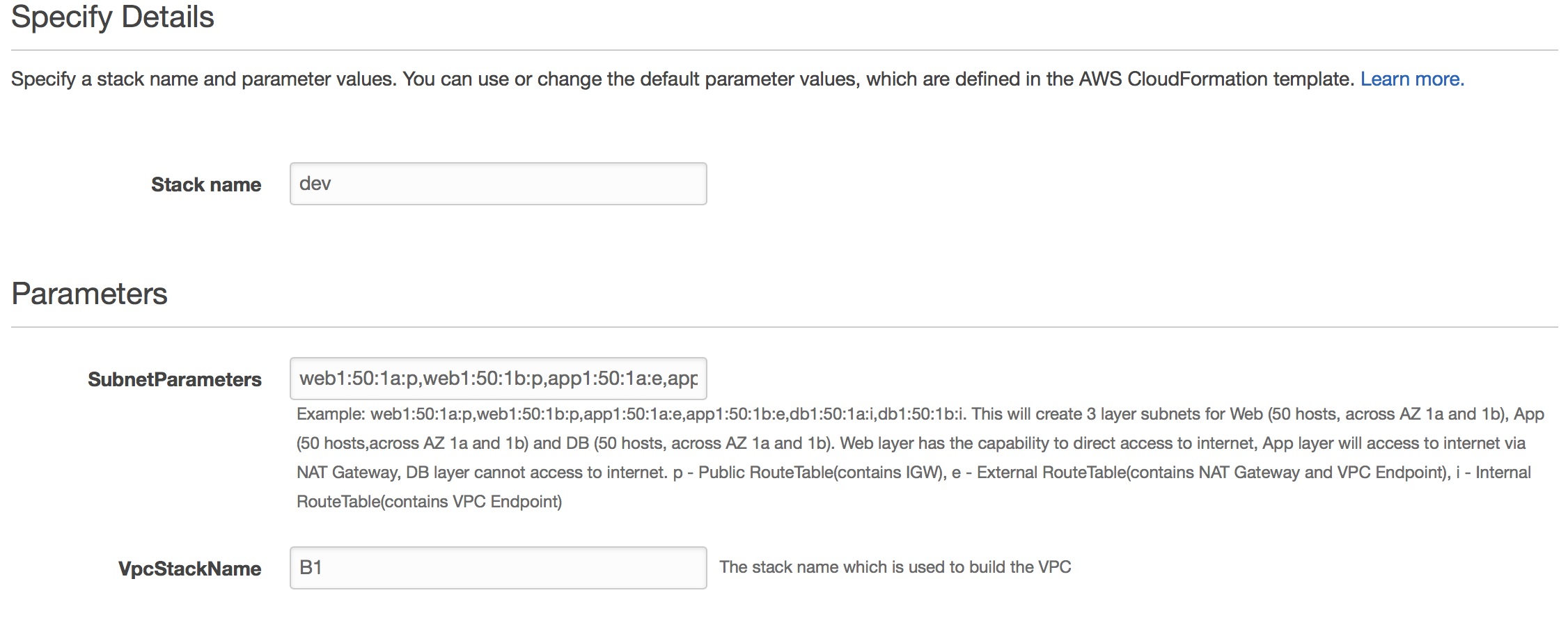


公共子网路由表：

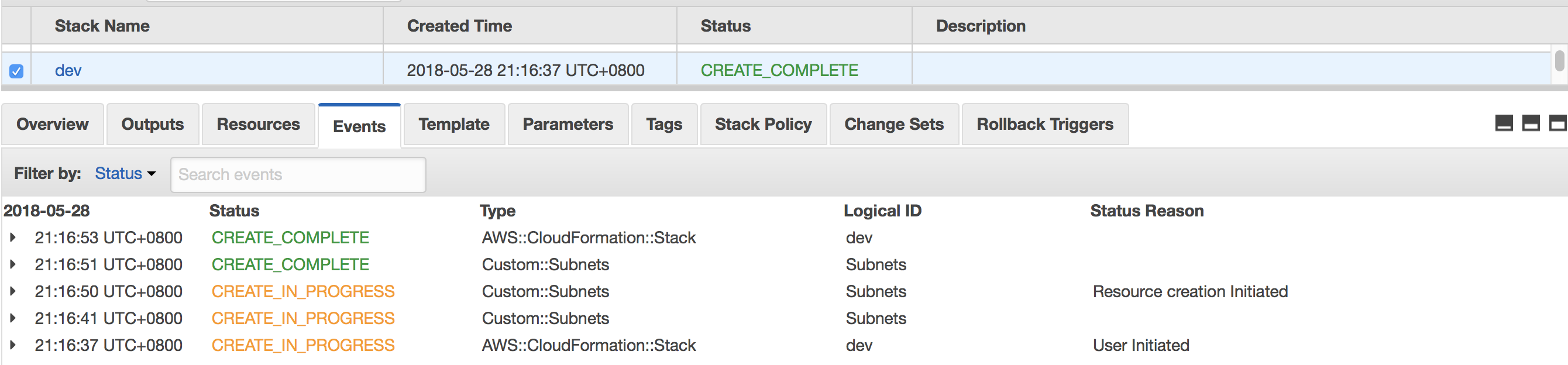


1. 打开AWS控制台，并选择CloudFormation，选择存储在本地的json文件SubnetAuto.json，运行CloudFormation模板。
2. 输入SubnetParameters：web1:50:1a:p,web1:50:1b:p,app1:50:1a:e,app1:50:1b:e,db1:50:1a:i,db1:50:1b:i

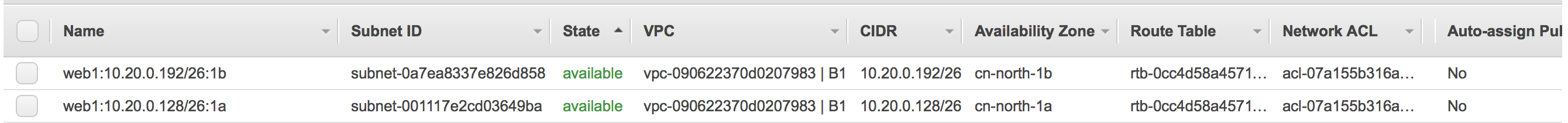
这将创建6个子网，其中Web、APP和DB各2个子网，分布在2个AZ中

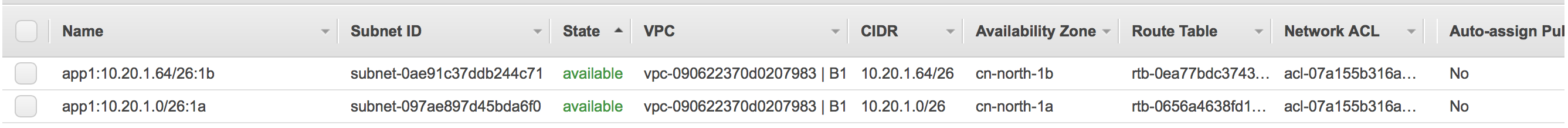


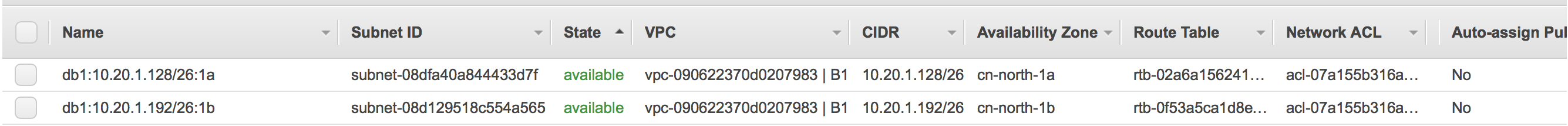
1. 运行结果如下



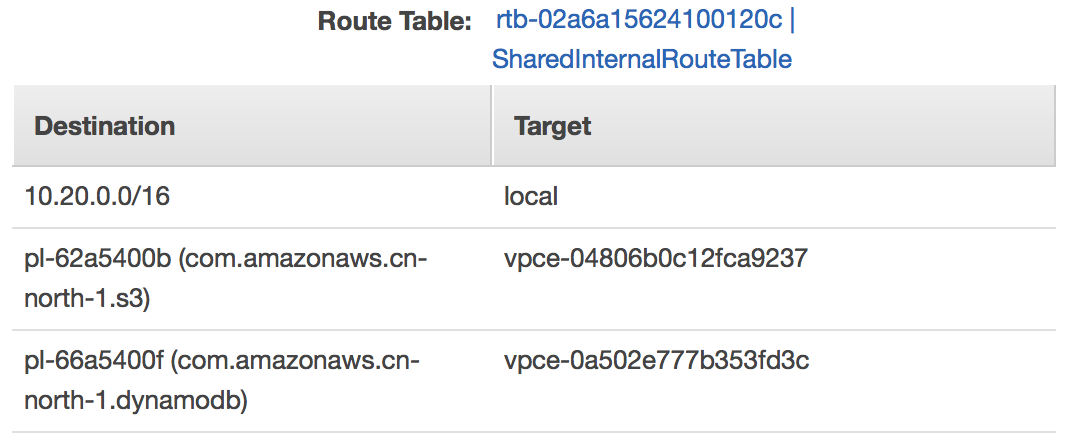
创建的子网：



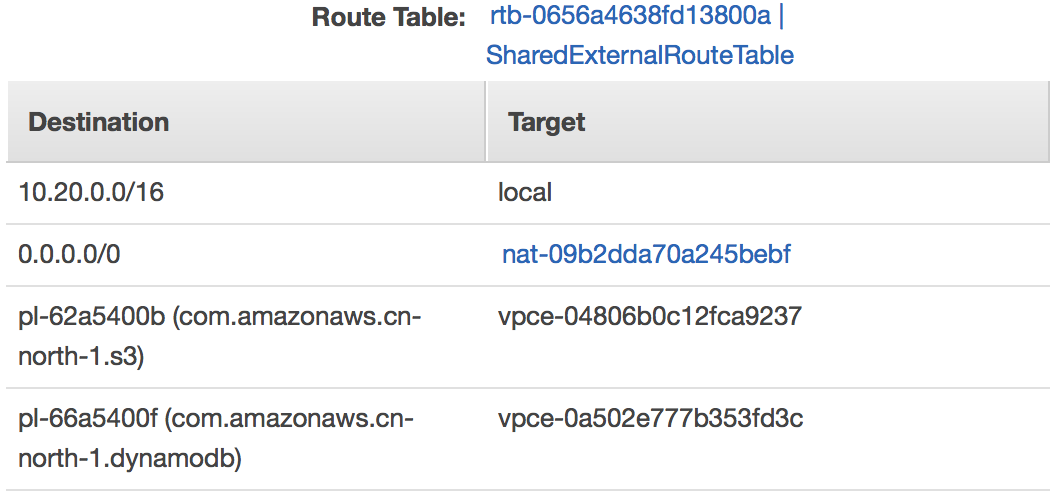




内部子网路由表：

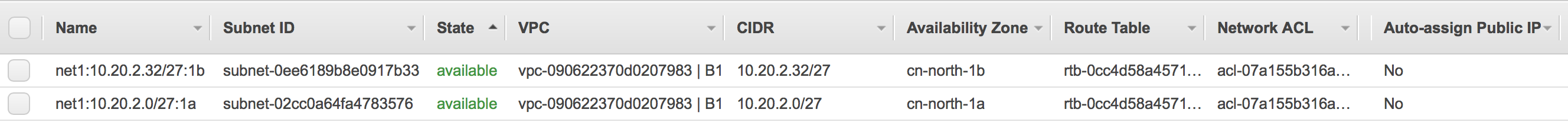


外部子网路由表：



假设现在还要创建一个包含16个有效IP的公共子网用于部署网络设备，可以再运行一次SubnetAuto.json，输出参数：net1:16:1a:p,net1:16:1b:p

则可以创建出如下子网：



## 与其他CloudFormation模板配合使用，进行Landing Zone部署

Landing Zone中文名称翻译成着陆区，是指AWS的基本环境，用户在其上部署安全和运维流程。Landing Zone的内容包含：账户结构、账户安全基线、网络结构和AWS用户访问管理。下面简单的介绍一下AWS Landing Zone的最佳实践。

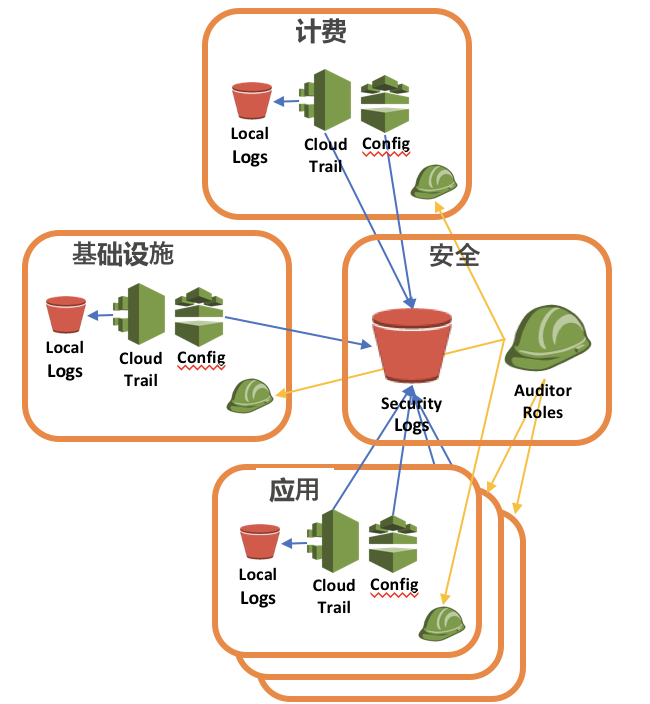
* 账户结构

AWS建议账户的划分与企业的组织架构和运维部门的组织架构一致。例如按照如下结构划分账户：



* 账户安全基线

AWS建议在所有账户内打开CloudTrail和AWS Config功能。所有日志信息要复制到安全账户内的S3存储桶中。建立跨账户访问的Auditor角色。



* 网络结构

AWS建议删除缺省VPC，建立客户自己定义的VPC。建立共享VPC（包含目录服务、邮件服务器等），应用VPC与共享VPC建立Peer关系。通过VPN或者Direct Connect与线下的数据中心建立网络连接，或者采用Transit VPC（参考 <https://aws.amazon.com/answers/networking/aws-global-transit-network/> ，<https://aws.amazon.com/blogs/aws/aws-solution-transit-vpc/> ）建立集中的网络控制机制。网络输入输出的安全控制（建立堡垒机，建立Security Group、网络ACL或者第三方的防火墙工具）

* AWS用户访问管理

包括建议基于SAML的单点登录，建立跨账户角色访问机制等。

上述介绍的建立VPC和子网的方法可以看成建立Landing Zone的基础，在此之上，我们还可以使用CloudFormation建立堡垒机，打开CloudTrail和AWS config，建立不同账户间的日志（log）复制机制，建立Config Rule进行合规性检查等等。 AWS已经开发出多个QuickStart CloudFormation脚本协助用户完成上述工作，但是这些脚本在中国区（BJS）运行时需要做一些修改。下表列出了一些可用的资源，其中中国区部署模板是我针对中国区的特点修改过的，可以在BJS正常运行。

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | **原始代码 参考** | **AWS 中国区部署模板** |
| **账户安全基线** | 配置AWS config和CloudTrail | <https://github.com/aws-quickstart/quickstart-compliance-pci> | <https://s3.cn-north-1.amazonaws.com.cn/shane/quickstart-security/logging.template> |
| 配置IAM角色 | <https://s3.cn-north-1.amazonaws.com.cn/shane/quickstart-security/iam.template> |
| 配置Config rules | <https://s3.cn-north-1.amazonaws.com.cn/shane/quickstart-security/config-rules.template> |
| 将CloudWatch Log转储到S3存储桶 | <https://github.com/alertlogic/cloudwatch-logs-s3-export#setup> | https://s3.cn-north-1.amazonaws.com.cn/shane/cwl-s3-export-new.template 使用说明：https://s3.cn-north-1.amazonaws.com.cn/shane/User+Guide+-+Copy+VPC+Flow+Logs+to+S3+CloudFormation+Templates.docx |
| 将一个账户下的S3存储桶复制到另一个账户的S3 |  | https://s3.cn-north-1.amazonaws.com.cn/shane/s3-to-s3/1source.json https://s3.cn-north-1.amazonaws.com.cn/shane/s3-to-s3/2target.json https://s3.cn-north-1.amazonaws.com.cn/shane/s3-to-s3/3source.json 使用说明：https://s3.cn-north-1.amazonaws.com.cn/shane/s3-to-s3/User+Guide+-+S3+to+S3+Replication+CloudFormation+Templates.docx |
| **网络结构** | 配置Linux Bastion | <https://github.com/aws-quickstart/quickstart-linux-bastion> | https://s3.cn-north-1.amazonaws.com.cn/shane/linux-bastion.template 不支持CentOS |
| 建立VPC和分配Subnet | <https://github.com/aws-quickstart/quickstart-aws-vpc> | <https://github.com/shaneliuyx/autosubnet_creation> |

希望这些工具会对Landing Zone的部署工作有所帮助。