Amazon Transit Gateway with Shared VPC in Single Account Quickstart

基于 Amazon Transit Gateway 的单一账户共享 VPC 快速部署解决方案

本方案是一个基于单账户多 Virtual Private Cloud (VPC)以 Amazon Transit Gateway 为核心的组网的 CloudFormation 模版，按照 TGW 和共享 VPC 模式设计，兼顾 IDC 和多云互联的考虑。

一、方案介绍

1、需求背景

在规划 Amazon Web Services 资源部署落地过程中，可能会面临着如下问题：

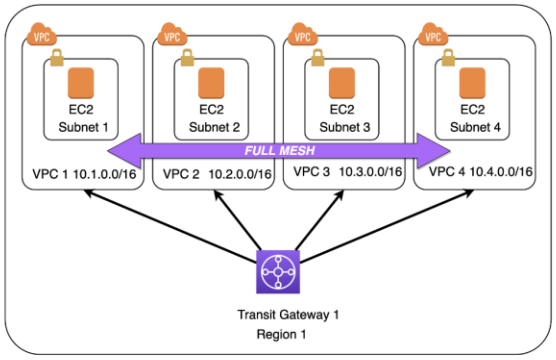
场景和挑战	部署需求
- 下属二级公司独立运营 IT 系统 - 采购商用第三方解决方案 - 外包开发 - 允许供应商直接远程登录进行维护	- 多 VPC 网段完全隔离每个应用系统独立部署在 VPC 内 - 东西向流量管控，应用间不可见 - 开发、测试、生产环境之间不可见 - VPC Peering 只能两两互联，不能统一交换数据
- 应用要求从互联网访问 - 应用分成多层架构，WEB 层允许外部访问， 应用服务器位于内网，只接受 WEB 服务器的 API 访问	- VPC 有从外部互联网访问需求 - 内部子网有向外部 API 访问需求
- IDC 与门店互联注重成本 - 众多门店与云之间需要构建互联	- Site-to-Site VPN 需求对接 IDC - 门店经常使用商用防火墙构建网络门店需要与特定应用互通访问，互通过程需要跨云
- 出海门店需要数据回国 - 出海员工需要使用国内系统进行日常办公	- 跨境部署应用 - 海外访问加速

由此需求，在单账户范围内，可以采用多 VPC 和 Transit Gateway 互联的形式，并且将一个 VPC 定义为共享服务 VPC，组建特定的网络架构。

2、Transit Gateway 组网模式简介

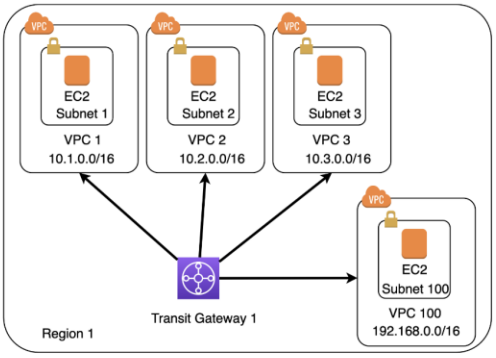
Transit Gateway 有两种组网模式，一种是全互通模式，一种是有用于部署共享服务的共享 VPC 模式。二者在 Transit Gateway 操作界面上完全相同，区别在于路由管控的设计和配置。

两种模式如下图所示。



Full mesh

全互通对等场景



Shared VPC

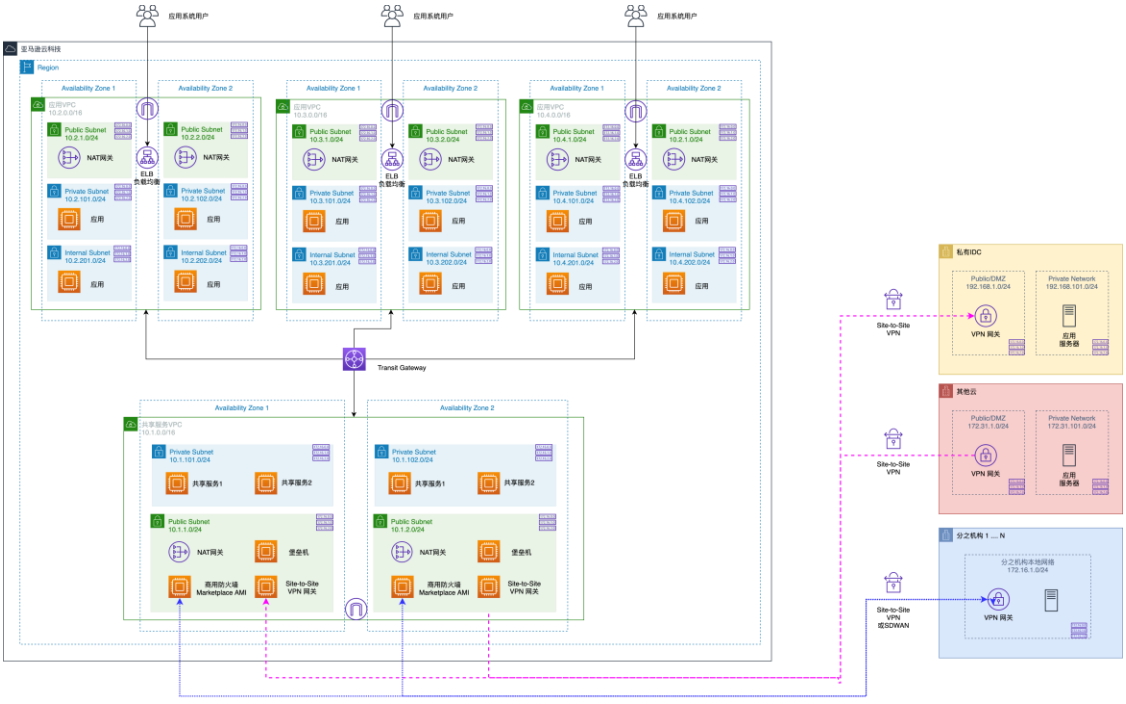
有共享的通用服务组件

或需要集中处理网络流量的需求

本方案采用的是共享服务 VPC 模式，如右侧图所示。

3、总体架构

总体架构图如下。



整个方案将创建 4 个 VPC，其中三个 VPC 作为业务 VPC，一个 VPC 作为共享服务 VPC。VPC 之间通过 TGW 互联。在以上架构图中，右侧的网络架构是云下的 IDC 组成部分，在本方案的 CloudFormation 模版中将不包含着一部分。

二、方案部署

1、前提和准备

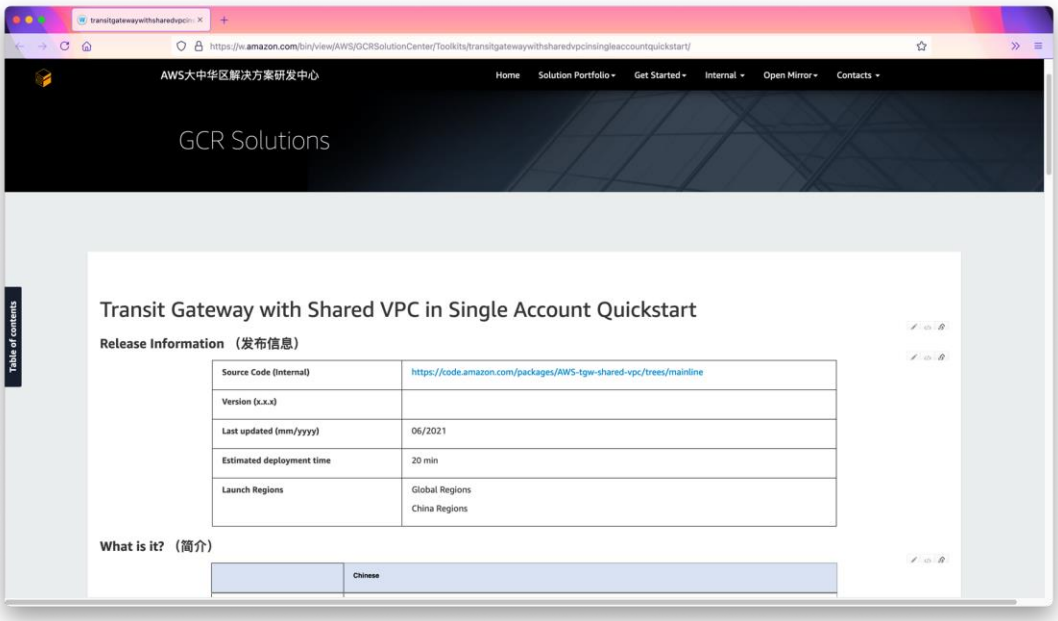
如上一章节的架构图所示，本方案将创建 4 个 VPC，每个 VPC 包含 2 个 NAT 网关、4 个子网分布在 2 个 AZ，并且为 NAT 网关和跳板机分配 EIP。因此，在使用本方案前，请通过技术支持工单，提升如下 Amazon Web Services 限制：

- 提升单个 Region 允许的 VPC 数量，从默认的 5 提升到 10。选择 Limit 类型为 `VPC`，选择对应的 region，选择 Limit 名称是 `VPCs per Region`，申请新的 limit 为 10。
- 提升单个 Region 允许的 EIP 数量，从默认的 5 提升到 20。选择 Limit 类型为 `Elastic IPs`，选择对应的 region，选择 Limit 名称是 `New VPC Elastic IP Address Limit`，申请新的数量为 20。

申请成功后，需要几个小时获得审批，即可开始使用本方案。如果没有完成本步骤提升 Limit 限额，在创建 CloudFormation 模版过程中会提示达到最大 VPC 数量限制，导致创建失败。

2、使用说明

从 Wiki 上获取解决方案入口，获取 CloudFormation 地址。如下截图。



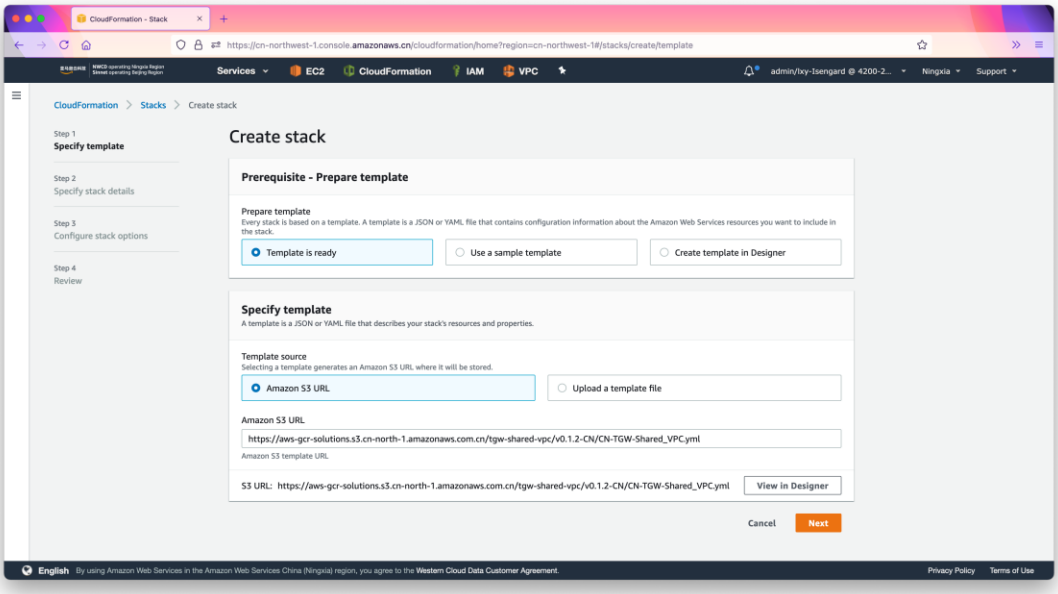
Global 区域：

https://aws-gcr-solutions.s3.amazonaws.com/tgw-shared-vpc/v0.2.3/SGP-TGW-Shared_VPC.yml

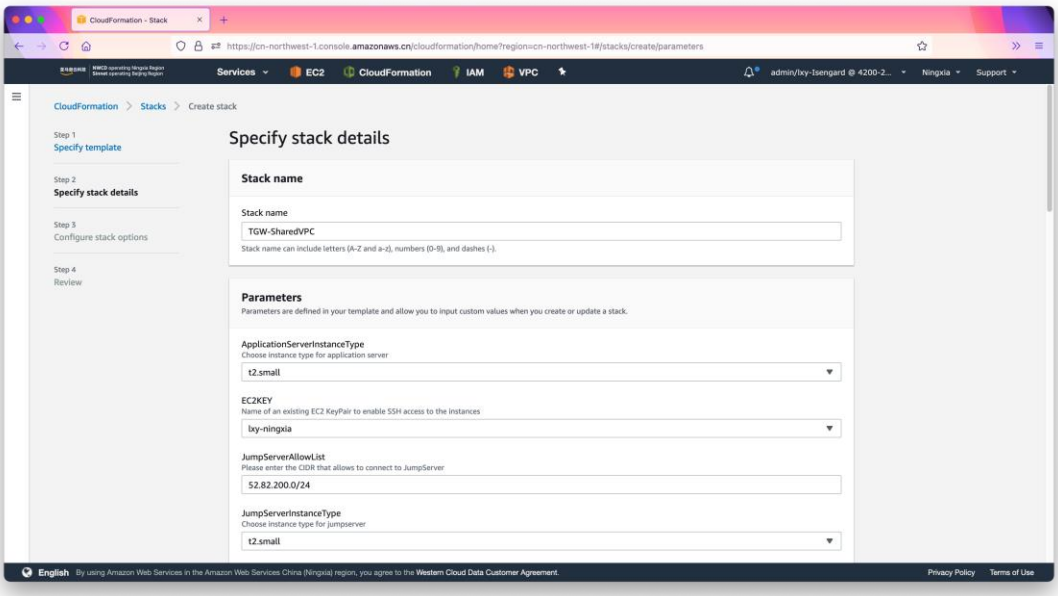
中国区：

https://aws-gcr-solutions.s3.cn-north-1.amazonaws.com.cn/tgw-shared-vpc/v0.2.3-CN/CN-TGW-Shared_VPC.yml

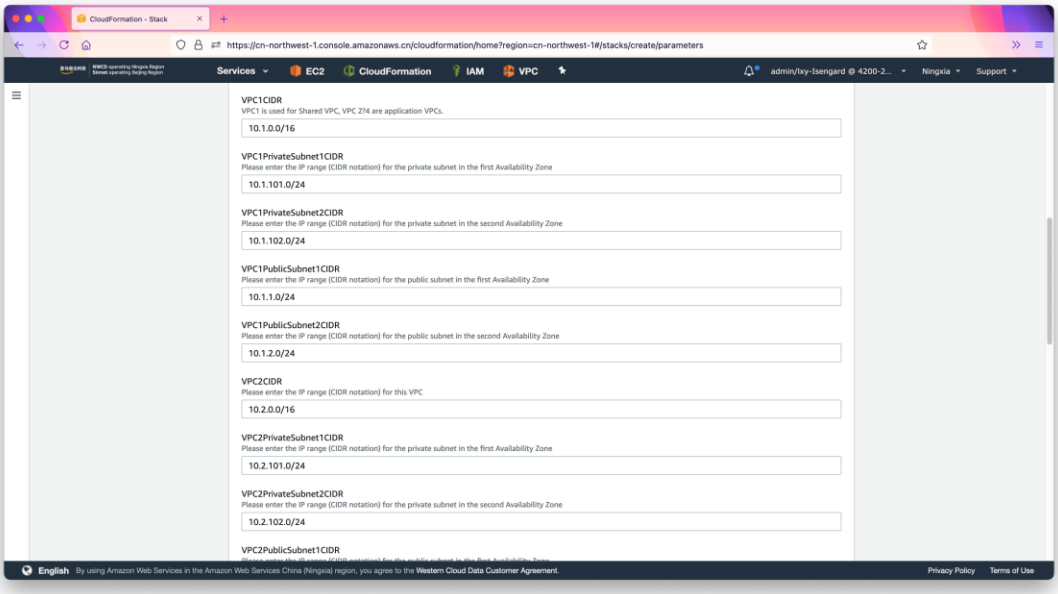
进入目标区域控制台，进入 CloudFormation 服务，选择创建服务。建议输入 S3 网址作为模版启动地址。点击下一步继续。如下截图。



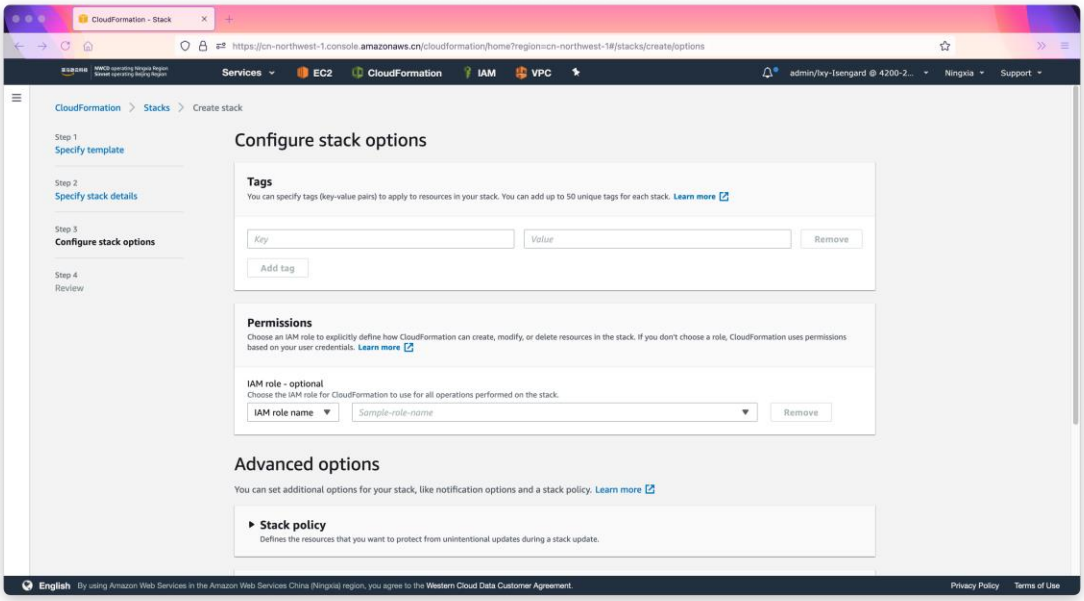
在启动 CloudFormation 向导的第二部，输入模版名称，并选择 EC2 登录密钥，跳板机规格、跳板机白名单 IP 地址等（替换为当前笔记本所在的公网出口地址）。然后向下继续滚动页面。如下截图。



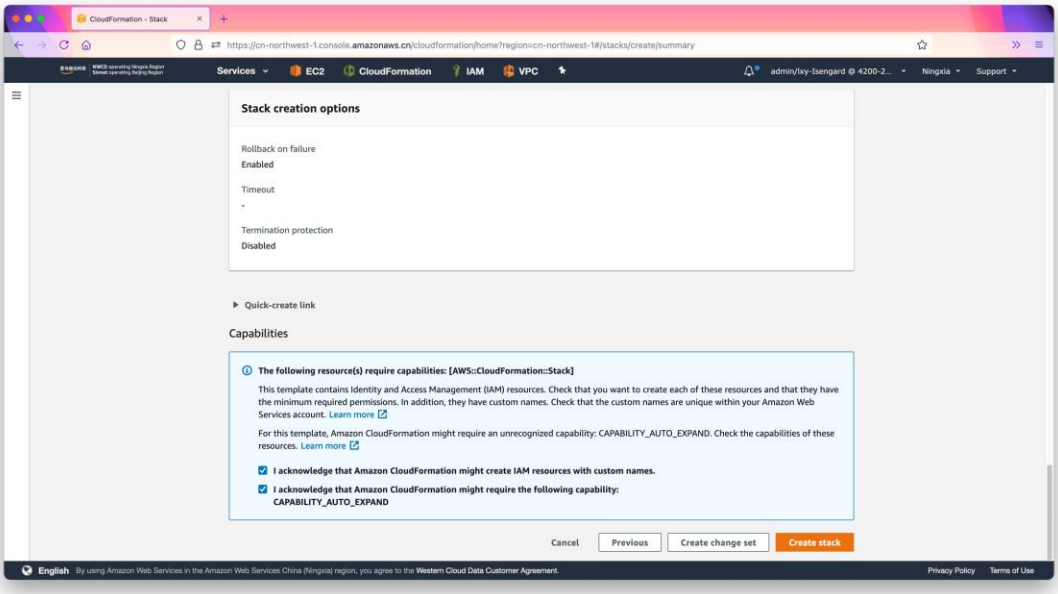
输入各 VPC 的 CIDR IP 地址段。其中代号 VPC1 的是共享服务 VPC，代号 VPC2、VPC3、VPC4 是部署应用的 VPC。如下截图。



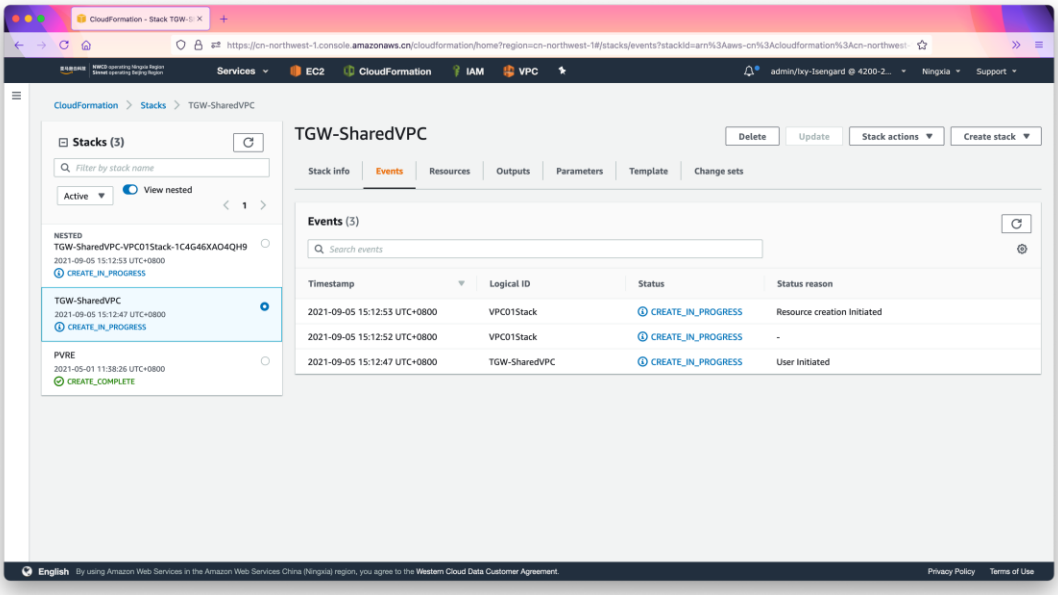
在向导的第三步，无须做任何设置，点击下一步继续。



在向导的第四步，将页面滚动到最下部，选择允许创建 IAM 角色的两个对话框。并点击创建 Stack。如下截图。



模版创建需要大改 15 分钟时间。请等待。如下截图。



整个模版包括：

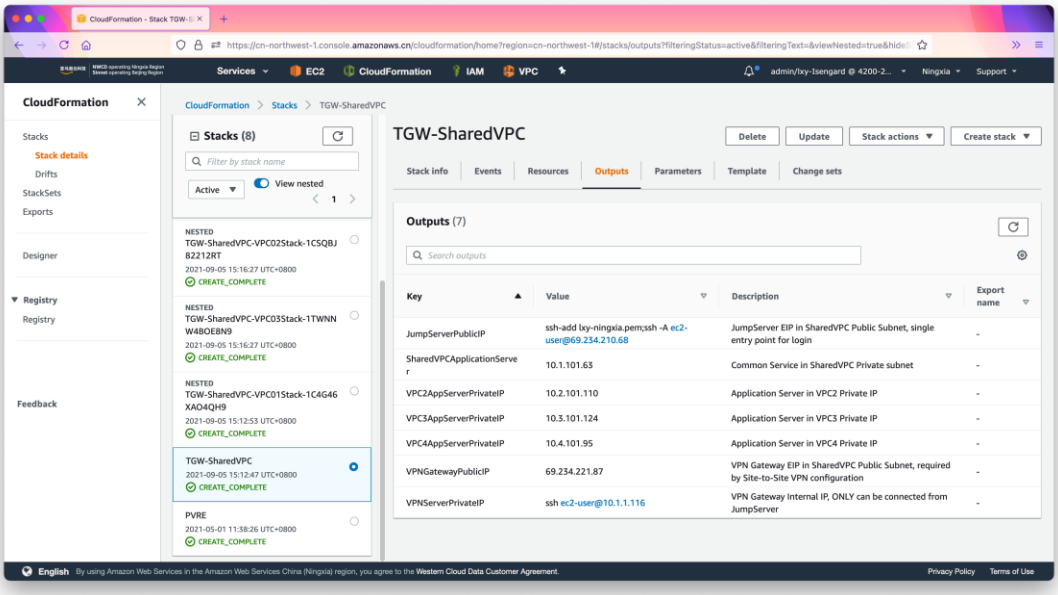
- 主模版（Main Stack）：负责 VPC 的 CIDR，跳板机规格等配置项输入；

- 嵌套模版（Nested Stack）：分别从 4 个嵌套模版生成各自的 VPC，包括 VPC、IGW、子网、路由表、NAT Gateway、测试用 EC2，IAM Role 角色（允许使用 Session Manager）；
- TGW 模版（Nested Stack）：创建 TGW，并与多个 VPC 配置 Attachment 挂载；
- TGW 路由表（Nested Stack）：补充整个网络架构所需要的东西南北相的路由。

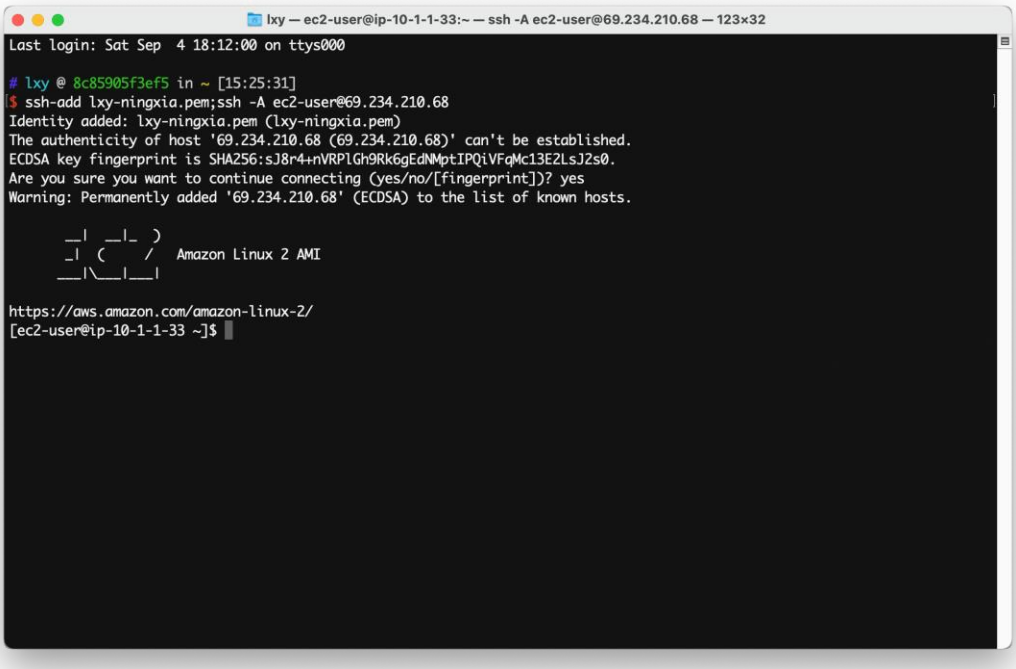
等待一段时间后，环境创建完成。

3、从跳板机登录环境

进入主模版的 CloudFormation 的 Outputs 标签页，可看到输出信息。从中我们记录下几个 VPC 内的 EC2 的内网 IP，稍后进行连通性测试。

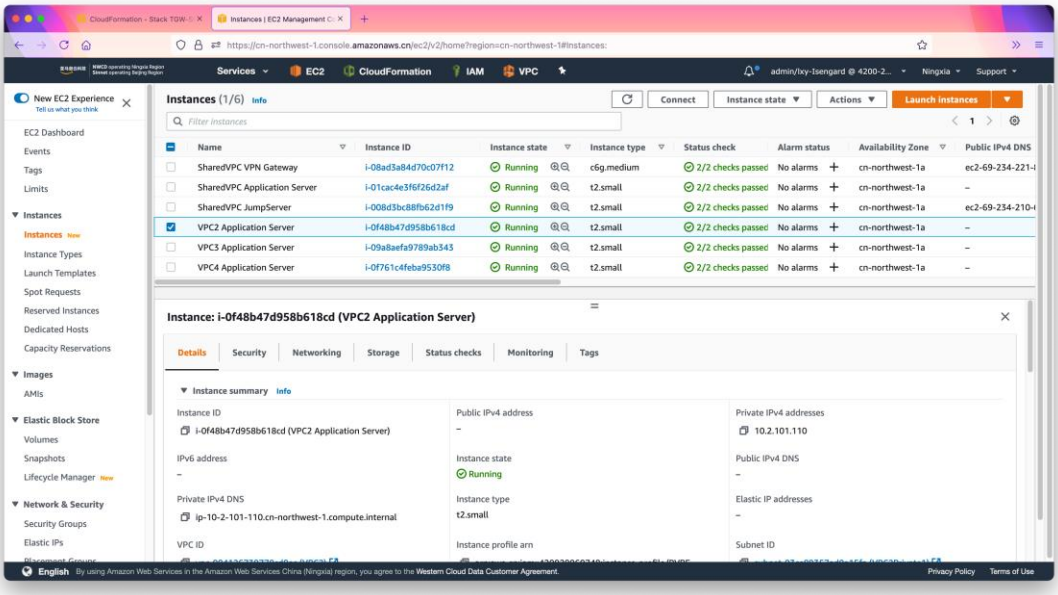


在输出信息中，可看到 `JumpServerPublicIP` 即可进行登录。登录成功如下截图。

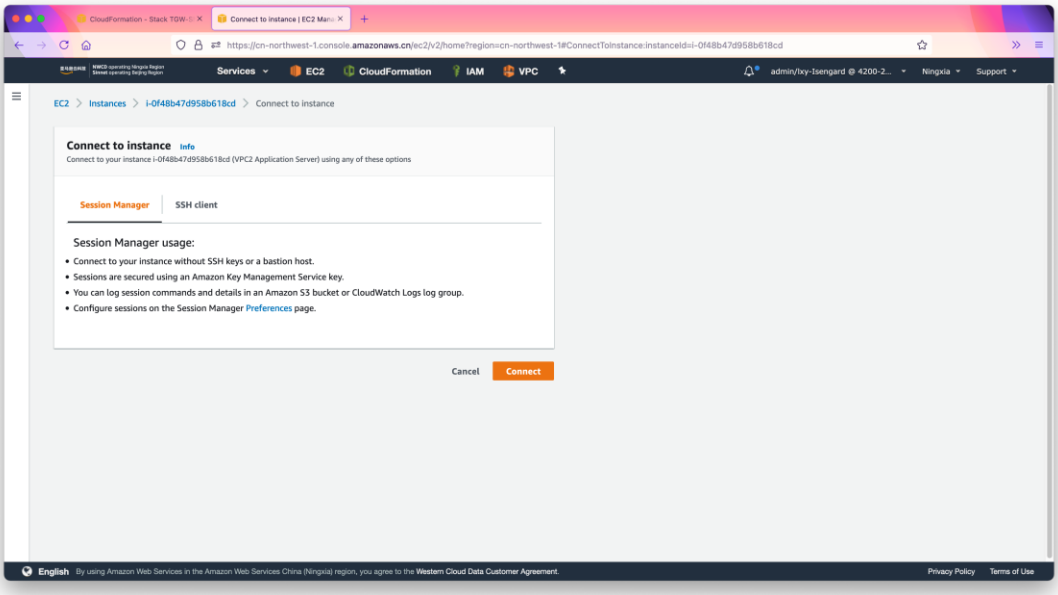


4、从 SSM Session Manager 登录环境

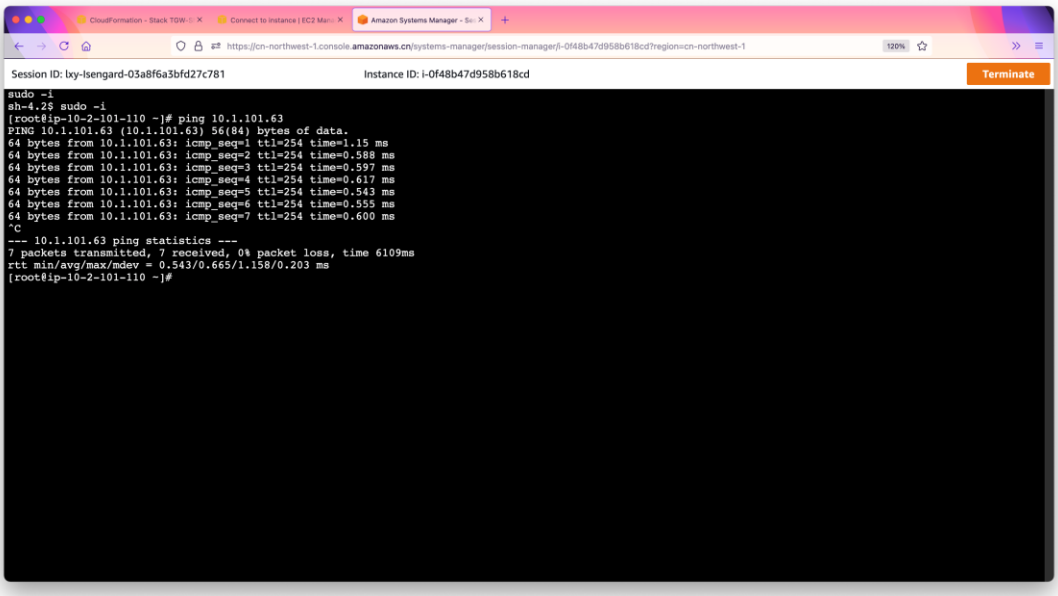
进入 EC2 控制台，选择第二个 VPC 内预先创建好的 EC2，点击右上角的 Connect 按钮，发起连接。如下截图。



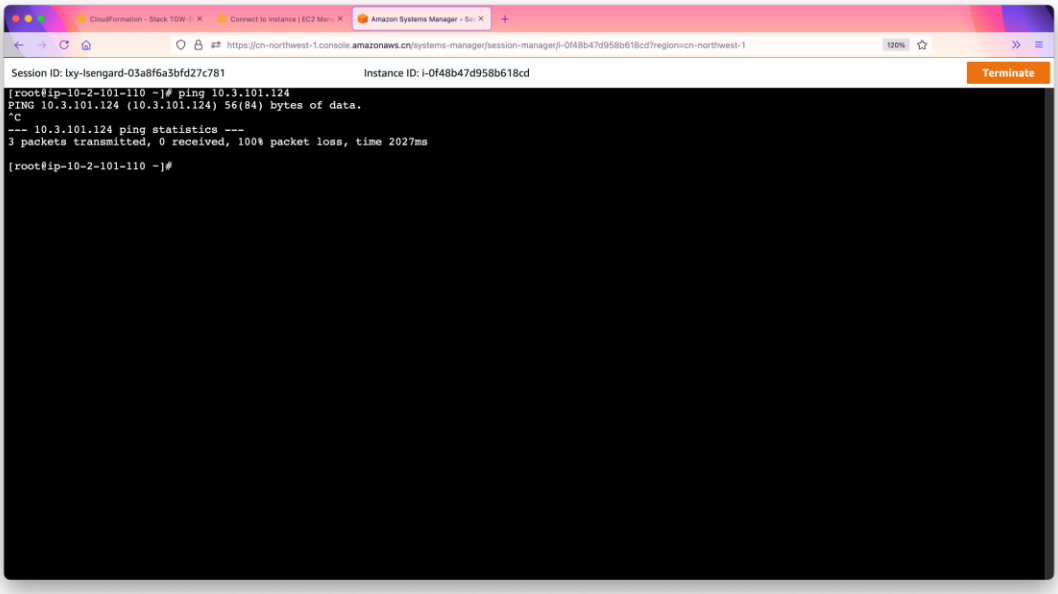
选择登录类型是 Session Manager。如下截图。



通过 Session Manager 方式登录 SSH 成功。从本机位置发起对共享 VPC（代号 VPC1）内的 EC2 的 ping 测试，可以看到访问成功。如下截图。



从本机位置发起对业务 VPC（代号 VPC3/4）内的 EC2 的 ping 测试，可以看到因为没有正确路由而无法通达。如下截图。



至此验证了东西和南北向流量正常。

5、开始创建应用

经过上述基本测试，环境部署完成且网络正常。每个 VPC 也都生成了 NAT Gateway 可以向外访问。接下来就可以在：

- VPC1 作为共享 VPC 内部署所有 VPC 都需要访问的应用
- VPC2、VPC3、VPC4 作为业务 VPC 部署独立的应用

三、方案补充配置

1、保护 CloudFormation Stack 不被修改和操作

为了保护生产环境下的 CloudFormation 不被意外操作破坏，可在日常操作管理员的基础上，增加一段 IAM Policy，禁止对这个的 CloudFormation 的 Stack 的查询和修改。参考如下，请替换其中的 Resource 部分的 stack 为 ID 为时机生成的 ID。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "cloudformation:CancelUpdateStack",
                "cloudformation:ContinueUpdateRollback",
                "cloudformation:CreateChangeSet",
                "cloudformation:DeleteStack",
```

```
                "cloudformation:GetTemplate",
                "cloudformation:GetTemplateSummary",
                "cloudformation:SetStackPolicy",
                "cloudformation:UpdateStack",
                "cloudformation:UpdateTerminationProtection"
            ],
            "Effect": "Deny",
            "Resource": "arn:aws:cloudformation:us-east-1:381727908625:stack/
mod-b80cbfb4f0844f0b/79610570-dc09-11eb-a8d9-0e1ad0c392f9"
        }
    ]
}
```

2、配置 Site-to-Site VPN 到 IDC（不可用于跨境）

在需要与 IDC 或者其他云互联组网、且不使用 Direct Connect 专线的场景下，建议通过 Site-to-Site VPN 组网。随 CloudFormation 模版生成的 Shared VPC 内的 EC2 作为 VPN Gateway，可采用 OpenSWAN 等软 VPN 方案进行部署。

需要注意的是：

- 只能作为国内与 IDC 互联只用，不能用于跨境网络连接
- 跨境请申请具有合法资质的专线（Direct Connect）或者 SDWAN（EC2/Marketplace AMI）
- 如果生产流量中包含事务类请求在 VPN 上通道，请考虑在第二个 AZ 配置另一个 EC2 作为路由器，实现冗余线路

3、使用 TGW Connect 连接到 SDWAN

Transit Gateway 可以通过 TGW Connect 功能与 SDWAN 集成，支持 GRE 封装和 BGP 协议，进一步简化了配置，而无须配置多个 VPN 通道。当前本 QuickStart 自动部署方案生成的环境只包含 Transit Gateway，不包含 Connect 类型的 Attachment。如果需要增加配置，请在 Transit Gateway 的 Attachment 界面创建类型为 Connect 的挂载。

-全文完-