介绍

Amazon Virtual Private Cloud (VPC)

自主进度实验室课程

版本 1.1c

spl84c-intro-vpc-1.1c

错误或更正？请发送电子邮件至 aws-course-feedback@amazon.com 联系我们。

其他问题？请通过 https://aws.amazon.com/contact-us/aws-training/ 联系我们

目录

介绍

概述

本指南向您介绍 Amazon VPC。在本实验室课程中，您将使用 Amazon VPC 向导创建 VPC、向其添加 Internet 网关、添加子网，然后为该 VPC 设置路由以便流量在 Internet 网关间传递。

所涵盖之主题

在此实验室课程结束时，您将能够：

- 创建 Amazon VPC。
- 为 Amazon VPC 设置路由。
- 在 Amazon VPC 中部署 Amazon EC2 实例。
- 向 Amazon VPC 附加 Internet 网关。
- 删除 Amazon VPC。

什么是 Amazon Virtual Private Cloud (VPC)？

Amazon Virtual Private Cloud (Amazon VPC) 允许您在 Amazon Web Services (AWS) 云中预配置出一个逻辑上隔离的部分，让您在自己定义的虚拟网络中启动 AWS 资源。您可以完全掌控您的虚拟联网环境，包括选择自有的 IP 地址范围、创建子网，以及配置路由表和网络网关。

您可以轻松自定义 Amazon Virtual Private Cloud 的网络配置。例如，您可以为能够访问 Internet 的 Web 服务器创建公有子网，而将数据库或应用程序服务器等后端系统放在不能访问 Internet 的私有子网中。您可以利用安全组和网络访问控制列表等多种安全层，帮助控制对各个子网中 Amazon EC2 实例的访问。

登录 AWS 管理控制台

登录 AWS 管理控制台

1. 单击“**启动实验**” 开始实验 。
2. 单击 “**登录网址**”，到达 AWS 管理控制台登录界面。
3. 使用这些证书登录控制台：

   在登录界面的“**用户名**”框中，输入“**账号**”。

   在“**密码**”框中，输入“**密码**”。
4. 单击“**登录**”。

创建 Amazon VPC

在本部分，您将创建一个 Amazon VPC。

5. 单击位于上方“服务”菜单，在“联网”分类中找到 VPC 并单击或是在空白搜寻栏位上直接输入 VPC。

6. 在 VPC 控制面板上，点击“**启动 VPC 向导**”。

7. 选择第一个选项“**带单个公有子网的 VPC**”，并点击“**选择**”。

8. 在“**VPC 名称**”框中，输入名称，如“myVPC”。

确认页面显示我们将用于该 VPC 和子网的 CIDR 范围（分别是 10.0.0.0/16 和 10.0.0.0/24）以及硬件租用设置。

9. 保留默认设置不变并点击“**创建 VPC**”来创建 VPC、Internet 网关、子网和路由表。

   状态窗口显示工作的进度。当工作完成时，状态窗口会确认您的 VPC 已成功创建。

10. 点击“**确定**”关闭状态窗口并返回 VPC 仪表板。

    控制台显示您的默认 VPC 和您刚刚创建的 VPC。

11. 选择“**myVPC**”，即您刚刚创建的 VPC。

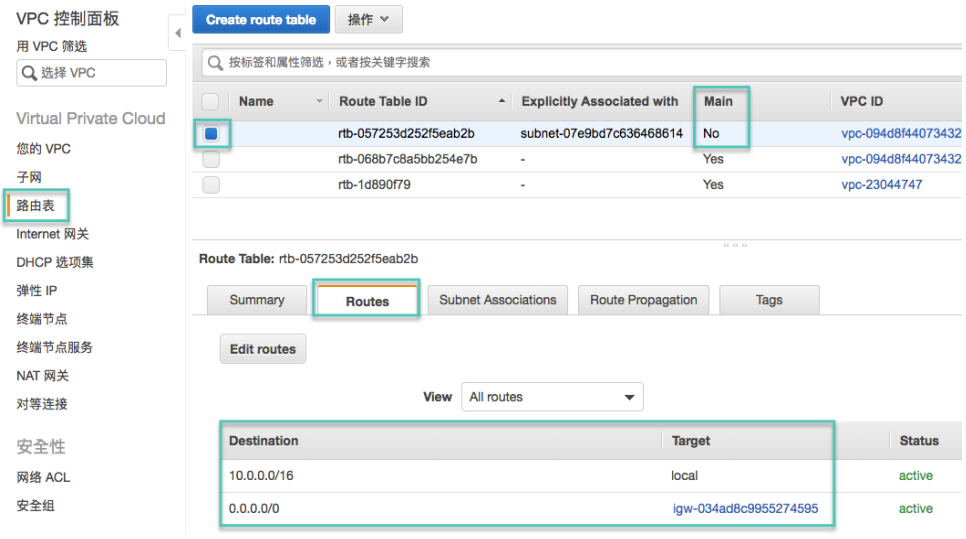
12. 要显示关于 Internet 网关的信息，请点击导航窗格中的“**Internet 网关**”。你已为您的默认 VPC 准备了一个 Internet 网关，而另一个用于您刚刚创建的 VPC。

您刚刚创建的 VPC 有两个路由表。VPC 默认自带一个主路由表，而 VPC 向导另外创建了一个自定义路由表。您的子网与自定义路由表关联，这意味着我们使用该表中的路由来确定子网流量的流动方式。如果您向 VPC 添加一个新子网，则它默认会使用主路由表。

要查看您的路由表，请执行以下操作：

13. 在导航窗格，点击“**路由表**”。

14. 选择自定义路由表（**Main** / 主路由表列为 **No**），并点击“**Routes**”选项在详细信息窗格中显示路由信息。



- 表的第一行是本地路由，用于启动 VPC 内部实例以进行通信。该路由默认显示在每个路由表中，并且不能删除。
- 第二行显示 VPC 向导添加的路由，用以支持流往 VPC (0.0.0.0/0) 外的 IP 地址的流量从子网流向 Internet 网关。我们将该子网称为*公有子网*，因为所有来自该子网的流量都流向 Internet 网关。

注意，上述的路由表与 Internet 网关皆是通过 VPC 向导由系统自动部署，若您不是通过 VPC 向导，而是自行从无到有建置 VPC 环境的话，路由表与 Internet 网关皆需要手动部署

设置安全组

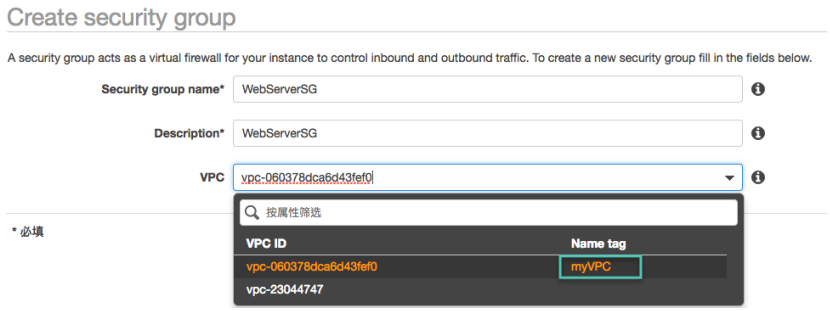
安全组充当虚拟防火墙，控制着允许进入关联实例的流量。要使用安全组，您需要创建组、添加您要使用的进站和出站规则，然后在您启动实例时，将它们与安全组关联起来。

15. 在导航窗格中点击“**安全组**” (位于左侧导航窗格中篇下方的位置)。

16. 点击“**Create Security Group**”按钮。

17. 输入 “WebServerSG”作为安全组的名称，描述的部分同样可以使用 WebServerSG。

18. 从 **VPC** 下拉列表中选择“myVPC”。



19. 点击“**Create**”。

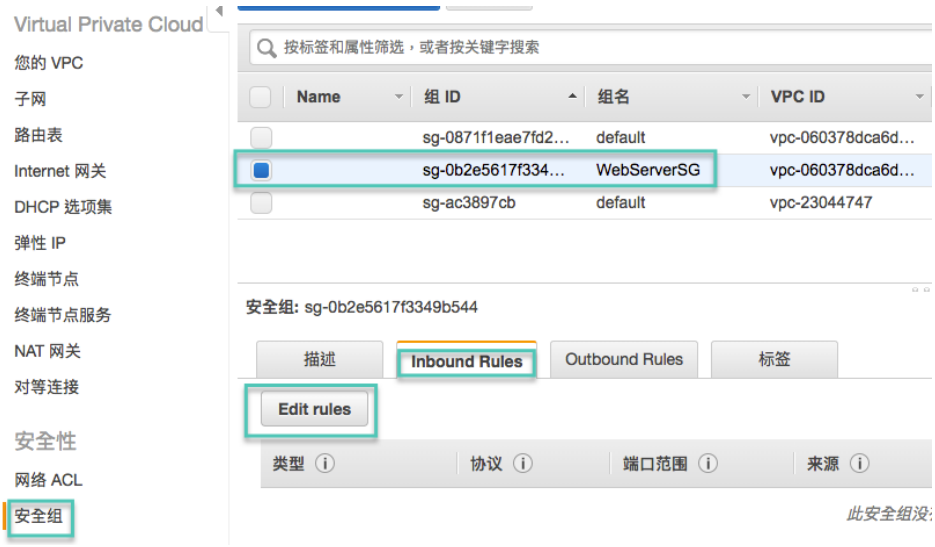
20. 创建完毕之后点击 Close 回到设定页面

现在，向安全组 **WebServerSG** 添加规则。

21. 选择您刚刚创建的“**WebServerSG**”安全组。下方视窗详细信息窗格包含显示安全组相关信息的选项卡，以及使用进站和出站规则的选项卡。

22. 点击“**Inbound Rules(入站规则)** ”选项卡。

23. 点击“**Edit rules**”。



24. 点击“添加规则”。

25. 从“**类型**”下拉列表中选择“**HTTP**”。

26. 在“**来源**”字段输入“**0.0.0.0/0**”。

27. 再次点击“**添加规则**”。

28. 从“**类型**”下拉列表中选择“**HTTPS**”。

29. 在“**来源**”字段输入“**0.0.0.0/0**”。

30. 再次点击“**添加规则**”。

31. 从“**类型**”下拉列表中选择“**SSH**”。

32. 在“**来源**”字段输入您网络的公有 IP 地址范围。在本实验室课程中，使用值 **0.0.0.0/0**。

33. 点击“**Save rules**”保存。

> **注意：**如果您使用 0.0.0.0/0，则表示您支持所有 IP 地址使用 SSH 或 RDP 访问您的实例。这在本次简短练习中是可以接受的，但是用于生产环境时不安全。在生产环境中，您将授权指定 IP 地址或地址范围访问您的实例。

启动 Web 服务器

现在，您将在您的 VPC 中创建一个 Amazon EC2 实例：

34. 在 AWS 管理控制台的首页，点击“**服务**”，然后点击“**EC2**”来打开 Amazon EC2 控制台。

35. 在控制台中，点击“**启动实例**”。
36. 在“选择一个 Amazon 系统映像(AMI)”页上，选择“**Amazon Linux AMI**”，然后点击“**选择**”。
37. 在“选择一个实例类型”页上，点击“**下一步：配置实例详细信息**”。
38. 在“配置实例详细信息”页上，“**网络**”选择“**myVPC**”
39. 在自动分配公有 IP 设定上，选择“启用”

40. 向下滚动直到“**高级详细信息**”部分并对其单击。
41. 对于**用户数据**，请选择“**以文本形式**”。

    因为您将会把您的 Amazon EC2 实例用作 Web 服务器，您需要确保 Apache httpd 服务器运行起来，且安装了 PHP 编程语言。我们可以通过简单的 Linux 外壳脚本完成此操作。下面的脚本使用 yum 软件包管理程序安装 httpd 和 PHP，然后启动 httpd 服务器。
42. 将以下初始化脚本复制粘贴到【高级详细信息】的“用户数据”框。


```
#!/bin/bash
yum install httpd -y
yum update -y
service httpd start
chkconfig httpd on
echo "<html><h1>You are AWSome!!</h1></html>" > /var/www/html/index.html
```

43. 其余部分保持默认的设定。接着点击“**下一步：添加存储**”。
44. 在“**添加存储**”页上，点击“**下一步：添加标签**”。

45. 在“**添加标签**”页上，点击”添加标签”。
46. 在“**键**”的空白栏位上输入 Name，接着在“**值**”的空白栏位上输入您的 EC2 实例的名称，如“myec2instance”，然后点击“**下一步：配置安全组**”。
47. 在“配置安全组”页上，点击“**选择一个现有的安全组**”。
48. 寻找您稍早建立的安全组名称 (**WebServerSG**) 并点击，然后再点击“**审核和启动**”。
49. 在“核查实例启动”页上，点击“**启动**”。
50. 显示新对话框：**选择现有秘钥对或创建新的秘钥对**。在该对话框中，指定您要用于该实例的密钥对。
51. 点击确认复选框。

    注意：关于管理密钥对的信息，请参阅 Amazon EC2 入门指南。
52. 当您准备好启动您的 Amazon EC2 实例时，点击“**启动实例**”。
53. 要查看实例的状态，请点击“**查看实例**”。

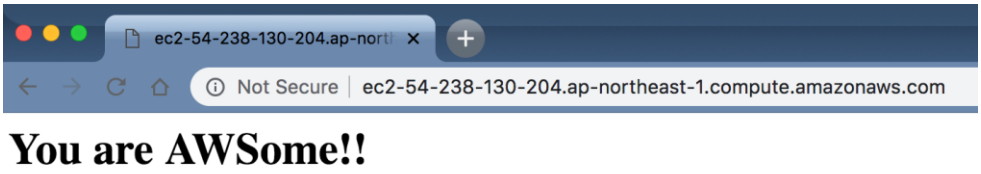
    当**实例状态**变为“**running**”并且“**状态检查**”显示“**2/2 的检查已通过**”时，即表示您的 Amazon EC2 实例已准备好。

查看您的网站

Amazon EC2 控制面板的“实例”页面上显示了当前所选区域中正在运行的所有 Amazon EC2 实例的列表。您可以在这里看到实例的状态。如果状态不是显示绿色的“*Running*”，则等待几分钟再刷新列表。

54. 选择您的实例，从而在下拉窗格中显示详细信息列表和状态更新。
55. 在列表中选择您的运行 Amazon EC2 实例 (myec2instance)。
56. 在窗口下方将**公有 DNS** 值复制到您的剪贴板中。该值看起来类似于 *ec2-54-84-236-205.compute-1.amazonaws.com.cn*。

    在此部分，您将使用新网站并查看您刚创建的网页内容。
57. 打开一个新的浏览器窗口，然后将公有 DNS 值粘贴到地址栏中。您看到的页面应该与下列页面类似：



删除您的 Amazon VPC

在您可以删除 VPC 之前，您必须先终止 VPC 中运行的所有实例。删除 VPC 也会删除与该 VPC 关联的资源，如子网、安全组、网络 ACL、DHCP 选项组、路由表以及 Internet 网关。要清除您的 AWS 资源，请执行以下操作：

58. 导航到 Amazon EC2 控制台。
59. 在导航窗格中点击“**实例**”。
60. 右击运行于 VPC 中的实例，将光标移到“**实例状态**”的上方并选择“**终止**”。
61. 看到确认提示时，点击“**是，请终止**”。
62. 导航到 Amazon VPC 控制台。
63. 在导航窗格中点击“**您的 VPC**”。
64. 选择该 VPC（名为“myVPC”）。
65. 在上方的“**操作**”下拉列表中，点击“**Delete VPC**”。
66. 看到确认提示时，点击“**Delete VPC**”。

您现在将停止因与 VPC 关联的资源而被计费。

结束您的实验室

遵循以下步骤关闭控制台、结束您的实验室。

67. 在 AWS 管理控制台的导航栏中，点击“**UPT15xxxxxxxxxx@**<AccountNumber>”，然后单击“**注销**”。
68. 关闭所有活动的 SSH 客户端会话或远程桌面会话。
69. 在云平台的实验页面上，单击“**结束实验**”。
70. 在确认消息中，单击“**确定**”。

结论

恭喜您！现在，您已成功地：

- 创建 Amazon VPC。
- 为 VPC 设置路由。
- 在 Amazon VPC 中部署 Amazon EC2 实例。

- 向 Amazon VPC 附加 Internet 网关。
- 删除 Amazon VPC。

其他资源

- 更多关于 Amazon VPC 的信息，请参阅 http://aws.amazon.com/vpc/
- 更多关于 AWS 培训和认证的信息，请参阅 http://aws.amazon.com/training/

如有反馈、建议或更正，请发送电子邮件至 aws-course-feedback@amazon.com 联系我们。