

云上灾备管理工具用户手册

Disaster Recovery Factory User Manual

亚马逊云科技专业服务团队

版本：1.2

最后更新时间: 2020 年 8 月

Copyright (c) 2020 by Amazon.com, Inc. or its affiliates.

目 录

摘要	3
绪论	3
框架图	3
环境准备	4
EC2 实例配置	5
VPC 终端节点配置	5
VPC 虚拟网复制	5
切换	6
新建项目	7
选择 EC2 实例	8
配置启动蓝图并切换	8
简易配置向导	9
回切	10
准备环境	10
选择 EC2 实例配置启动蓝图并回切	10
最佳实践	11
结论	11
部署	11
部署资源	11
部署后配置	14

摘要

云上灾备中心解决方案通过提供云上灾备管理工具对 Amazon Elastic Compute Cloud (EC2) 实例进行迁移和保护，旨在亚马逊云科技跨区域环境下，在源区域与目的区域之间建立 EC2 实例的数据实时复制机制，以应对始料未及的灾难并有效进行灾难恢复的过程。当需要进行灾难恢复时，于目的区域按照与源区域相同或相似的参数设定，基于复制的数据启动各 EC2 实例，从而完成服务恢复和切换。本文着重介绍该过程的详细说明与操作步骤，主要涉及虚拟网和 EC2 实例数据两项内容的迁移和保护，以及正向切换与反向回切两个方向的切换操作。

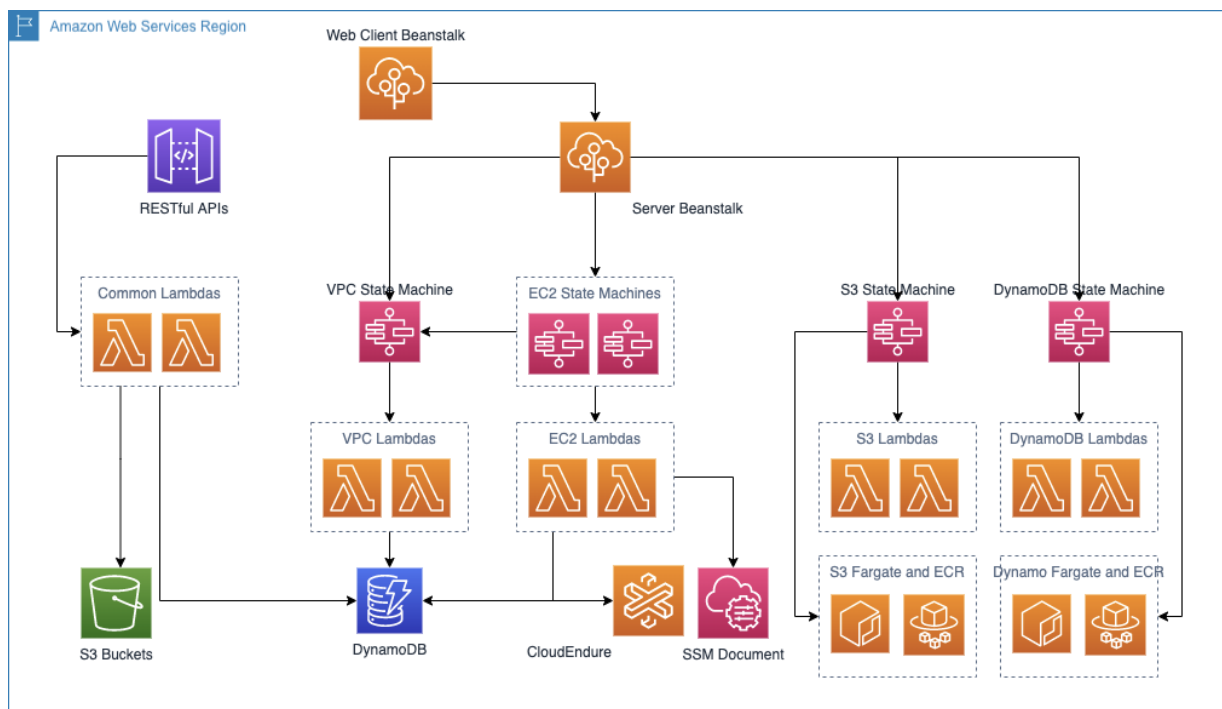
绪论

许多客户常常需要部署灾备中心，以保障关键业务应用在 IT 基础设施发生不可预知的重大故障时，能继续提供服务。灾备中心建成后，经常演练是验证灾备中心有效的常用手段。然而，使用传统方法做灾备演练，搭建环境、演练操作都过程复杂、成本高昂，难以保证常规化灾备演练。

云上灾备中心的核心是通过简洁和高效的云上灾备管理工具（以下简称灾备工具），帮助客户在亚马逊云上快速完成灾难恢复方案的部署、演练和实施，从而实现预期的业务连续性目标。该工具提供简单易用的操作界面、根据最佳实践预设的管理平台、灵活多样的数据同步方案，方便用户在混合部署环境下高效的实现数据复制、EC2 实例部署、灾备演练等操作，杜绝手工操作带来的失误。

框架图

本文着重介绍虚拟网及 EC2 实例的迁移复制与灾难恢复部分。



灾备工具对 EC2 实例迁移保护的核心思想，是实时把源区域 EC2 实例数据复制到目的区域。通过必要的网络设置，打通源区域与目的区域，两区域与管理平台之间的通讯，保持数据实时复制的畅通。当数据一致性建立后，即进入温备保护模式。当未知灾难发生或者进行灾备演练时，即可于目的区域，根据事先配置的启动蓝图，启动新的 EC2 实例，加载实时复制的数据，完成切换，从而保障服务连续性。

一个完整的 EC2 实例灾备，包括从源区域到目的区域的正向切换，也包括从目的区域回到源区域的反向回切。此时，系统恢复到最初的状态。上述两大切换步骤，皆基于两个基本要件，一是网络环境，特别是 VPC 虚拟网环境的正确设置；二是 EC2 实例的 Amazon Elastic Block Store (EBS) 数据的完整复制及数据一致性建立。以下按照 EC2 实例灾备的主要步骤，依次介绍如何利用灾备工具完成 EC2 实例迁移保护操作。

环境准备

环境准备包括三个方面。其一是配置 EC2 实例配置文件，赋予必要的权限策略以便使用 Amazon Systems Manager (SSM) 的核心服务。其二是对现有虚拟网进行相应配置，使得 SSM 可以正确控制和操作私有子网中的 EC2 实例。其三是把源区域的虚拟网完整复制到目的区域，为 EC2 实例切换准备好网络环境。

EC2 实例配置

EC2 实例配置主要是对实例配置文件的设定，必须包含策略 `AmazonSSMManagedInstanceCore`，使得 EC2 实例具有使用 Amazon Systems Manager 核心服务的权限。之后在灾备工具中选择 EC2 实例的时候，如果 EC2 实例的实例配置文件没有包含该策略，则会被过滤而不能被选择。

VPC 终端节点配置

灾备工具利用 SSM 与 EC2 实例交互，主要用 Run Command 功能来批量安装客户端代理软件，进行数据复制通信。如果 EC2 实例在私网中，且不希望 SSM 通过互联网访问这些 EC2 实例，那么还需要对所属的 VPC 虚拟网终端节点做相应配置。具体来说，需要正确配置 `ssm`, `ec2messages`, 和 `ssmmessages` 这三个终端节点服务：

- 建立服务对应的终端节点，并勾选 EC2 实例所在子网
- 启用私有 DNS 名称属性
- 安全组允许 EC2 实例访问 443 端口（例如对安全组自身开放，或者对所在虚拟网开放）

完成上述配置后，SSM 即可以为私网中的 EC2 实例顺利运行 Run Command 命令。

VPC 虚拟网复制

准备工作还包括在目的区域复制一份和源区域一模一样的虚拟网，以承载新的 EC2 实例。在导航栏中选择 环境准备 → VPC 虚拟网。按下图所示新建虚拟网复制项目。项目新建后，名称和区域不能再次修改，且区域信息必须与 EC2 实例迁移区域信息保持一致。

新建虚拟网复制项目

名称

test-vpc-use1-usw1

至少 5 个字符

源区域

us-east-1

暂不支持政府区域

目的区域

us-west-1

暂不支持政府区域

取消 新建

虚拟网复制的具体内容包括 VPC，DHCP，子网，网络 ACL，NAT 网关，安全组及其规则，Egress 网关，互联网网关，路由表，终端节点等。根据虚拟网复杂度，复制时间约为数分钟。复制虚拟网时，灾备工具会在 Amazon DynamoDB 数据库中记录所有源区域和目的区域资源的一一对应关系。一个虚拟网同一个时间只会记录一份此类关系。故当为同一个虚拟网再次复制后，前次记录的对应关系即被抹去不能使用。虚拟网复制是 EC2 实例复制的前置条件。

在 EC2 实例页面选择 VPC 虚拟网 → 添加复制项 选择 VPC 虚拟网并开始复制。在复制虚拟网时，可以对其 CIDR 块进行修改。例如从 10.0.0.0/16 改为 20.0.0.0/16。此功能旨在解决潜在 IP 地址冲突的问题。根据虚拟网复杂程度，复制时间在数分钟左右。

切换

虚拟网复制妥当后，即可开始 EC2 实例灾备准备。EC2 实例复制技术主要是基于 EBS 数据的复制来完成的。用灾备工具进行 EC2 实例迁移和保护的优势主要体现在：

- 尽可能简化手工操作步骤。通过提供最佳实践方案，最大化自动化程度，减少人工判断和干预过程。
- 批量管理 EC2 实例，一键对多 EC2 实例安装客户端软件，一键对多 EC2 实例配置启动蓝图。
- 通过对 VPC 虚拟网复制建立两区域资源对应关系数据，自动填充相关网络信息，自动配置启动蓝图。

新建项目

在导航栏中选择 温备 → EC2 实例。按下图所示新建 EC2 实例迁移项目。项目新建后，名称、区域、密钥等所示信息不能再次修改。数据传输可以经由公共互联网传输，也可以经由亚马逊云私有虚拟网传输。公网传输对现有 VPC 无需进行任何修改。私网传输则是通过建立 VPC 对等实现的，且需要添加相关路由。左下角源区域 VPC 虚拟网指的是在上一步中复制妥当的源端虚拟网。如果虚拟网复制失败，此处则无虚拟网可选。缺省机型是指当目的区域没有源区域机型时，启动 EC2 实例所采用的默认机型。

新建 EC2 实例复制项目

☑ 查询已复制的虚拟网

名称
test-ec2-use1-usw2-project
至少 5 个字符

☒ 私网传输
数据经私网而非互联网传输。但需建立 VPC 对等连接，并添加相关路由。

☐ 公网传输
数据经互联网传输。无需对现有 VPC 进行任何更改，对 CIDR 无限制。

🔑 公钥

Access Key

🔑 密钥

Secret Key

源区域
us-east-1
暂不支持政府区域

目的区域
us-west-2
暂不支持政府区域

源区域 VPC 虚拟网
vpc-0bbe00a0721...
复制妥当的源端虚拟网

缺省源端机型
t2.micro
回切无对应机型时使用

缺省目的端机型
t2.micro
正切无对应机型时使用

取消 新建

点击新建后，灾备工具即建立 EC2 实例复制项目。此处的项目名称不能重名，否则会报错。所以新建项目 workflows 中有一步是判断是否重名。上述信息在项目建立以后均不能再次修改。如果必须修改，可将项目删除后，用新信息重新建立项目。如果源区域没有 SSM 安装脚本的文档，灾备工具会在最开始时于源区域部署 SSM 安装脚本。

选择 EC2 实例

在项目主表中选择一个温备项目，在右上角菜单选择 EC2 实例 → 添加 EC2 实例。满足以下两个条件的 EC2 实例会被显示出来以备选：

1. EC2 实例的实例配置文件包含策略 AmazonSSMManagedInstanceCore
2. EC2 实例所在的虚拟网与温备项目的虚拟网相同

勾选欲添加的 EC2 实例后，点击 安装代理软件，灾备工具即通过 SSM 安装数据复制客户端代理软件。稍等片刻，可以通过源端事件表查看代理软件安装情况。例如：

- 开始安装后，会出现：Attempting to install agent on machine i-*
- 安装成功后，会出现：Agent installed successfully on machine i-*

配置启动蓝图并切换

代理软件安装成功后，灾备工具即开始跨区域复制 EC2 实例的 EBS 数据。根据数据大小，复制时长各异。可通过刷新源端 EC2 实例表实时查看数据复制情况。当待复制量为 0，完成度为 100% 时，表示数据复制完成。但仍需等待数据一致性的建立，即有数据一致性时间，且一致性建立时间距今间隔也为 0 时，表示两区域数据完全一致，可以安全进行切换操作。下图是一个数据复制完成，数据一致性也成功建立的例子。

名称 ▾	编号 ▾	待复制量 ▾	总量 ▾	完成度 ▾	最近一致时间 (UTC) ▾	距今 ▾	启动蓝图配置 ▾
ce-private-instance	i-060dc81451cf6163c	0B	8.00GB	100%	2020-05-08T10:41:52.248351Z	00:00:00	✓
ce-public-instance	i-089df47a21f1d9536	0B	8.00GB	100%	2020-05-08T10:41:52.268726Z	00:00:00	✓

切换前还必须配置启动蓝图，以示意灾备工具如何正确的启动 EC2 实例。灾备工具提供一键配置功能，利用虚拟网复制时建立的一一对应关联关系，自动填入包括机型，私网 IP 地址，子网，安全组，磁盘类型，EC2 实例实例配置文件，标签等的关键信息。在右上角菜单选择 EC2 实例 → 配置启动蓝图。配置成功后，EC2 实例表以绿色圈勾标示。

满足数据一致性，以及配置好启动蓝图两个前置条件后，则可以进行测试切换，或者正式切换。

在源端 EC2 实例表中选择欲切换的 EC2 实例，在右上角菜单选择 EC2 实例 → 测试启动 EC2 实例/正式启动 EC2 实例。测试切换和正式切换，分别对应于启动 EC2 实例时的不同启动类型，即 TEST 和 CUTOVER。稍等片刻，就可以在源端事件表中查看 EC2 实例启动情况。例如：

- 测试启动时，会出现：Initiated launch of test machine for Source machine i-*
- 正式启动时，会出现：Cutover initiated for machine i-*

之后可以登录亚马逊云控制台，在目的区域查看并验证 EC2 实例启动情况。EC2 实例正常启动后，切换即宣告完成。目前灾备工具支持一键启动多个 EC2 实例，而不考虑前后顺序。对于启动顺序有依赖关系的情况，会在以后逐步支持。

简易配置向导

从最初复制虚拟网，到建立数据一致性的前述各步骤，归纳起来有以下几大步：

1. 建立虚拟网复制项目
2. 选择虚拟网并复制到目的区域
3. 建立 EC2 实例复制项目
4. 选择 EC2 实例并安装代理软件
5. 配置 EC2 实例启动蓝图

为了简化操作，本工具提供了简易 EC2 实例温备项目创建向导，可在一个页面上完成上述一至四步。在首页选择 EC2 实例温备 → 创建向导，或者在 EC2 实例页面选择 温备向导 进入该向导页面。根据源区域和目的区域等依次填入相关信息，当所有条件正确填写后，点击“创建”进行创建。根据配置信息复杂程度，创建时间在数分钟至数十分钟左右。该向导将一至四步内容一次性配置完成，直接进入 EC2 实例数据复制状态。请注意，第五步并不包括在向导的工作中，还是需要单独点击菜单配置。

回切

反向回切 EC2 实例，是指将在目的区域切换启动成功的 EC2 实例，反方向又切换回源区域的操作。可以视为正向切换的逆操作。从整个温备项目的角度来看，相当于 EC2 实例运行情况又回到了最初的状态。虽然回切是一个逆操作，但是并不是所有步骤都是镜像对称的。通过尽可能利用正切已经准备好的基础环境，简化和省却尽可能多的操作步骤。

准备环境

准备回切环境时，不需要重新建立温备项目，而是共用已有的项目。当然，理论上也可以把回切，从一个全新的正切项目的角度来操作。此时新建温备项目以及复制虚拟网等环境准备工作就必不可少。

在主表右上角菜单选择 EC2 实例 → 准备回切。灾备工具会询问是否关闭源区域 EC2 实例。如果选择是，灾备工具则会代为关闭源区域 EC2 实例。注意，关闭 EC2 实例的操作是不可逆的。此时灾备工具会准备回切。先判断是否关闭源区域 EC2 实例，之后在源区域部署公共虚拟网，以安放组织（staging）阶段 EC2 实例。最后作为一个步骤调用新建项目的工作流，利用现有温备项目信息，反向在系统中新建一个迁移项目。

选择 EC2 实例配置启动蓝图并回切

可以在灾备工具目的端事件表中查看回切的准备工作处理情况。由于是回切操作，即默认两边虚拟网已经同步，无需再次复制。同时，项目成功建立后，接下来的回切步骤和前述正向切换大同小异，包括：

- 添加目的端 EC2 实例，安装数据复制客户端代理软件
- 一键为目的端 EC2 实例配置启动蓝图
- 等待目的端 EC2 实例数据复制完成，数据一致性成功建立
- 测试切换目的的 EC2 实例到源端直至成功，而后可以正式切换到源端

上述操作与切换时类似，但是在数据提取，特别是针对虚拟网对应关联关系的提取，也是反向的。即基于目的端映射到源端资源数据查找时，是通过目的端值找源端键，

而不是通过源端键找目的端值。当目的端 EC2 实例反向回切到源端后，即宣告该温备项目完成了回切操作，形成 EC2 实例切换闭环。此时位于源端的 EC2 实例运行状态，与最初所有操作之前的状态一致。

最佳实践

- 用户权限方面，在建立项目时需要提供密钥。此时该密钥说赋予的权限，应该按照要求的最小权限设置。
- 数据传输方面，尽可能通过私网进行传输，从而保证数据安全。但是私网传输有可能产生额外的成本开销。

结论

本文着重介绍了利用云上灾备管理工具对 EC2 实例进行跨区迁移保护、灾难切换及回切的详细过程与步骤。可以为用户高效进行灾备演练提供相关参考与操作指导。基于本工具快速部署的特性，以及图形化的简易管理平台，利用自动化工具进行灾备测试与演练，将极大提高演练效率与效用，增强系统对抗灾难的能力，减少突发灾难对系统的影响，提高系统业务连续性能力，从而最终为客户提供更加可靠和健全的业务连续性服务。

部署

本文的步骤主要针对在运行在由西云数据运营的亚马逊云科技宁夏区域或由光环新网运营的北京区域，您可以使用以下链接快速启动一个 CloudFormation 堆栈来部署和管理整个方案：

[Launch Stack](#) 

部署资源

点击链接，打开管理控制台（如果还没登录会先跳转到登录页面，登录后进入模板启动页面）。默认情况下，此模板在北京区域启动，您同时可以使用控制台右上方的区域选择链接在其他的区域启动此方案。

Create stack

Prerequisite - Prepare template

Prepare template

Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the resources you want to include in the stack.

☒ Template is ready

☐ Use a sample template

☐ Create template in Designer

Specify template

A template is a JSON or YAML file that describes your stack's resources and properties.

Template source

Selecting a template generates an Amazon S3 URL where it will be stored.

☒ Amazon S3 URL

☐ Upload a template file

Amazon S3 URL

`://aws-solutions-reference.s3.cn-north-1.amazonaws.com.cn/BCSDisasterRecoveryPortalDeployment/v1.0/DRPortal.template`

Amazon S3 template URL

S3 URL: Will be generated when URL is provided

[View in Designer](#)

点击下一步，进入详细参数的配置页面。本方案需要设置一个参数，即 CloudEndure 的 API 序列号。登录到 CloudEndure 控制台，选择任一项目，在 Setup & Info 选项卡最下方可以找到 API 序列号。将该序列号填入 CloudFormation 创建向导中的参数框。点击下一步，并在下一步的配置堆栈选项保留默认。

Setup & Info

GENERATE NEW TOKEN

API Token

3918-

When making API calls (whether from the command line or in scripts) it is best to use this token to sign in rather than your username and password. See the [API documentation](#) for more details.

REGENERATE TOKEN

Stack name

Stack name

DRPortal

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

CloudEndureApiToken

The API token provided by CloudEndure.

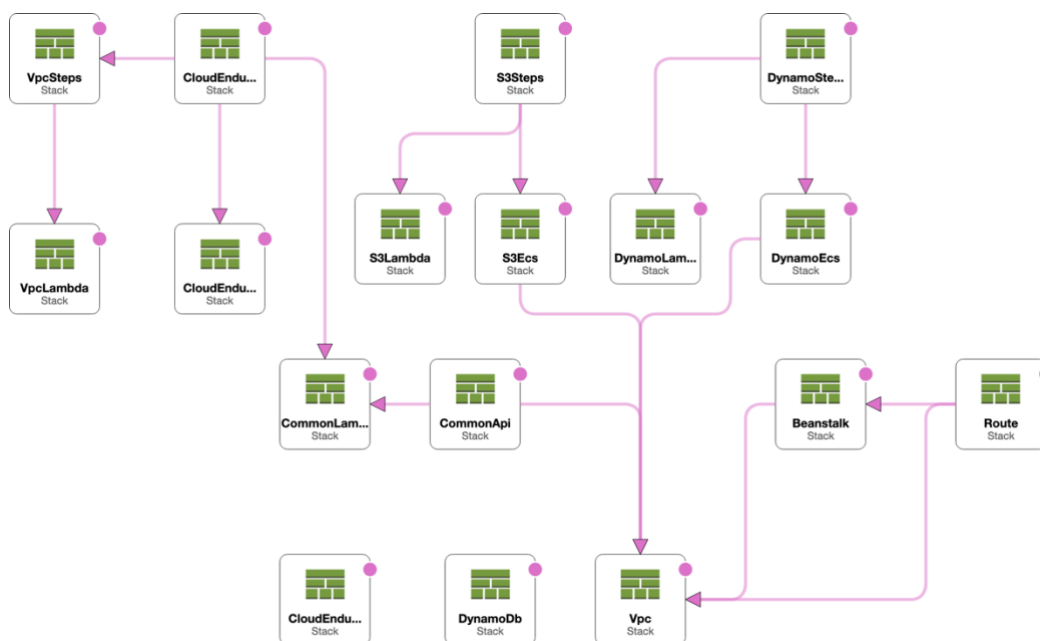
API token obtained in the CloudEndure console for your account

在最后的审核页面中，勾选最下方的【我确认，CloudFormation 可能创建 IAM 资源】选择框，因为这个解决方案需要调用 CloudWatch、Lambda、ECS Fargate 等资源，需要相应的 IAM 权限支持。接下来点击【创建堆栈】，开始堆栈的创建。

您可以在 CloudFormation 控制台的【状态】列中查看堆栈的状态，并点击右上方的刷新按钮更新状态。大约数分钟内，您可以看到堆栈状态变为 CREATE_COMPLETE，此时堆栈创建成功。

☐	DRPortal-VpcLambda-1LCRAQ8MIKX1N NESTED	✔ CREATE_COMPLETE
☐	DRPortal-DynamoLambda-1LODIA9D... NESTED	✔ CREATE_COMPLETE
☐	DRPortal-S3Lambda-17XW55L612RCL NESTED	✔ CREATE_COMPLETE
☐	DRPortal-CloudEndureLambda-2SGHC... NESTED	✔ CREATE_COMPLETE
☐	DRPortal-CommonLambda-2YY1H05A... NESTED	✔ CREATE_COMPLETE
☐	DRPortal-DynamoDb-1GC9G02SMOALS NESTED	✔ CREATE_COMPLETE
☐	DRPortal-CloudEndureSsm-QKM4880... NESTED	✔ CREATE_COMPLETE
☐	DRPortal	✔ CREATE_COMPLETE

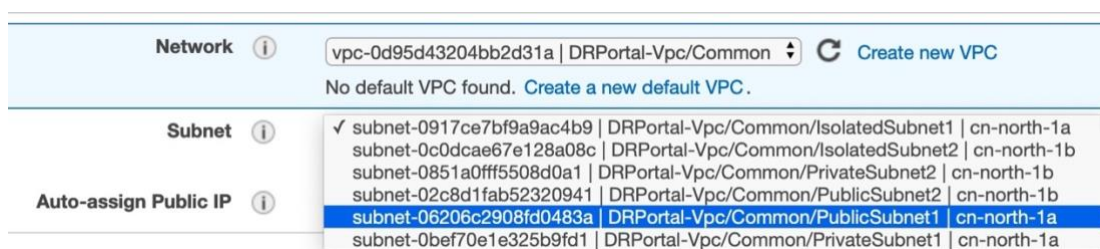
选中堆栈后短则【资源】标签，可以看到这个堆栈启动的所有资源，如果您感兴趣可以一点一点进去查看，了解每一部分的功能。各堆栈之间的相关关系如下：



部署后配置

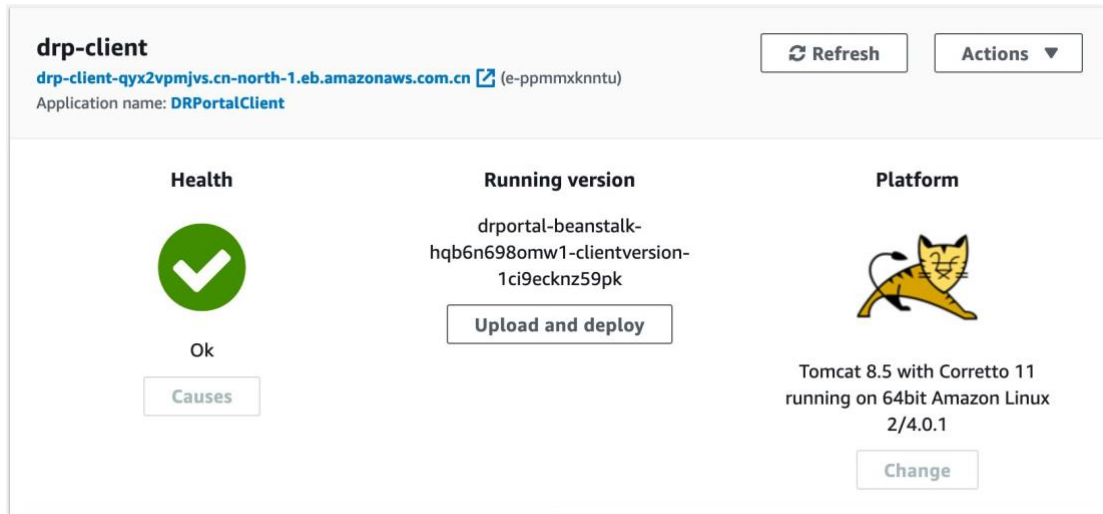
云上灾备管理工具提供一个网页应用程序与用户交互。要访问该网页程序，还需要进行以下配置。

基于安全性考虑，该网页程序不能通过互联网直接访问。所以需要通过内网访问。方法之一是在网页程序所在的 VPC 建立一个 EC2 实例，通过该实例访问网页。在 EC2 控制面板新建一个 Windows 的 EC2 实例，选择 DRPortal-Vpc/Common 这个虚拟网中的公有子网。确保实例所属安全组对你的 IP 打开 3389 端口。



在 Elastic Beanstalk 控制台找到 DRPortalClient 应用程序名为 drp-client 的环境。在环境信息页面中找到网页程序的地址，类似：

<http://drp-client-qyx2vpjmjvs.cn-north-1.elb.amazonaws.com.cn/>



利用 Microsoft Remote Desktop 连接到第一步建立的 EC2 实例，安装 Firefox。输入第二步得到的网址访问云上灾备管理工具网页客户端。

