利用 Amazon 虚拟专有云扩展您的 IT 基础设施

2013 年 12 月

(请访问 http://aws.amazon.com/whitepapers/ 以获取本份白皮书的最新版本)

目录

简介

利用 Amazon Virtual Private Cloud （即 Amazon 虚拟专有云，简称 Amazon VPC），大家可以配置一套专有型隔离 Amazon Web Services（简称 AWS）云分区，并立足于此在您定义的虚拟网络当中启动各类 AWS 资源。利用 Amazon VPC，大家能够定义出一套与自有数据中心内传统网络高度相似的虚拟网络拓扑结构。大家还能够对自己的虚拟网络环境加以全面控制，具体包括选择您自己的 IP 地址范围、创建子网并配置路由表与网络网关。举例来说，利用 VPC 大家能够：

- 对现有内部基础设施加以扩展。
- 为您的环境启动一套备份堆栈以实现灾难恢复能力。
- 启动一套支付卡行业数据安全标准（简称 PCI DSS）合规网站，用以接收各安全支付操作。
- 启动隔离化开发与测试环境。
- 立足于企业网络之内提供虚拟桌面应用程序。

在使用传统方案实现上述用例时，大家可能需要大量前期投入用以构建自己的数据中心、配置必要硬件、获取所需安全认证、雇用系统管理员并保证一切正常运行。而利用 AWS 当中的 VPC 服务，大家只需承担少部分前期投入，并能够根据需要对基础设施规模进行任意伸缩。大家能够享有安全环境带来的一切助益，且无需为此支付费用; AWS 安全控制、认证、资质以及特性能够满足各类大型企业及政府机构客户提出的最为严苛的安全标准要求。欲获取相关认证与资质的完整列表，请访问 AWS 合规性中心。

本份白皮书将着重探讨 Amazon VPC 及其相关服务中的常见用例及最佳实践。

了解 Amazon 虚拟专有云

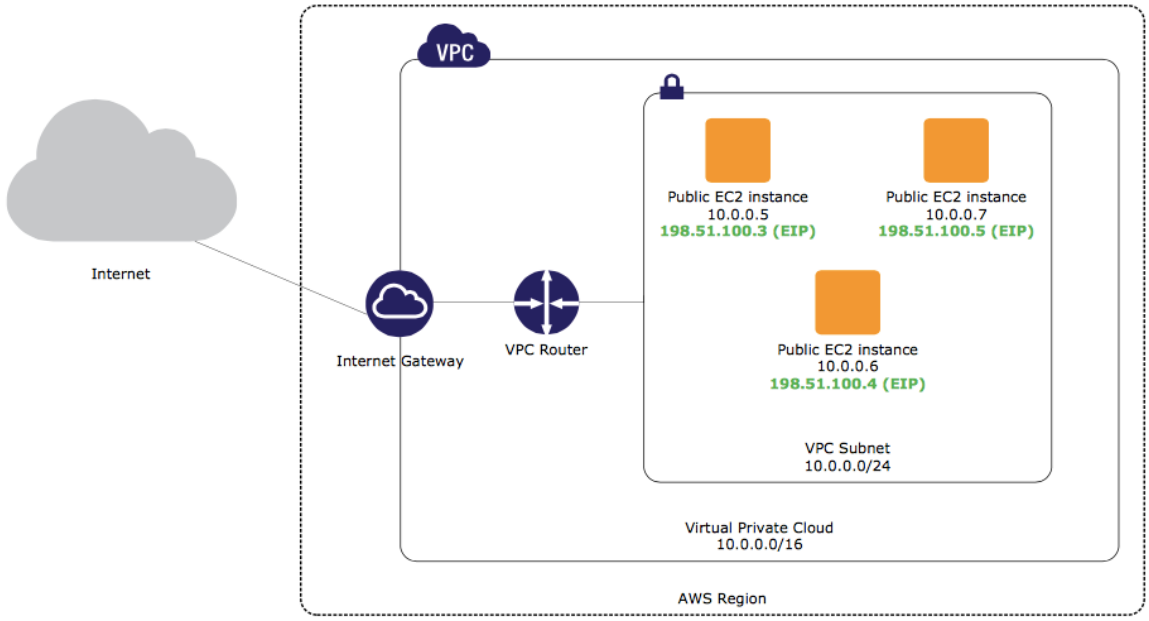
Amazon VPC 属于 AWS 云当中的一套安全、专有、隔离化分区，大家可以立足于您所定义的虚拟网络拓扑启动各类 AWS 资源。在创建一套 VPC 时，大家可以提供专有 IP 地址组以供 VPC 内的各实例使用。大家可以通过无类域间路由（简称 CIDR）块的方式指定该地址组，例如 10.0.0.0/16。大家也可以在/28（即 16 个 IP 地址）与/16（即 65536 个 IP 地址）之间随意指定块大小。

在 Amazon VPC 当中，每个 Amazon Elastic Compute Cloud （即 Amazon 弹性计算云，简称 Amazon EC2）实例都具备一个默认网络接口，其可被分配至您 Amazon VPC 网络上的一个首选专有 IP 地址。大家可以创建其它弹性网络接口（简称 ENI）并将其附加至 VPC 之内的任意 Amazon EC2 实例当中。每个 ENI 皆拥有自己的 MAC 地址。其能够拥有多个专有 IP 地址，并可被分配至特定安全组内。每套实例所能支持的 ENI 与专有 IP 地址数量取决于具体实例类型。ENI 可在同一可用区内的多套子网当中进行创建，并被附加至单一实例中用以构建诸如低成本管理网络或者网络与安全方案等。第二 ENI 及专有 IP 地址可被移动至同一子网内的其它实例当中，从而实现低成本高可用性解决方案。对于每个专有 IP 地址，大家都能够为其关联一个公共弹性 IP 地址（简称 EIP）以确保该实例能够通过互联网进行接入。大家还可以配置自己的 Amazon EC2 实例，确保其在启动时被分配予一个公共 IP 地址。被分配至您实例的公共 IP 地址来自 Amazon 的公共 IP 地址池；其不会与您的账户相关联。凭借着多 IP 与 EIP 的支持，大家能够在单一服务器之内使用多套 SSL 证书并将每套证书关联至单一特定 IP 地址。

大家可以在自己的 VPC 当中部署的组件数量默认存在上限，具体信息请参阅 Amazon VPC 限制条款。要申请提升其中部分限制，大家需要填写 Amazon VPC 限制表单。

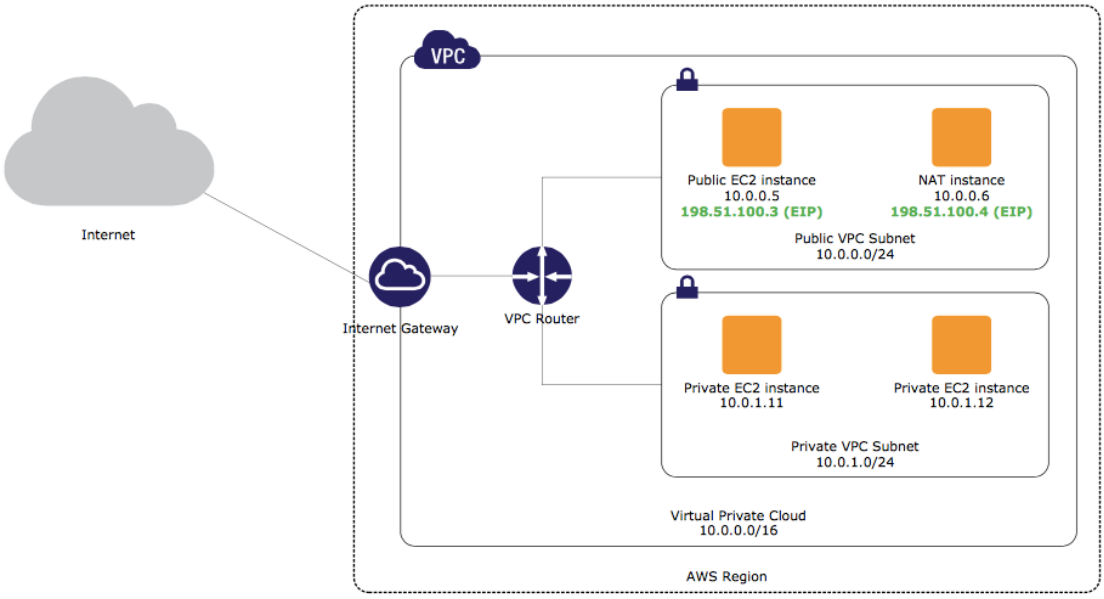
不同网络隔离级别

大家可以将自己的 VPC 子网设置为公共、专有或者仅 VPN 形式。为了设置一套公共子网，大家需要配置其路由表，从而确保来自该子网且指向互联网的流量能够经由与该 VPC 相关联的互联网网关进行路由，具体参见图一。通过将 EIP 地址分配给该子网内的各个实例，大家能够确保这些实例同样可与互联网相对接。作为一项最佳实践，建议大家通过使用有状态安全组规则对各实例加以管理，从而确保其传入与传出流量受到控制。无状态网络过滤机制同样可通过设置网络访问控制列表（简称 ACL）的形式在子网当中实现。



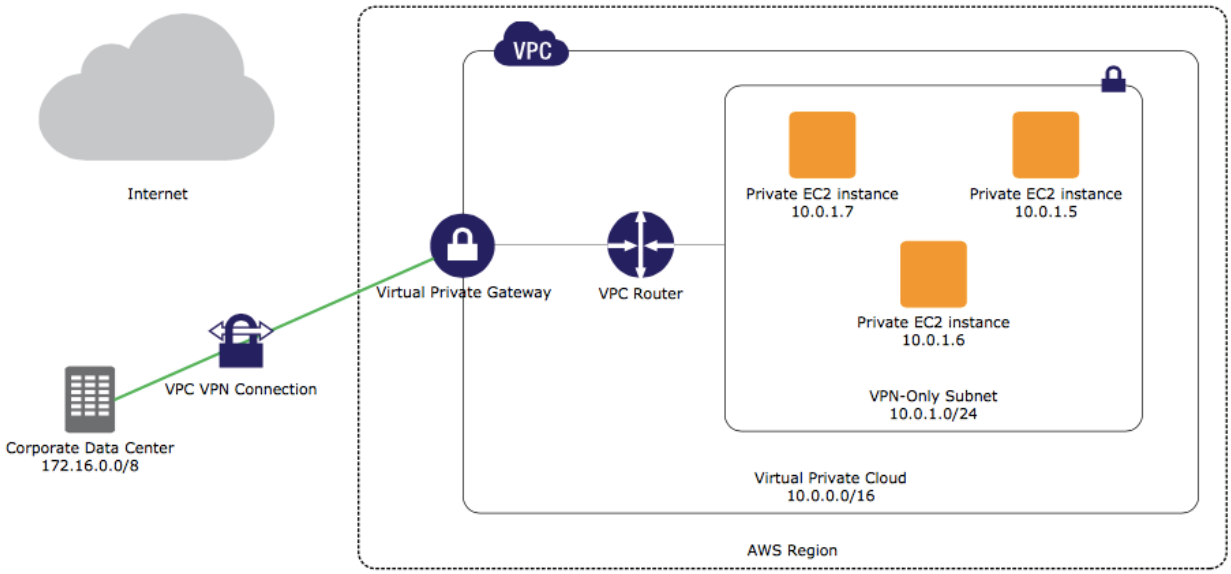
图一：仅使用公共子网的 VPC 示例

对于专有子网，指向互联网的流量可经由特定网络地址转换（简称 NAT）实例配合公共 EIP 实现路由——此公共 EIP 驻留于一套公共子网当中。这种配置方式允许大家专有子网当中的资源将出站流量接入互联网，而无需分配 EIP 或者直接接受入站连接。AWS 提供一套预配置 NAT 服务器镜像，大家也可以使用自己的定制化 AMI 以支持 NAT。图二所示为同时使用公共与专有子网的 VPC 架构。



图二：配合公共与专有子网的 VPC 示例

通过将一套虚拟专有网关附加至您的 VPC，大家可以在您的 VPC 与自有数据中心之间建立一条 VPN 连接，具体如图三所示。此 VPN 连接利用行业标准 IPsec 通道（IKEv1-PSK, AES-128, HMAC-SHA-1, PFS）作为相互认证网关，从而防止数据在传输途中被窃听或者篡改。为了实现冗余效果，每条 VPN 连接皆拥有两条通道，每条通道皆使用惟一的虚拟专有网关公共 IP 地址。



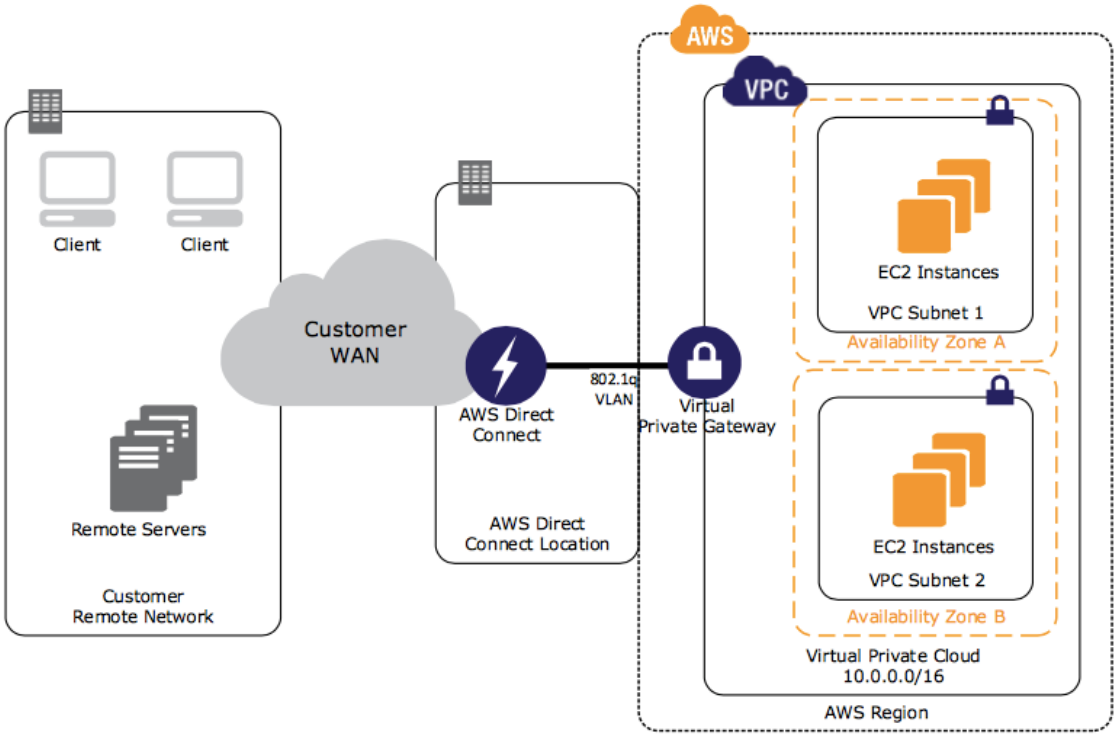
图三：与互联网相隔离，并利用 VPN 接入企业数据中心的 VPC 示例

大家拥有两种路由选项，可用于设置一条 VPN 连接：边界网关协议（简称 BGP）或者静态路由。在 BGP 方面，大家需要在将客户网关附加至 VPC 之前，了解其 IP 地址与 BGP 自治系统编号（简称 ASN）。一旦获得了这些信息，大家即可为各类不同 VPN 设备下载一套配置模板，并对两条 VPN 通道进行配置。对于那些不支持 BGP 的设备，大家可以通过在配置 VPN 连接时为其提供对应的 CIDR 范围，从而设置一套或者多套指向内部网络静态路由器。在此之后，大家能够在自己的 VPN 客户网关以及其它内部网络设备上配置静态路由，从而通过 IPsec 通道将流量路由至您的 VPC。

如果大家选择仅保留一套由单一连接指向内部网络的虚拟专有网关，大家则可以经由 VPC 路由自己的互联网边界流量并根据现有安全策略与网络控制机制控制一切传入流量。

大家也可以使用 AWS Direct Connect 以建立一条由内部网络直接指向 Amazon VPC 的专有逻辑连接。AWS Direct Connect 提供一条专有高传输带宽网络连接，用于对接您的网络与 VPC。大家可以利用多条逻辑连接以建立指向多套 VPC 的专有连接，同时继续保持网络隔离性。

利用 AWS Direct Connect，大家可以在 AWS 与任意 AWS Direct Connect 位置之间建立起 1 Gbps 或者 10 Gbps 专用网络连接。大家可使用行业标准 802.1Q VLAN 将一条专用连接可被拆分为多条逻辑连接。通过这种方式，大家能够使用同一条连接接入多种公共资源，例如存储在使用公共 IP 地址空间的 Amazon Simple Storage Service （即 Amazon 简单存储服务，简称 Amazon S3）内的各个对象，亦可接入利用专有 IP 空间运行在 VPC 内的 Amazon EC2 实例等专有资源——且完全不影响公共与专有环境之间的隔离性。大家还可以从 AWS 合作伙伴网络（简称 APN）当中选择一家合作伙伴，从而将 AWS Direct Connect 位置中的 AWS Direct Connect 端点与您的远程网络相集成。图四所示为一套典型的 AWS Direct Connect 设置方案。



图四：利用 VPC 与 AWS Direct Connect 接入客户远程网络示例

最后，大家可以将各类不同选项加以结合，从而满足业务及安全性层面的各类策略需求。举例来说，大家可以利用虚拟专有网关将 VPC 附加至现有数据中心内，同时设置一套额外的公共子网以接入其它并未运行在该 VPC 内的其它 AWS 服务，例如 Amazon S3、Amazon Simple Queue Service（即 Amazon 简单队列服务，简称 Amazon SQS）或者 Amazon Simple Notification Service（即 Amazon 简单通知服务，简称 Amazon SNS）。在这种情况下，大家亦能够利用 IAM 角色立足 Amazon EC2 访问上述服务，同时配置 IAM 策略以保证仅允许来自 NAT 服务器弹性 IP 地址的访问请求。

示例场景

考虑到 Amazon VPC 的固有灵活性优势，大家可以利用其设计出能够满足自身业务需求的虚拟网络拓扑结构，同时确保其能够遵循不同使用场景下的 IT 安全要求。要了解 Amazon VPC 的潜在优势，下面一起了解几种最为常见的用例：

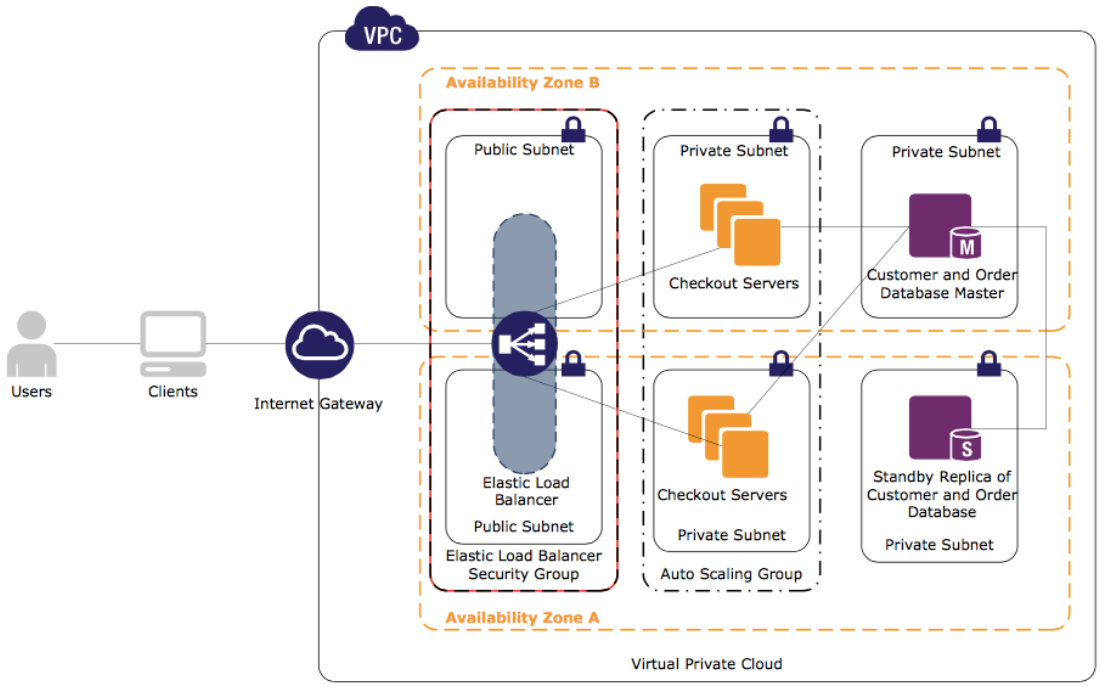
- 托管一套 PCI 合规性电子商务网站
- 构建一套开发与测试环境
- 灾难恢复与业务连续性规划
- 将您的数据中心扩展至云环境中
- 创建分支办公与业务部门网络

托管一套 PCI 合规性电子商务网站

电子商务网站通常需要处理大量敏感数据，例如信用卡信息、用户个人资料以及购买历史记录等。有鉴于此，其需要一套支付卡行业数据安全标准（简称 PCI DSS）合规基础设施，从而保护敏感客户数据。

由于 AWS 被评为一级 PCI DSS 服务供应商，因此大家能够在 PCI 合规技术基础设施之上运行自己的应用程序，从而立足云端实现信用卡信息的存储、处理与传输。作为商家，大家仍然需要管理自己的 PCI 认证，不过通过使用认证基础设施服务供应商，大家不再需要提供额外的基础设施层级 PCI 合规性证明。欲了解更多与 PCI 合规性相关的信息，请参阅 AWS 合规性中心。

举例来说，大家可以创建一套 VPC 以托管客户数据库同时管理电子商务网站的结算流程。为了实现高可用性保障，大家需要在同一服务区内的各个可用区内设置专有子网，而后将您的客户与订单管理数据库部署在各个可用区之内。大家的结算服务器将经由多个可用区间多套子网存在于一套 Auto Scaling 组内。这些服务器还将配合一套弹性负载均衡器，后者负责将各公共子网扩展至全部所用可用区内。通过将 VPC、子网、网络 ACL 以及安全组加以结合，大家能够以细粒度方式控制一切指向您 AWS 基础设施的访问活动。大家还能够确保您电子商务网站内的高度敏感性部分有能力抵御各类主要挑战——包括可扩展性、安全性、弹性以及可用性。

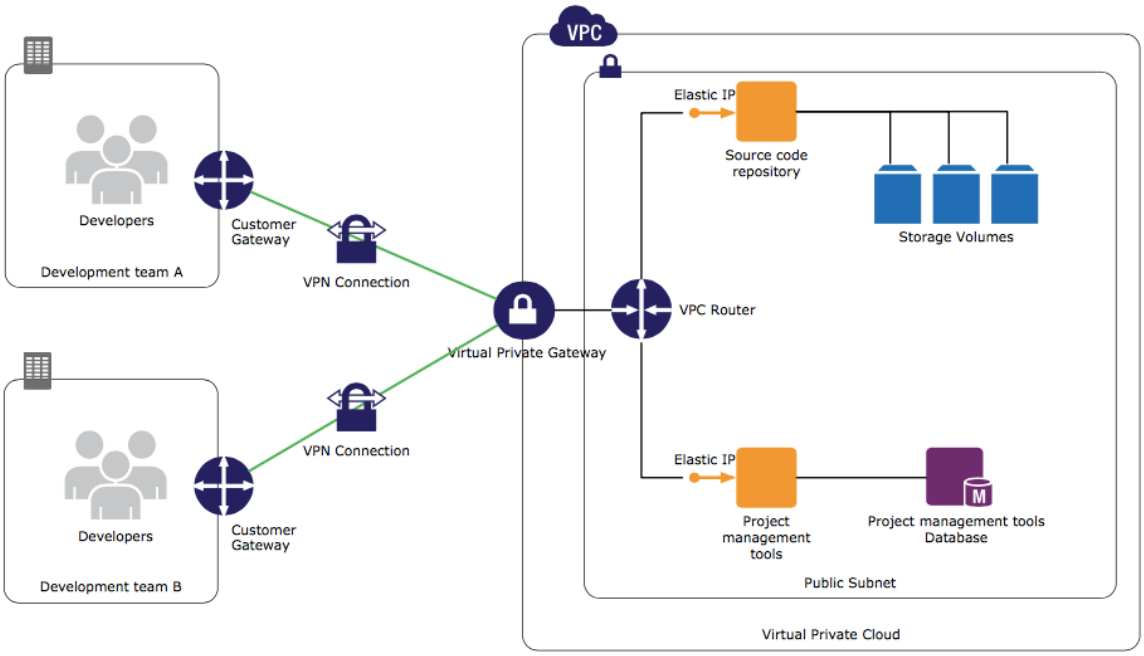


图五：结算架构示例

构建一套开发与测试环境

软件环境始终保持不断变化，其中包括新版本、新功能、新补丁以及更新的持续发布。软件变更得到快速部署，且用于测试的时间周期需要得到有效控制。理想的测试环境应当为生产环境的精确复制，大家能够在其中应用自己的更新，而后针对典型工作负载对其加以测试。当更新或者新版本通过全部测试之后，大家应该能够更具信心地将其推送至生产环境当中。

要在内部设施当中构建一套测试环境，大家需要配置大量硬件设备，且其中相当一部分长期处于闲置状态。有时候未使用硬件可能被挪作它用，意味着您可能在需要测试时无法进行灵活切换。Amazon VPC 能够帮助大家构建起一套极具经济性与功能性的测试环境，用以模拟您的实时生产环境并可在需要时随时启动，并在测试完成后立即关闭。大家不需要购置昂贵的硬件；您能够以更出色的灵活性与敏捷性实现环境变更；您的测试环境可以透明化方式利用 LDAP、消息收发以及监控机制与内部网络进行交互；另外，您只需要为实际使用的 AWS 资源付费。图六所示为一套开发与测试环境示例。



图六：开发与测试环境示例

同样的逻辑亦适用于实验性应用程序。当大家评估一套新型软件包时，大家自然希望能够保证其与生产环境相互隔离。在这种情况下，您可以将其安装在多个 VPC 测试环境内的 Amazon EC2 实例当中，而后由特定内部用户组加以访问。如果一切进展顺利，大家随后可将这些镜像迁移至生产环境并关闭不必要资源。

灾难恢复与业务连续性规划

在灾难事故的情况下，灾难事件给数据中心带来的后果可能给企业声誉造成严重影响。我们应当投入时间以制定相关策略，从而最大程度降低事故发生时运营体系受到的影响。传统灾难恢复方案通常要求使用人力密集型备份与昂贵的预备设备。相反，大家应当考虑将 Amazon VPC 纳入您的灾难恢复规划。AWS 的弹性与动态特性非常合适应对出现在灾难场景下的突发性资源需求时。

大家首先需要判断哪些 IT 资产对于您的业务运营最为关键。正如本份白皮书前文的测试环境部分所描述，大家可以通过自动化方式将您的生产环境进行复制，从而实现关键性资产功能冗余。利用自动化流程，大家能够将自己的生产数据备份至 Amazon Elastic Block Store（即 Amazon 弹性块存储，简称 Amazon EBS）分卷或者 Amazon S3 存储桶当中。大家可以编写声明式 AWS CloudFormation 模板以描述您的 VPC 基础设施堆栈，并将其自动启动于任意 AWS 服务区或者可用区当中。

在灾难事故情况下，大家可以快速在 VPC 之内启动一套环境副本，而后将您的业务流量引导至这些服务器当中。如果灾难事故影响到内部服务器并导致数据丢失，大家能够利用此前进行备份存储的 Amazon EBS 数据分卷实现信息恢复。

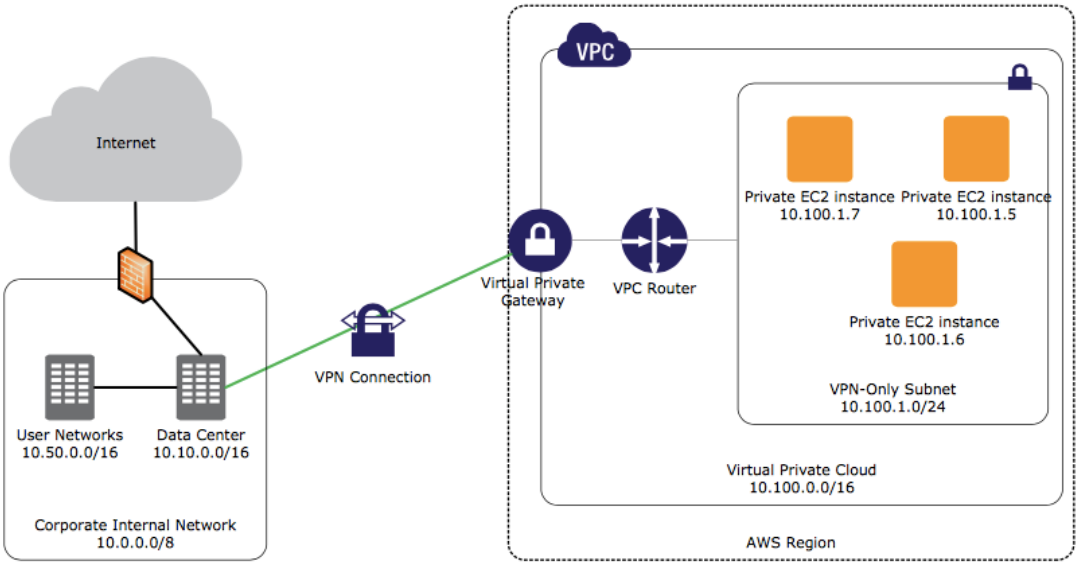
欲了解更多细节信息，请参阅《利用 Amazon Web Services 实现灾难恢复》，其包含在 AWS 架构中心网页当中。

将您的数据中心扩展至云环境中

如果大家已经投资构建了自己的数据中心，则可能在处理持续容量变更需求时面临一系列挑战。突发性资源需求峰值可能超出您的总体容量上限。如果大家的企业业务发展顺利，那么即使是日常运营需求也将最终达到您数据中心的容量上限——这意味着大家必须决定如何进行资源扩展。建立一座新数据中心当然也是一种可行方法，但这类方案成本极高且周期缓慢，同时很可能造成配置不足或者配置过高等问题。在这两类场景之下，Amazon VPC 可以作为一种非常有效的数据中心扩展手段。

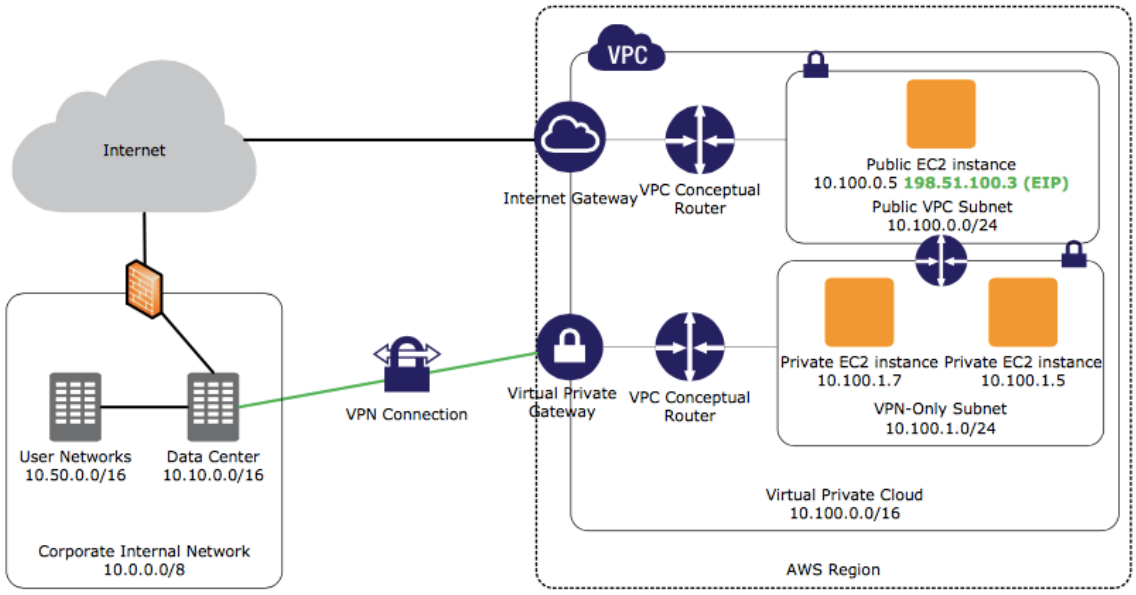
Amazon VPC 允许大家指定自己的 IP 地址范围，这样大家即可将自己的网络扩展至 AWS 当中，具体实现方式基本等同于将现有网络扩展至新的物理数据中心或者分支办公环境处。VPN 与 AWS Direct Connect 连接选项允许这些网络以无缝化及安全方式实现集成，从而创建出能够支持您全部用户及应用程序——无论其具体处于哪些位置——的单一企业网络。另外，与物理数据中心扩展工作类似，托管在 VPC 当中的 IT 资源同样能够利用现有中央 IT 系统，例如用户验证、监控、日志记录、变更管理或者服务部署等等，且无需变更用户或者系统管理员访问或管理各原有应用程序的具体方式。

大家同样能够立足于这套扩展型虚拟数据中心建立外部连接。大家可以选择将全部 VPC 流量指向至现有网络基础设施，从而控制您的 Amazon EC2 实例所能够访问的现有内部与外部网络。这套方案允许大家利用全部现有基于互联网的网络控制举措实现整体网络管理。图七所示即为将数据中心扩展至 AWS 当中的相关架构示例。



图七：利用客户的现有互联网连接将数据中心扩展至 AWS 当中

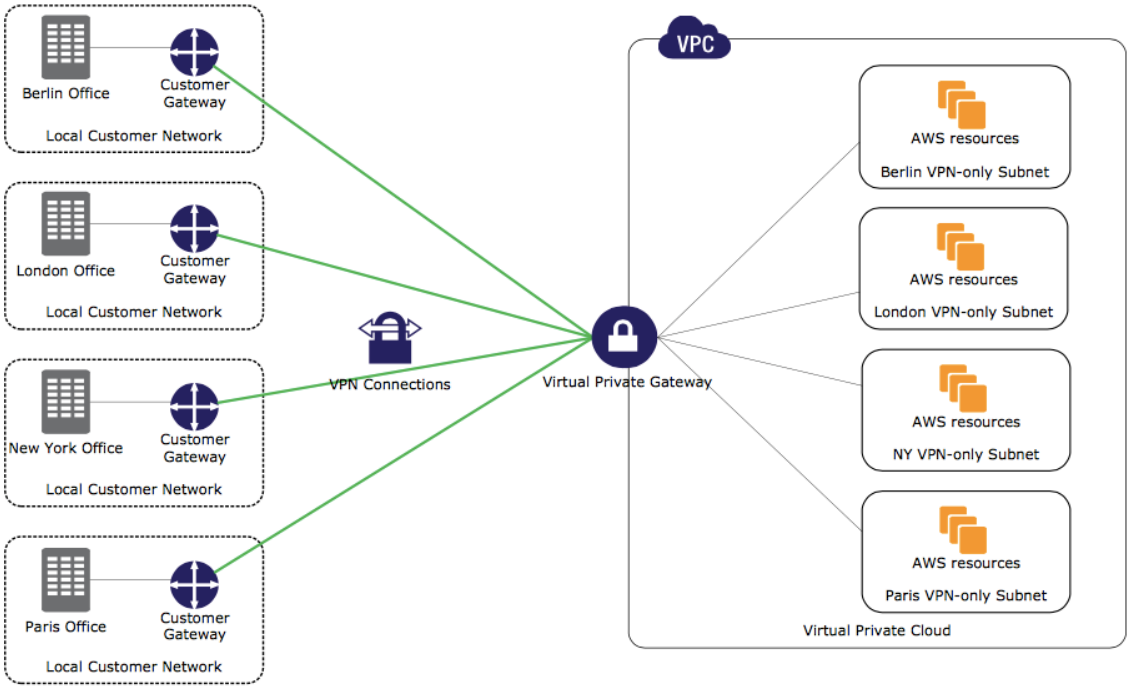
另外，大家也可以选择利用 AWS 互联网通道以处理希望直接由 VPC 交付至客户的面向互联网子网流量，同时利用 VPN 连接以后端资源提供无缝化最终用户体验，具体如图八所示。



图八：利用互联网连接将数据中心扩展至 AWS 中相关实例

创建分支办公与业务部门网络

如果大家的分支办公环境需要独立但又具备互连能力的本地网络，则可以考虑将资源部署在 Amazon VPC 当中，而后为各个办公环境分配其自有子网。VPC 子网内的应用程序能够轻松实现彼此通信，同时遵循您所设定的 VPC 安全组规则。各应用程序还能够通过虚拟路由器实现跨子网通信。如果大家需要将网络通信限制在子网之内或者之间，则可配置网络组或者网络 ACL 规则以定义各实例是否能够进行彼此通信。大家亦可以利用同样的思路根据业务部门职能进行应用程序分组。与特定业务部门相关的应用程序可被安装在独立子网之内，每套子网对应一个部门。图九所示为利用 VPC 与 VPN 构建的分支办公场景示例。



图九：利用 VPC 与 VPN 建立的分支办公场景示例

利用 Amazon VPC 相较于配置专用内部硬件以支持分支办公环境的主要优势与其它云计算方案类似：大家能够以弹性方式实现资源的横向与垂直规模伸缩从而满足具体需求，同时确保不存在资源配置不足或者过度配置的状况。添加更多容量同样非常简单：利用您的自定义 Amazon Machine Images（简称 AMI）启动更多 Amazon EC2 实例即可。当容量需求降低时，大家可以轻松手动或者利用 Auto Scaling 策略自动关闭多余的实例。尽管客户仍然需要利用运营手段确保资产正常运行，但您将不必招聘专门的远程工作人员，亦能够利用 AWS 的按实际用量计费模式节约大量开支。

Amazon VPC 使用最佳实践

在使用 Amazon VPC 时，大家应当遵循以下几条最佳实践：

- 以自动化方式部署基础设施。
- 在 VPC 中使用多可用区部署机制实现高可用性。
- 使用安全组与网络 ACL 机制。
- 利用 IAM 用户与策略控制访问活动。
- 利用 Amazon CloudWatch 监控您 VPC 实例与 VPN 链路的运行状态。

以自动化方式部署您的基础设施

以手动方式管理自有基础设施过程繁琐、易于出错、速度缓慢且成本高昂。举例来说，一旦出现灾难恢复状况，大家的规划应当仅包含少数手动操作步骤，因为其会严重影响整个流程的执行速度。即使是在重要程度较低的用例当中，例如构建开发与测试环境，我们仍然建议大家确保自己的预备环境精确对应实际生产环境。手动复制生产环境往往极具挑战，而且很可能提升出现部署依赖性相关 bug 的风险。

利用 AWS CloudFormation 实现自动化部署，大家可以以声明方式编写模板以描述您的基础设施。大家可以利用该套模板在任意 AWS 服务区内以极短时间部署预定义堆栈。这套模板能够以完全自动化方式创建子网、路由信息、安全组、AWS 资源配置——大家可根据需要自行选择。通过使用 AWS CLoudFormation 帮助脚本，大家可以使用标准 Amazon Machine Images（简称 AMI）以启动 Amazon EC2 实例，同时安装一切部署中所必需之软件的正确版本。

自动化基础设施部署方案应当被全面整合至您的业务流程当中。大家应当将自己的自动化脚本视为与软件一样需要根据标准与策略进行测试与维护的对象。大部分 VPC 用例将能够从良好的自动化策略当中获得助益。顺畅的自动化测试流程往往能够带来远优于手动方式的速度水平、成本水平、可靠性以及安全性。

在 VPC 中使用多可用区部署以实现高可用性

高可用性方面的架构设计思路往往会以冗余方式将各 AWS 资源分发至同一服务区内的多个可用区当中。如果单一可用区内的某项服务发生中断，大家可以将流量重新定向至其它可用区以控制中断事故影响。这一常规最佳实践亦适用于包含 Amazon VPC 的架构方案。

尽管 VPC 能够在多个可用区间进行跨越，但该 VPC 内的每套子网仅限于单一可用区。为了部署一套多可用区 Amazon RDS 数据库实例，大家首先需要在同一服务区内的各个数据库实例启动所在的可用区中进行 VPC 子网配置。同样的，Auto Scaling 组与弹性负载均衡器亦需要通过部署跨 VPC 子网的方式在多个可用区间进行传播。

使用安全组与网络 ACL

Amazon VPC 经由 Amazon EC2 经典环境提供额外的安全功能。VPC 安全组允许大家控制全部传入与传出流量（Amazon EC2 安全组仅能够控制传入流量），而大家亦能够为全部 IP 协议与端口定义规则。（Amazon EC2 安全组仅能够面向 TCP、UDP 与 ICMP 进行规则定义。）欲了解 Amazon EC2 与 Amazon VPC 内安全组差异的全面概述，请参阅《VPC 中的安全组》一文。Amazon EC2 与 Amazon VPC 双方的安全组皆属于有状态防火墙。

网络 ACL 属于一套额外的安全层，能够作为防火墙对传入及传出子网的流量进行控制。大家可以为每套子网定义具体的访问控制规则。尽管 VPC 安全组能够在实例层级执行，但网络 ACL 却能够在子网层级起效。对于一套网络 ACL，大家可以同时为传入与传出流量指定允许及拒绝规则。网络 ACL 属于无状态防火墙。

作为一项最佳实践，大家应当利用多个防御层对自己的基础设施加以保护。通过在 VPC 内运行您的基础设施，大家可以控制哪些实例能够通过互联网接入，同时定义安全组与网络 ACL 以进一步立足于基础设施及子网层级保护自己的基础设施。另外，大家亦应当利用操作系统层级的防火墙保护自己的各个实例，同时遵循 AWS 安全资源页面中提供的其它安全最佳实践。

利用 IAM 用户与策略控制访问活动

利用 AWS 身份与访问管理（简称 IAM）机制，大家可以在自己的 AWS 账户当中创建并管理多个用户。每个用户可属于需要与 AWS 进行交互的个人或者应用程序。利用 IAM，大家能够以集中化方式管理自己的用户、其安全凭证，例如访问凭证以及可控制用户对 AWS 资源访问活动的对应权限。大家通常需要为用户创建 IAM 用户，而为应用程序创建 IAM 角色。

我们建议大家利用 IAM 以实现最低权限安全策略。举例来说，大家不应使用自己的主 AWS 账户以管理 AWS 基础设施内的全部组件。相反，我们建议大家为不同的职能任务定义用户群组，从而限制各位用户在 AWS 之上所能执行的操作与其职能内容切实相符。举例来说，大家可以在 IAM 当中创建一个“网络管理员”用户群组，而后仅为该群组提供创建及修改 VPC 的权限。对于各个用户群组，定义严格的管理策略以确保其中用户成员仅能访问与其职能相关的服务与资源。确保只有企业内的授权人员能够访问这些用户，同时定期变更凭证以降低基础设施的安全违规风险。

欲了解更多与定义 IAM 用户与策略相关的信息，请参阅《控制对 Amazon VPC 资源的访问活动》指南。

利用 Amazon CloudWatch 以监控您的 VPC 实例与 VPN 链路运行状态

与使用公共 Amazon EC2 实例一样，大家亦可以利用 Amazon CLoudWatch 以监控运行在您 VPC 之内各个实例的性能表现。Amazon CloudWatch 提供与资源利用率、运作性能以及整体需求模式相关的查看能力，具体包括 CPU 利用率、磁盘读取与写入乃至网络流量。这部分信息将显示在 AWS 管理控制台当中，亦可经由 Amazon CloudWatch API 接受调用，意味着大家能够将其集成至您的现有管理工具当中。

大家也可以使用 AWS 管理控制台或者发起 API 调用以查看 VPN 连接的当前状态。各条 VPN 通道的状态将包含各 VPN 通道的运作状态（在线/下线），并在发生通道下线时提供错误信息。

总结

Amazon VPC 提供一系列重要工具，旨在帮助大家更为有效地控制自己的 AWS 基础设施。在 VPC 当中，大家可以通过定义子网与路由表定义您自己的网络拓扑结构，同时利用网络 ACL 与 VPC 安全组分别立足于子网层级与资源层级实现访问活动控制。大家能够将自己的资源与互联网间相隔离，同时将其经由 VPN 接入您的自有数据中心。另外，大家可以为多个实例分配弹性 IP 地址，并通过互联网网关将其接入公共互联网，同时将基础设施的其余部分继续运行在专有子网当中。VPC 帮助大家更为轻松地保护 AWS 资源，同时继续享受由 AWS 所带来的灵活性、可扩展性、弹性、性能、可用性以及按使用量付费计费模式的优势。

参考文献与扩展阅读

- Amazon VPC 产品页面: http://aws.amazon.com/vpc/
- Amazon VPC 说明文档: http://aws.amazon.com/documentation/vpc/
- AWS Direct Connect 产品页面： http://aws.amazon.com/directconnect/
- AWS Direct Connect 说明文档: http://aws.amazon.com/documentation/directconnect/
- AWS 架构中心： http://aws.amazon.com/architecture/
- AWS 合规性中心: http://aws.amazon.com/compliance/
- AWS 安全中心: http://aws.amazon.com/security/
- AWS 安全资源: http://aws.amazon.com/security/security-resources/
- Amazon VPC 连接选项:

http://media.amazonwebservices.com/AWS_Amazon_VPC_Connectivity_Options.pdf

- AWS 安全最佳实践: http://media.amazonwebservices.com/AWS_Security_Best_Practices.pdf
- 利用 AWS 实现灾难复: http://media.amazonwebservices.com/AWS_Disaster_Recovery.pdf
- 云架构设计：最佳实践：http://media.amazonwebservices.com/AWS_Cloud_Best_Practices.pdf

版本修订

2013 年 12 月

- 重大修订，用以反映 Amazon VPC 中的新功能。
- 为 Amazon VPC 添加新的用例。
- 添加章节“了解 Amazon 虚拟专有云”
- 添加新的章节“Amazon VPC 使用最佳实践”

2010 年 1 月

- 初版发布