安全流程概述

2016 年 6 月

(请咨询 **http://aws.amazon.com/security/** 以获取本份白皮书的最新版本)

通告

本文档所提供的信息仅供参考，且仅代表截至本文件发布之日时 AWS 的当前产品与实践情况，若有变更恕不另行通知。客户有责任利用自身信息独立评估本文档中的内容以及任何对 AWS 产品或服务的使用方式，任何“原文”内容不作为任何形式的担保、声明、合同承诺、条件或者来自 AWS 及其附属公司或供应商的授权保证。AWS 面向客户所履行之责任或者保障遵循 AWS 协议内容，本文件与此类责任或保障无关，亦不影响 AWS 与客户之间签订的任何协议内容。

目录

简介

Amazon Web Services（简称 AWS）提供一套具备主度可扩展能力的云计算平台，其同时具备出色的可用性与可靠性，为利用各类工具帮助客户运行多种应用程序。AWS 一直以保护客户系统与数据的机密性、完整性与可用性为核心目标。本份白皮书旨在回应经常困扰客户的各类安全性问题，例如“AWS 如何保护我的数据？”具体来讲，AWS 如何对管理下的网络与服务器基础设施提供物理与运营安全流程，同时实现指向特定服务的安全机制。

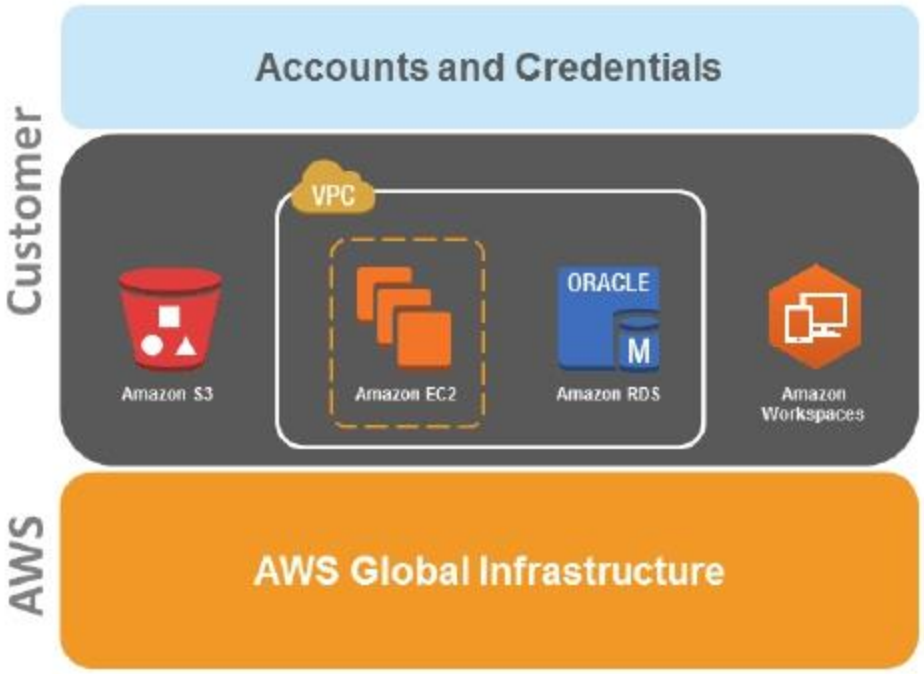
共享安全责任模式

在使用 AWS 服务时，客户仍能控制自身业务内容，同时需要负责管理关键性内容安全要求，具体包括：

- 选择将哪些内容存储在 AWS 之上。
- 利用哪些 AWS 服务处理这部分内容。
- 将内容存储在哪个国家的基础设施当中。
- 内容的格式与结构，以及是否对其进行屏蔽、匿名或者加密。
- 谁有权访问这些内容，这些访问如何进行合理细分、管理与撤销。

由于 AWS 客户仍然对其数据拥有控制权，因为他们也需要承担起对应部分责任，并作为 AWS“共享责任”模式中的组成部分。这种共享责任模式有助于理解客户与 AWS 在云安全原则背景之下的各自角色。

在共享责任模式之下，AWS 负责运营、管理及控制主机操作系统及虚拟层各个组件以及服务运行所在设施的物理安全任务。在另一方面，客户则需要负责管理其操作系统（包括更新及安装安全补丁）、其它相关应用软件以及对 AWS 提供的安全组防火墙进行配置。客户应当认真考量其选择的服务项目，因为其具体职责会根据所选择服务的不同、各服务向内部 IT 环境的集成以及应用法规与监控要求而存在巨大差别。大家可以利用主机防火墙、主机入侵检测/预防以及加密等手段显著提升安全性水平并/或满足严格的合规性要求。AWS 提供各类工具与信息，辅助客户立足自身定位高效管理并控制自己的延伸 IT 环境。欲了解更多与 AWS 合规性中心相关的细节信息，请参阅 http://aws.amazon.com/compliance。



图一：AWS 共享安全责任模式

大家需要承担的安全配置工作的具体数量在很大程度上取决于您所选择的服务项目以及数据的实际敏感度。然而，也有相当一部分安全功能，例如个人用户账户与凭证、SSL/TLS 数据传输以及用户活动日志等等，应被部署至您所使用的任意 AWS 服务当中。欲了解更多关于安全功能的细节信息，请参阅后文中的“AWS 账户安全功能”章节。

AWS 安全责任

AWS 负责对运行全部服务以提供 AWS 云的全球基础设施提供保护。这套基础设施由用于运行 AWS 服务的硬件、软件、网络以及其它设施共同构成。保护这套基础设施是 AWS 的首要任务，而且大家无法亲身前往数据中心或者办公地点查看我们的保护工作。我们将定期发布由第三方审计机构撰写的报告，由其利用各类计算安全标准与监管要求对我们的合规性水平进行验证（欲了解更多安全标准与监管要求信息，请参阅 aws.amazon.com/compliance）。

需要注意的是，除了保护全球基础设施之外，AWS 还负责对自身作为托管服务的产品进行安全配置。此类服务实例包括 Amazon DynamoDB、Amazon RDS、Amazon Redshift、Amazon Elastic MapReduce、Amazon WorkSpaces 以及多种其它服务。这些服务能够提供以云环境为基础的高度可扩展及灵活资源，同时亦可通过托管形式带来其它优势。对于此类服务，AWS 将承担基本安全任务，例如访客操作系统与数据库补丁安装、防火墙配置以及灾难恢复等等。对于大部分此类托管服务，大家只需要配置面向资源的逻辑访问控制机制，同时保护自己的账户凭证即可。其中部分服务还要求配合其它任务，例如设置数据库用户账户，但总体来讲安全配置工作基本由服务本身加以执行。

客户安全责任

利用 AWS 云，大家可以配置虚拟服务器、存储、数据库以及桌面环境，整个过程只需要数分钟而非数周。大家亦能够利用基于云的分析与工作流工具根据需要处理自己的数据，而后将其存储在云环境中或者自有数据中心之内。大家所使用的 AWS 服务将检测您在安全责任之内需要执行的具体配置工作数量。

AWS 产品包含多种易于理解及使用的基础设施即服务（简称 IaaS）方案，例如 Amazon EC2 与 Amazon VPC，其完全受客户控制并要求您对其执行必要的安全配置与管理任务。举例来说，对于 EC2 实例，大家需要负责管理访客操作系统（包括更新及安全补丁安装）、各类应用软件或者其它安装在实例上的工具，同时为每套实例配置 AWS 提供的防火墙（被称为安全组）。这些任务与大家管理自有服务器时的安全保障工作完全一致。

AWS 托管服务，例如 Amazon RDS 或者 Amazon Redshift，提供大家在执行特定任务时所需要的全部资源，但无需承担任何与之相关的配置工作。利用托管服务，大家不需要为实例启动及维护、访客操作系统或者数据库补丁安装或者数据库复制而费心——AWS 将负责一切此类工作。然而，在各项服务当中，大家都应当保护好自己的 AWS 账户凭证并利用 Amazon 身份与访问管理（简称 IAM）设置个人用户账户，从而确保每位用户都拥有自己的凭证以及与之职位相对应的操作权限。我们还建议大家在各个账户当中使用多因素验证（简称 MFA）机制，要求用户利用 SSL/TLS 与 AWS 资源进行通信，同时使用 AWS CloudTrail 设置 API/用户活动记录。欲了解更多与此类举措相关的细节信息，请参阅 AWS 安全资源页面。

AWS 全球安全基础设施

AWS 运营着全球云基础设施，大家可以利用其配置一系列基础计算资源，包括处理与存储资源等。AWS 全球基础设施当中包含设施、网络、硬件以及操作软件等等（例如主机操作系统、虚拟化软件等），其负责支持上述资源的配置与使用。AWS 全球基础设施在设计与管理当中充分考虑到安全性最佳实践以及一系列安全合规性标准。作为 AWS 客户，大家完全可以信赖这套全球安全性最高的计算基础设施，并在此基础之上构建网络架构。

AWS 合规性计划

Amazon Web Services 合规性旨在帮助客户理解 AWS 采取以维护云环境内安全性与数据保护成效的各类强大控制能力。在系统立足于 AWS 云基础设施进行构建时，合规性责任亦需要由双方进行分担。通过将治理思路、审计友好服务功能与各项合规性与审计标准相结合，采用 AWS 合规性服务的客户将能够建立并运营一套具备高度安全控制能力的 AWS 环境。AWS 提供的 IT 基础设施能够为其客户提供囊括各类安全最佳实践与 IT 安全标准的设计与管理方案，其支持的项目具体如下：

- SOC 1/SSAE 16/ISAE 3402 (即原 SAS 70)
- SOC2
- SOC3
- FISMA
- FedRAMP
- DOD SRG Levels 2 与 4
- PCIDSSLevel1
- EU Model Clauses
- ISO 9001 / ISO 27001 / ISO 27017 / ISO 27018
- ITAR
- IRAP
- FIPS 140-2
- MLPS Level 3
- MTCS

另外，AWS 平台提供的灵活性与控制能力亦允许客户部署各类解决方案，从而满足多种行业特定标准，其中包括：

- 刑事司法信息服务(简称 CJIS)
- 云安全联盟(简称 CSA)
- 家庭教育权利与隐私法案(简称 FERPA)
- 健康保险流通与责任法案(简称 HIPAA)
- 美国电影协会(简称 MPAA)

AWS 还提供多种与其 IT 控制环境相关的重要信息，旨并以白皮书、报告、认证、资质以及其它第三方证明的方式向客户交付。欲了解更多相关信息，请参阅风险与与合规性白皮书 http://aws.amazon.com/compliance/。

物理与环境安全

AWS 的数据中心拥有最为先进的规划与设计，其采用创新型建造与工程实现方法。AWS 在建造及运营大型数据中心领域拥有多年经验，而这一经验已经在 AWS 平台与基础设施当中得到全面应用。AWS 数据中心皆位于保密位置，且由专业保安人员与建筑入口处的视频监控装置、入侵检测系统及其它电子设备严格控制物理访问。授权人员必须经过至少两次双因素验证方可进入数据中心。另外，所有访客与承包商都需要出示身份证，签署责任协议并由经过授权的工作人员全程陪同。

AWS 仅向拥有合法业务需求的员工与承包商提供访问数据中心及内部信息的相关权限。当某位员工完成一项任务且不再需要此种权限，他或者她的访问资格将被立即撤销——即使其继续为 Amazon 或者 Amazon Web Services 工作。针对数据中心的全部物理访问活动皆由 AWS 员工记录并进行定期审计。

火灾检测与处理

基础设施当中安装有火灾自动探测与灭火装置，旨在降低数据中心被毁的见。火灾探测系统会在整套数据中心内安装多个烟雾探测传感器，其涵盖机械与电力基础设施空间、冷却水机组室与发电设备室等。这些区域将铺设有具备双保护联锁的预喷射水管，或者采用气体自动灭火系统。

供电

数据中心的电力供应系统在设计中充分纳入冗余与可维护机制，其不会对正常运营造成任何影响，且全天 24 小时、每周 7 天持续运作。不间断电源（简称 UPS）单元会在发生电力故障后自动起效，从而保护设施中关键性负载。各数据中心还能够利用自有发电机为整体设施提供备用电力。

气候与温度

气候控制机制负责维护服务器等硬件正常运作所需要的恒定温度，从而防止由过热引发的性能下降甚至是服务中断事故。数据中心内的空调始终将空气状态维持在最佳水平。人力与系统配合以监控并控制温度与湿度始终处于适当范围。

管理

AWS 会对系统及设备的电气、机械与生命支持状况进行持续监控，以确保快速发现任何问题。另外，AWS 还会定期执行预防性维护以保障设备的持续可操作性。

存储设备清退

当一台存储设备达到其使用寿命终点时，AWS 会通过清退流程对其加以替换，且避免在此期间客户数据为未经授权的他人所窥探。

业务连续性管理

AWS 的基础设施拥有出色的可用性水平，同时为客户提供必要功能以部署一整套弹性 IT 基础设施。AWS 在系统设计中构建起一套极具容错能力的方案，能够最大程度降低硬件故障对客户的影响。AWS 的数据中心业务连续性管理机制受到 Amazon 基础设施部门的指导。

可用性

各数据中心在全球多个地理位置建立集群。各座数据中心皆同时在线并为客户提供服务；其中不存在任何“冷门”数据中心。一旦出现故障，将有对应的自动化流程将客户数据流量引导出受影响区域。核心应用会被部署为 N+1 配置模式，这意味着当某座数据中心无法正常运行，仍将有必要容量帮助对应流量以负载均衡的方式运行在其它站点当中。

AWS 为大家提供灵活安置实例并在多个地理区域内存储数据的能力，同时亦支持客户跨越同一服务区内的多个可用区。每个可用区都作为独立故障区进行运作。这意味着同一都市区域内的各可用区彼此之间保持物理隔离，且全部位于低风险冲积平原位置（具体的洪水区判定根据不同地区而有所差别）。除了独立的不间断电源（简称 UPS）与现场备用发电设施之外，各可用区还采用不同的公共设施网格以进一步降低单点故障可能性。各可用区全部以冗余方式接入多家一级中转商。

大家应当在规划 AWS 使用方案时，充分考虑对多服务区与可用区设计优势的利用。将应用程序分发至多个可用区能够帮助大家面对大多数故障状况时继续保持理想的业务弹性，其中包括自然灾害与系统故障等等。

事故响应

Amazon 事故管理团队利用行业标准诊断规程对可能影响客户业务的各类因素加以分析。运维人员则提供 24 x 7 x 365 全天候事故检测与影响管理支持。

企业内执行审查

Amazon 的内部审计团队会定期对 AWS 弹性规划加以审查，同时亦由高层管理团队与董事会审计委员会定期加以检验。

通信

AWS 已经在全球范围内实现了多种内部通信方法，帮助各位员工了解自己的角色与职责，同时及时就重大事件进行交流。这些方法包括为新员工提供指导与培训方案; 通过运营业绩及其它事项会议调整日常管理; 利用视频会议及电子邮件等传达消息; 同时通过 Amazon 内部网络发布信息。

AWS 还利用多种外部通信机制以支持其客户群体与相关社区。已经部署到位的各类机制允许客户支持团队及时了解到会对客户体验造成影响的各类业务问题。客户支持团队还提供并负责维护“服务运行状况仪表板”，用于提醒客户关注一切可能对其业务造成影响的问题。而“AWS 安全中心”则用于帮助大家了解与 AWS 安全性与合规性相关的各类信息。大家也可以订阅 AWS 技术支持方案，其中包含与客户支持团队直接交流以及在发生任何影响客户的问题时发出提醒等服务。

网络安全

AWS 网络在架构设计当中允许大家针对自己的实际工作负载需求选择安全性与弹性级别。为了帮助大家利用云资源构建起地理隔离型高容错网络基础设施，AWS 采用世界一流网络基础设施，同时对其加以严密监控与管理。

安全网络架构

网络设备——包括防火墙与其它边界设备——已经部署到位，旨在监控并控制网络外部边界处的通信活动以及网络之内的内部边界关键行为。这些边界设备遵循预设规则集、访问控制列表（简称 ACL）以及配置机制，从而以强制性方式将信息流引导至特定信息系统服务。

ACL 或者流量流政策在各托管接口当中得到确切定义，其负责管理并引导流程或者流量。ACL 策略则由 Amazon 信息安全部门负责审批。这些策略会利用 AWS 的 ACL-Manage 工具进行自动推送，从而帮助客户确保其托管接口已经使用最新 ACL 设定。

安全接入点

AWS 在云环境中以战略性方式设定了接入点数量上限，从而更为全面地监控入站与出站通信及网络流量。这些客户接入点被称为 API 端点，其能够接纳安全 HTTP 访问（即 HTTPS），从而允许大家利用 AWS 当中的存储或者计算实例建立起一安全的通信会话。为了支持客户提出的 FIPS 加密要求，AWS GovCloud（美国）中的 SSL 终止负载均衡器符合 FIPS 140-2 标准要求。

另外，AWS 还采用了专门管理与互联网服务供应商（简称 ISP）间接口通信的网络设备。AWS 采用一套冗余型连接，这意味着 AWS 网络中各个面向互联网的边缘皆具备超过一项通信服务。这些连接各自拥有专用网络设备作为支持。

传输保护

大家可以通过 HTTP 或者 HTTPS 利用安全嵌套层（简称 SSL）接入任一 AWS 接入点，这项加密协议用于保护通信内容免受窃听、篡改或者伪造行为的影响。

对于那些希望网络安全附加层的客户，AWS 还提供 Amazon Virtual Private Cloud（即 Amazon 虚拟专有云，简称 VPC），其负责在 AWS 云内实现一套专有子网，能够利用一套 IPsec 虚拟专有网络（简称 VPN）设备在 Amazon VPC 与客户数据中心之间提供加密信道。欲了解更多与 VPC 配置选项相关的细节信息，请参阅后文中的 Amazon 虚拟专有云（简称 Amazon VPC）安全性章节。

Amazon 企业分离

从逻辑角度讲，AWS 生产网络与 Amazon 企业网络彼此分离，其各自拥有一套复杂的网络安全/分离设备。AWS 企业网络上的开发人员与管理员必须通过 AWS 申请系统提交访问请求，而后方可接入企业网络。所有请求皆需要进行审查，并确保要求之权限与该用户的工作内容切实相关。

获得批准的 AWS 用户随后可通过一套受限主机接入 AWS 网络，其限定了此次接入所能访问的网络设备及其它云组件，同时亦会记录全部行为以供安全审查。接入该主机要求使用主机上全部用户账户的 SSH 公钥验证。欲了解更多在 AWS 上实现开发人员与管理员逻辑访问，请参阅后文中的 AWS 访问章节。

容错设计

AWS 的基础设施拥有高度可用性水平，且允许大家借此部署一套弹性 IT 架构。AWS 在系统设计当中充分考虑到容错系统或者硬件故障等实际情况，旨在最大程度降低客户受到的影响。

数据中心通过分布于全球各地理位置的集群构建而成。全部数据中心皆在线运作并为客户提供服务; 其中不存在任何“冷门”数据中心。一旦发生故障，自动化流程会将客户的数据流量引导出受影响区域。核心应用则以 N+1 形式进行配置，这意味着一旦某座数据中心发生故障，其将把相关流量以负载均衡的形式引导至其它正常站点。

AWS 为大家提供灵活选项，可将实例与数据部署在多个地理区域内，亦可在同一服务区中跨越不同可用区。每个可用区在设计中皆为独立故障区。这意味着这意味着同一都市区域内的各可用区彼此之间保持物理隔离，且全部位于低风险冲积平原位置（具体的洪水区判定根据不同地区而有所差别）。除了独立的不间断电源（简称 UPS）与现场备用发电设施之外，各可用区还采用不同的公共设施网格以进一步降低单点故障可能性。各可用区全部以冗余方式接入多家一级中转商。

大家应当在设计 AWS 使用架构时充分考虑如何利用多服务区与多可用区优势。将应用程序跨越多个可用区进行分发能够保证其在面对大多数故障场景时保持良好的弹性表现，其中包括自然灾害或者系统故障。然而，大家亦应当注意不同区域内的隐私与合规性要求差异，例如欧盟数据隐私法令。除非客户主动操作，否则各地区间的数据不会自行复制，这将帮助客户更为主动地处理由地理位置带来的数据隐私要求，从而建立符合自身需求的环境。需要注意的是，各地区间的全部通信皆经由公共互联网基础设施实现; 因此，大家应当利用适当的加密手段保护敏感性数据。

截至撰稿时，AWS 共提供十二大服务区，分别为：美国东部（北弗吉尼亚州）、美国西部（俄勒冈州）、美国西部（北加利福尼亚州）、AWS GovCloud（美国）、欧洲（爱尔兰）、欧洲（法兰克福）、亚太（新加坡）、亚太（东京）、亚太（悉尼）、亚太（首尔）、南美（圣保罗）与中国（北京）。

AWS GovCloud (美国) 是一套隔离型 AWS 服务区，旨在帮助美国各政府机构与客户将工作负载迁移至云端，同时满足各类特定监管与合规性要求。AWS GovCloud（美国）框架允许美国各政府机构及其承包商遵循美国国际武器贸易条例（简称 ITAR）以及美国联邦风险与授权管理计划（简称 FedRAMP）的要求处理美国国际事务流量。AWS GovCloud（美国）已经获得了来自美国健康与人类服务部（简称 HHS）提供的授权代理运营（简称 ATO）资质，同时部分 AWS 服务还通过了由 FedRAMP 认可的第三方评估机构（简称 3PAO）进行的监管审核。

AWS GovCLoud（美国）服务区提供与其它服务区相同的容错性设计，其中包含两个可用区。另外，AWS GovCLoud（美国）服务区还默认以强制性方式以 AWS 虚拟专有云（简称 VPC）的形式交付，旨在建立一套隔离化 AWS 云分区，其中启动的各 Amazon EC2 实例皆拥有专有（RFC 1918）地址。欲了解更多细节信息，请参阅 AWS 网站上的 GovCLoud 介绍页面：http://aws.amazon.com/govcloud-us/。

图二：服务区与可用区

请注意，可用区具体数量可能发生变动。

网络监控与保护

AWS 利用一系列自动化监控系统以提供出色的安全性能与可用性保障。AWS 使用的各监控工具旨在检测入口与出口通信点上的各类异常或者未授权行为。这些工具能够监控服务器与网络使用情况、端口扫描活动、应用程序使用以及未经授权的入侵尝试等等。另外，这些工具亦能够为异常活动设置定制化性能指标阈值。

AWS 当中的系统普遍以指标为单元接受关键性运营监控。大家亦可配置警报以自动向运维及管理人员发出通知，从而保证其迟早了解到各关键性运营指标中的阈值异常。另外系统中还配备随时可用的调度机制，可供工作人员快速响应各类运营问题。其中具体包括一套分页系统，确保将警报信息快速可靠地交付至运维人员手中。

说明文档亦得到有效维护，旨在帮助运维人员用于处理各类事故或问题。如果特定问题需要进行协作解决，其中亦提供会议系统用以支持通信与日志记录功能。经过严格培训的管理者负责在运维问题处理过程中协调相关通信与进程控制工作。只要出现任何严重问题（无论是否产生外部影响），其后都将有取证工作加以配合，旨在确保找到产生问题的根源并防止类似状况再次发生。

另外 AWS 还将利用预防性措施每周对运营状况加以追踪。

AWS 安全监控工具能够帮助发现多种拒绝服务（简称 DoS）攻击，其中包括分布式、洪水式及软件/逻辑攻击。当 DoS 攻击被发现之后，AWS 事故响应流程即会被激活。除了 DoS 预防工具之外，各个服务区还配备有冗余电信供应商以及额外的容量保护机制，用于对抗可能出现的 DoS 攻击状况。

AWS 网络能够为传统网络安全问题提供有效保护，大家亦可借此结合自身需求实现更深层次的保护。以下为部分相关示例：

· 分布式拒绝服务（简称 DDoS）攻击。AWS API 端点托管在大规模互联网级别先进基础设施当中，且共享 Amazon 在建立全球最大在线零售网络过程中积累起的工程技术经验。系统中将采用适当的 DDoS 解决技术。另外，AWS 的网络体系还跨越多家供应商的多个地理区域，旨在持续提供互联网接入能力。

· 中间人(简称 MITM) 攻击。全部 AWS API 皆可通过 SSL 保护下的端点加以使用，其负责提供服务器验证机制。Amazon EC2 AMI 会在首次引导时自动生成新的 SSH 主机凭证，并将其记录在实例控制台当中。大家随后可以使用安全 API 以调用该控制台，确保在首次登录至对应实例之前访问各主机凭证。我们建议大家利用 SSL 保护一切与 AWS 的交互活动。

· IP 欺诈。Amazon EC2 实例无法发送欺诈网络流量。这套由 AWS 控制并采用主机防火墙的基础设施将不会利用实例向任意存在于自身体系之外的源 IP 或者 MAC 地址发送流量。

· 端口扫描。由 Amazon EC2 客户发起的未经授权的端口扫描会被视为违反 AWS 可接受使用政策。对 AWS 可接受使用政策的违反行为会带来严重后果，且各相关报告将作为违法活动加以研究。客户如果接触到涉嫌滥用的相关行为，可在我们的网站中进行举报：http://aws.amazon.com/contact-us/report-abuse/。当 AWS 发现未经授权的端口扫描活动，其会立即将其阻断。一般来讲，针对 Amazon EC2 实例的端口扫描将无法起效，因为默认情况下 Amazon EC2 实例的全部入站端口都会被关闭，并只能由客户手动打开。大家需要严格遵循安全组管理机制，并借此进一步应对端口扫描类威胁。如果配置的安全组允许接收来自任何来源并指向特定端口的操作，那么该端口将能够接受扫描操作。在这种情况下，大家必须使用适当的安全机制以保护监听服务，从而避免未授权端口扫描对由此被发现的应用程序造成影响。举例来说，一套 Web 服务器必须明确向外界开放端口 80（HTTP），而此服务器的管理员则负责保障 Apache 等 HTTP 服务器软件的安全工作。大家可能需要对应权限以进行漏洞扫描，从而满足特定合规性要求。然而，这些扫描操作必须限定在自身实例当中，且不得侵犯 AWS 可接受使用政策。

· 其他租户对数据包进行嗅探。对于运行在混合模式下的虚拟实例而言，各虚拟实例间将不可能接收或者“嗅探”到其它实例的流量。虽然大家以混合模式部署接口，但虚拟机管理程序不会为各虚拟实例分配地址，因此也就不会向其交付任何流量。即使两套虚拟实例存在于同一物理主机的同一集群当中，其仍然无法监听彼此的流量。ARP 缓存中毒等攻击活动无法在 Amazon EC2 与 Amazon VPC 当中起效。虽然 Amazon EC2 已经为客户提供了充分的数据隔离保障机制，但大家仍然应当对高度敏感性流量进行标准化加密。

除了监控机制之外，大家还应当利用多种相关工具对 AWS 环境中运行的各类主机操作系统、Web 应用程序以及数据库定期进行安全漏洞扫描。另外，AWS 安全团队亦提供订阅服务，可向客户提供供应商漏洞信息、主动监控供应商网站以及新型补丁推送等内容。AWS 客户亦能够通过以下地址在漏洞报告网站中向 AWS 报告各类已发现漏洞：

http://aws.amazon.com/security/vulnerability-reporting/

AWS 访问

AWS 生产网络独立于 Amazon 企业网络之外，且利用一套独立的逻辑访问凭证实现保护。Amazon 企业网络利用用户 ID、密码以及 Kerberos 保障安全，而 AWS 生产网络则要求配合堡垒主机配合 SSH 公钥验证。

使用 Amazon 企业网络的 AWS 开发人员与管理员如果需要访问 AWS 云组件，则必须通过 AWS 访问管理系统发出访问请求。全部请求都会由对应的资源持有者或者管理员进行审查与批准。

账户审查与审计

各账户每 90 天接受一次审查; 一旦过期则需要进行重新审核，否则对资源的访问会被自动拒绝。另外，如果某位员工在 Amazon 人力资源系统中被标记为已离职，则其访问同样会被自动拒绝。Windows 与 UNIX 账户会被禁用，而 Amazon 权限管理系统亦会同时将该用户从全部系统中移除。

访问中的变更请求会由 Amazon 权限管理工具审计日志所捕捉。当变更内容与员工的职能相关时，该项访问必须获得明确批准，否则请求会被自动拒绝。

背景调查

AWS 已经建立起正式策略与规程限定，作为对 AWS 平台及基础设施主机逻辑访问活动的最低管理标准。AWS 亦会在法律许可的范围之内进行刑事背景调查，并将此作为员工职位与访问级别设置合理性的预先筛查内容。该项政策亦会确定逻辑访问机制中的各项管理职责与安全性水平。

证书策略

AWS 安全团队已经建立起一套证书策略，其中包含必要的配置与到期时间间隔。密码内容必须足够复杂且每 90 天进行变更。

安全设计原则

AWS 开发流程允许执行各项安全软件开发最佳实践，其中包括由 AWS 安全团队提供的正式设计审查、威胁建模以及风险评估机制。标准构建流程将必须采用各类静态代码分析工具，且所有已部署软件必须由精心挑选的行业专家进行多次渗透测试。我们的安全风险评估工作将在设计初期阶段即行介入，并在运营过程当中持续存在。

变更管理

针对现有 AWS 基础设施的常规、紧急与配置变更需要经过授权、记录、测试及批准，同时遵循行业内类似系统的记录规范指导。针对 AWS 基础设施的更新必须确保尽可能降低对客户的影响，且基本不影响其服务使用感受。AWS 会通过电子邮件或者 AWS 服务运行状态仪表板（当服务可能面临负面影响时）与客户进行沟通。

软件

AWS 利用一套系统性方案以管理变更，从而确保可能对客户造成影响的变更活动经过严格审查、测试、批准与妥善沟通。AWS 变更管理流程在设计当中尽可能避免意料之外的服务中断，且努力为客户保持服务完整性。对部署在生产环境中的各项组件进行变更时，其必须经过：

- 审查：由技术领域同行对技术变更内容进行评审。
- 测试：各项变更必须经过测试，旨在确保其发挥与预期相符的效果且不会对性能产生负面影响。
- 批准：全部变更必须被分配以适当的授权，从而保证其对业务的影响始终处于监控及可接受范围之内。

各项变更通常会以逐进方式推送至生产环境，其起步阶段不会造成任何严重影响。另外，部署内容会在单一系统上接受测试，同时受到严格监控以保证相关影响得到有效评估。服务拥有者可利用一系列可配置指标以量化服务上游依赖性的运行状态。这些指标通过阈值及警报机制进行密切监控。变更管理申请系统还会进行详尽记录以确保回滚规程始终可行。

在可能的情况下，变更会通过常规变更窗口进行调度。指向生产系统的紧急变更在优先级方面高于标准变更管理规程，这是为了更为主动地处理突发事件并对整个过程进行记录与批准。

每隔一段时间，AWS 会对关键性服务执行自我审计以监督其质量表现、保证高标准实效并对管理流程进行持续改进。一旦出现异常状况，AWS 会对其加以分析从而确定问题根源，进而采取适当行动以保障合规性或者在必要时回滚至原有稳定版本。在此之后，AWS 会采取行动以确定引发问题的到底是流程还是人为因素。

基础设施

Amazon 的企业应用团队开发并管理相关软件，旨在立足 UNIX/Linux 主机以自动化 IT 流程实现第三方软件交付、肉痛开发软件以及配置管理工作。该基础设施团队负责维护并运营一套 UNIX/Linux 配置管理框架，用于解决硬件可扩展性、可用性、审计以及安全管理等问题。通过利用这一自动化变更管理流程实现主机集中化控制，AWS 得以充分践行基础设施的高可用性、可重复性、可扩展性、安全性与灾难恢复目标。系统与网络工程师可以连续方式监控这些自动化工具的运行状态，同时审查报告以响应故障主机，从而确保其获得或者更新必要的配置与软件。

当新硬件完成配置后，其同时会安装内部开发的配置管理软件。这些工具运行在全部 UNIX 主机之上，用于验证其是否遵循主机角色标准完成了对应配置及软件安装。这款配置管理软件还能够帮助客户定期对已经安装在主机内的软件进行补丁更新。经过批准的个人执行的各项操作，都会通过权限服务报告在各中央配置管理服务器内得到记录。

AWS 账户安全功能

AWS 提供一系列工具与功能，帮助大家用于保障自己的 AWS 账户与资源免受未授权使用的影响。其中包括各项凭证的访问控制、HTTPS 端点数据传输加密、独立 IAM 用户账户创建、用于安全监控的用户活动记录以及 Trusted Advisor（受信顾问）安全检查等等。大家可以利用一切必要安全工具对云资产加以保障，其适用于全部具体服务。

AWS 凭证

为了帮助大家确保仅有具备授权的用户及进程可访问您的 AWS 账户与资源，AWS 采用多种类型凭证以进行验证。其中包括密码、加密密钥、数字化签名以及证书等等。我们还提供多因素验证（简称 MFA）选项，用于管理 AWS 账户或者 IAM 用户账户的登录行为。以下表格展示了各类 AWS 凭证及其适用场景：

凭证类型	用例	描述
密码	用于登录至AWS管理控制台的 AWS root 账户或者 IAM 用户账户	由字符构成的字符串，用于登录至您的 AWS 账户或者 IAM 账户。AWS 密码最小长度为 6 位字符，且最高长度上限为 128 个字符。
多因素验证 (简称 MFA)	用于登录至AWS管理控制台的 AWS root 账户或者 IAM 用户账户	除了密码内容之外，用户还需要提供惟一的六位数编码以登录至 AWS 账户或者 IAM 用户账户。
访问密钥	要求利用数字签名以使用 AWS API（使用 AWS SDK、CLI 或者 REST/Query API）	包含一条访问密钥 ID 与一条访问密钥。大家可以利用访问密钥对 AWS 的编程请求进行数字签名。
密钥对	· SSHlogintoEC2 实例 · CloudFront 签名 URL · Windows 实例	要登录至您的实例，大家必须创建密钥对，在实例启动时为该密钥对指定名称，同时在接入该实例时提供对应的私钥。Linux 实例不设密码，大家可使用密钥对经由 SSH 完成登录。在 Windows 实例中，大家可使用密钥对以获取管理员密码，而后利用 RDP 完成登录。
X.509 证书	· 数字签名 指向AWS API的SOAP请求 · 用于 HTTPS 的 SSL 服务器证书	X.509 证书仅用于签署基于 SOAP 的请求（目前仅用于 Amazon S3）。大家可以利用 AWS 创建一份 X.509 证书与私钥以供下载，也可以利用证书报告功能上传自己的证书。

大家可以随时从安全凭证页面为自己的账户下载证书报告。这份报告将列出账户的全部用户以及其凭证状态——包括使用的密码、其密码是否过期、最后一次变更密码、最后一次轮换访问密钥以及是否使用 MFA 功能。

出于安全考量，如果大家的凭证丢失或者被遗忘，用户将无法将其恢复或者重新下载。然而，大家可以创建新的凭证而后禁用或者删除旧有凭证集。

事实上，AWS 建议大家定期变更（轮换）自己的访问密钥与证书。为了帮助大家避免可能给应用程序可用性造成的影响，AWS 支持多套并发访问密钥与证书。利用这项功能，大家可以定期轮换密钥及证书，而不会造成任何应用程序不可用状况。这种方式有助于消除访问密钥或者证书丢失或者外泄等隐患。AWS IAM API 可帮助大家轮换 AWS 账户以及 IAM 用户账户的访问密钥。

密码

大家在访问自己的 AWS 账户、个人 IAM 用户账户、AWS 论坛以及 AWS 支持中心时，必须提供对应密码内容。大家在初次创建账户时需要指定密码内容，并可随时在安全凭证页面当中对其进行变更。AWS 密码最大长度为 128 位字符，且可包含特殊字符，这是为了鼓励用户创建难以被猜测的高强度密码。

大家可以为自己的 IAM 用户账户设置一项密码策略，用于确保必须使用高强度密码且密码内容须频繁变更。一项密码策略实际上就是一组规则，用于定义 IAM 用户所能设置的密码类型。欲了解与密码策略相关的更多信息，请参阅使用 IAM 章节中的管理密码部分。

AWS 多因素验证(简称 AWS MFA)

AWS 多因素验证（简称 AWS MFA）属于额外安全层，用于保护 AWS 服务的访问操作。当大家启用这项可选功能时，您将需要在标准的用户名与密码凭证之外提供一条六位数字惟一编码，从而顺利接入自己的 AWS 账户设置或者 AWS 服务与资源。大家通过物理授权设备接收这一六位数编码。之所以将其称为多因素验证，是因为在接入完成前大家需要以多种因素接受身份检查：密码（记忆在脑中的传统身份验证因素）与来自授权设备的特定编码（实际持有的新型验证因素）。大家可以为自己的 AWS 账户启用 MFA 设备，亦可在利用 AWS IAM 创建 AWS 账户时为其他用户指定相关因素。另外，大家也可以为跨 AWS 账户访问创建 MFA 保护机制，例如用户可能希望立足一个 AWS 账户中的 IAM 角色访问另一 AWS 账户中的资源。在这种情况下，大家可以要求对应用户使用 MFA 以通过额外安全层验证其身份。

AWS MFA 支持使用硬件令牌与虚拟 MFA 设备。虚拟 MFA 设备采用与物理 MFA 设备相同的协议机制，但能够运行在任意移动硬件设备之上，包括智能手机。虚拟 MFA 设备利用软件应用以生成六位数字身份编码，其兼容 RFC 6238 中描述的基于时间的一次性密码（简称 TOTP）标准。大部分虚拟 MFA 应用允许大家同时托管多套虚拟 MFA 设备，这意味着其在便携性方面要优于物理 MFA 设备。然而，大家亦需要注意虚拟 MFA 的运行平台可能安全性较差，特别是在智能手机之上，因此虚拟 MFA 在安全性水平方面往往不及硬件 MFA 设备。

大家也可以为 AWS 服务 API 强制添加 MFA 验证，从而为各类重要或者高权限操作提供额外的保护层，例如终止 Amazon EC2 实例或者读取存储在 Amazon S3 中的敏感数据等。要实现这一目标，大家可以向 IAM 访问策略中添加 MFA 验证要求。另外，大家也可以将这些访问策略引入 IAM 用户、IAM 群组或者各类支持访问控制列表（简称 ACL）功能的资源中，例如 Amazon S3 存储桶、SQS 队列以及 SNS 主题等。

我们能够轻松从第三方供应商处获取硬件令牌，亦可通过应用商店下载虚拟 MFA 应用，并通过 AWS 网站将其导入。欲了解更多与 AWS MFA 相关的细节信息，请访问 AWS 网站上的相关页面。

访问密钥

AWS 要求全部 API 请求进行签名——这意味着其必须包含一条数字签名，由 AWS 用于验证请求者的实际身份。大家可以利用加密哈希功能计算该数字签名。在这种情况下，哈希功能的输入内容包括您的请求文本以及访问密钥。如果大家使用任何 AWS SDK 生成请求，则该数字签名会自动计算完成; 在其它情况下，大家可以使用自己的应用进行计算，而后通过说明文档中的指引将其导入至 REST 或者 Query 请求。

除了通过防止请求被自发以保护信息完整性之外，这一签名机制还能够避免数据在传输过程中遭遇重播攻击。根据请求时间戳，AWS 要求各请求必须在 15 分钟内到达目标位置，否则该请求会被直接拒绝。

目前最新版本的数字签名计算方案为 Signature Version 4，其能够利用 HMAC-SHA256 协议完成签名计算。版本 4 还提供额外的保护机制，要求大家明智由访问密钥提供的另一密钥进行信息签名——而非使用访问密钥本身。另外，大家也可以根据现有凭证范围进行密钥签署，其将负责以加密方式隔离该签名密钥。

一旦落入恶意人士之手，访问密钥必然会遭到滥用，因此我们建议大家将其保存在安全位置且千万不要将其嵌入至代码当中。对于那些需要对 EC2 实例进行弹性扩展的客户，使用 IAM 角色可能更加安全且易于完成对访问密钥分发机制的管理。IAM 角色提供临时性凭证，其不仅能够自动加载至目标实例当中，同时亦会在一天之内多次进行轮换。

密钥对

Amazon EC2 利用公钥加密机制对登录信息进行加密与解密。公钥加密方案利用一条公钥对数据片段进行加密——例如密码内容——而后利用私密实现数据解密。公钥与私钥的组合即被称为密钥对。

要登录到实例当中，大家必须创建密钥对，在启动实例时为该密钥对指定名称，而后在接入该实例时提供其中的私钥。Linux 实例不设密码，大家可以利用密钥对经由 SSH 完成接入。而在 Windows 实例中，大家则可以利用密钥对获取管理员密码，而后利用 RDP 完成登录。

创建密钥对

大家可以利用 Amazon EC2 创建自己的密钥对。欲了解更多相关信息，请参阅利用 Amazon EC2 创建自己的密钥对指南。

作为备选方案，大家也可以使用第三方工具并将由其生成的公钥导入至 Amazon EC2 实例。欲了解更多相关信息，请参阅将自有密钥对导入至 Amazon EC2。每个密钥对皆需要设定名称。请确保您选择的名称易于记忆。Amazon EC2 会利用大家指定的密钥名称进行公钥关联。

Amazon EC2 仅存储公钥内容，私钥则由大家自行负责存储。任何持有私钥的使用者皆可完成登录信息解密，因此请务必将私钥存储在安全位置。Amazon EC2 所使用的密钥为 2048 位 SSH-2 RSA 密钥。大家可以在每个服务区中最多保有 5000 个密钥对。

X.509 证书

X.509 证书用于签署基于 SOAP 的请求。X.509 证书当中包含一条公钥与其它元数据（例如客户上传证书时由 AWS 验证的过期日期），同时与一条私钥相关联。当大家创建一条请求时，亦同时利用私钥创建了一条数字签名，随后该签名会同证书一道被纳入请求当中。AWS 会利用证书中的公钥对签名进行解密，从而完成请求方身份验证。AWS 还会验证您所发送的证书是否与您此前上传至 AWS 的证书相匹配。

在 AWS 账户当中，大家可以使用下载获得由 AWS 创建的 X.509 证书及私钥，亦可由安全凭证页面上传您自己的证书。对于 IAM 用户，大家必须使用第三方软件创建 X.509 证书（签名证书）。相较于 root 账户凭证，AWS 无法为 IAM 用户创建 X.509 证书。在完成证书创建之后，大家利用 IAM 将其附加至 IAM 用户处即可。

除了 SOAP 请求之外，X.509 证书亦可作为 SSL/TLS 服务器证书，帮助客户利用 HTTPS 加密自己的传输流量。要将其引入 HTTPS，大家可以使用 OpenSSL 等开源工具创建一条惟一私钥。大家需要此私钥以创建证书签署请求（简称 CSR），并将此请求提交至证书颁发中心（简称 CA）以获取服务器证书。在此之后，大家即可利用 AWS CLI 将证书、私钥与凭证链上传至 IAM。

大家还需要利用 X.509 证书为 EC2 实例创建自定义 Linux AMI。该证书仅用于创建基于特定实例的专用 AMI（与基于 EBS 的 AMI 相反）。大家可以通过安全凭证页面要求 AWS 创建一份 X.509 证书与一条私钥。

个人用户账户

AWS 提供 AWS 身份与访问管理（简称 IAM）这一集中化控制机制，用于在 AWS 账户之内创建并管理个人用户。其中各用户可代表任意个人、系统或者其它需要与 AWS 资源进行交互的应用程序，且可采用编程方式或者经由 AWS 管理控制台或 AWS 命令行界面（简称 CLI）实现交互。每个用户在 AWS 账户内皆拥有惟一名称，且配备不与其他用户共享的特定安全凭证。AWS IAM 能够帮助大家摆脱密码或者密钥共享等工作，从而最大程度简化 AWS 账户凭证的使用难度。

利用 IAM，大家可以定义策略以控制用户所能访问及具体操作的 AWS 服务。大家也能够借此确保用户只具备与其职能内容匹配的必要权限。欲了解更多细节信息，请参阅后文中的 AWS 身份与访问管理（简称 AWS IAM）章节。

安全 HTTPS 接入点

为了更好地对接入 AWS 资源的通信机制进行保护，大家应当利用 HTTPS 取代 HTTP 作为数据传输载体。HTTPS 采用 SSL/TLS 协议，其借助公钥加密机制预防窃听、篡改与伪造等恶意行为。全部 AWS 服务皆提供安全客户接入点（亦被称为 API 端点），允许大家借此建立安全的 HTTPS 通信会话。

部分服务现在亦提供更为先进的加密套件，其可利用椭圆曲线 Diffie-Hellman 临时（简称 ECDHE）协议进行加密。ECDHE 允许 SSL/TLS 客户端提供完整转发安全性，即利用临时性且不存储于任何位置的会话密钥。这一机制能够在长期密钥本身遭遇泄露的情况下，继续避免未经授权宾第三方对捕捉到的数据进行解密。

安全日志

与凭证及加密端点同样重要，我们亦应当严格防止安全问题的实际发生，因此在问题发生后对日志内容进行分析就变得非常重要。另外，为了让安全工具切实起效，除了何时发生过哪些事件之外，我们还应当在日志当中对来源进行身份确认。为了帮助大家完成事后调查及近实时入侵检测，AWS CLoudTrail 提供指向您账户内各 AWS 资源的请求日志记录机制，且适用于多种受支持服务。对于每项事件，大家能够查看到访问的具体服务项目、对方执行了哪些操作以及由谁发起相关请求。CloudTrail 能够面向一切受支持 AWS 资源捕捉与 API 调用相关的信息，其中包括登录事件。

一旦大家启用了 CloudTrail，事件记录即会每五分钟进行一次交付。大家可以对 CloudTrail 进行配置，以确保其能够将来自多个服务区的日志文件汇总至单一 Amazon S3 存储桶内。在这里，大家随后可以将其上传至自己熟悉的日志管理与分析解决方案，从而执行安全分析并检测用户的行为模式。在默认情况下，日志文件会以安全方式被存储在 Amazon S3 当中，但大家也可以将其归档至 Amazon Glacier 以满足审计与合规性要求。

除了 CloudTrail 提供的用户行为日志之外，大家也可以使用 Amazon CloudWatch Logs 功能以立足于各 EC2 实例及其它来源，通过近实时方式收集并监控系统、应用程序与自定义日志文件。举例来说，大家可以监控自己的 Web 服务器日志文件，从而验证用户信息以检测指向访客操作系统的未授权登录尝试。

AWS Trusted Advisor 安全检查

AWS Trusted Advisor（即受信顾问）客户支持服务不仅能够对云服务的性能与弹性加以监控，同时亦高度关注云安全。受信顾问服务会检查您的 AWS 环境，并就成本节约、系统性能提升或者安全漏洞解决等问题提供建议与思路。此项服务提供针对多种常见安全配置错误的警报机制，包括开放某些容易受到恶意人士攻击或者非法访问的端口、忘记为您的账户创建 IAM 内部用户、允许对 Amaozn S3 存储桶进行公共访问、未启动用户活动记录（AWS CLoudTrail）或者未在 root AWS 账户中使用 MFA 等问题。大家还可以选择使用安全联系人服务，从而每周收取邮件提醒并借此了解受信顾问在安全检查中发现的最新状况等。AWS 受信顾问服务免费为全部用户提供四项检查，其中包括三项重要安全检查：root 账户特定端口未受限制、IAM 与 MFA 使用情况。如果大家购买了商业或者企业级 AWS 支持服务，那么能够自动获得全部受信顾问检查项目。

AWS 特定服务安全性

除了在 AWS 基础设施中的各个层级内置安全性保障，AWS 还将安全保障方案引入各独立服务。AWS 服务在网络与平台架构设计上充分考虑到执行效率与安全要求。每项服务皆提供广泛的安全性功能，旨在确保大家能够保护自己的敏感数据与应用程序。

计算服务

Amazon Web Services 提供一系列基于云的计算服务，其中包括多种可自动进行规模伸缩以满足应用或者企业需求的计算实例类型。

Amazon Elastic Compute Cloud (Amazon EC2)

安全性

Amazon Elastic Compute Cloud (即 Amazon 弹性计算云，简称 EC2) 属于 Amazon 基础设施即服务（简称 IaaS）当中的一大关键性组件，其负责在 AWS 数据中心内提供可随意进行计算容量伸缩的服务器实例。Amazon EC2 的设计思路旨在帮助大家顺畅完成容量的获取与配置工作，从而简化 Web 规模计算资源的实现流程。大家可以创建并启动多个实例，其中包含对应的平台硬件与软件组合。

多安全级别

Amazon EC2 中的安全性以多层级方式实现：主机平台操作系统、虚拟实例操作系统或者访客操作系统、防火墙以及签名 API 调用 。其中各个项目间彼此协同配合。其目标在于避免 Amazon EC2 中容纳的数据受到未授权系统或者用户的影响，同时亦能够在不影响配置灵活性的前提下完成 Amazon EC2 实例交付。

虚拟机管理程序

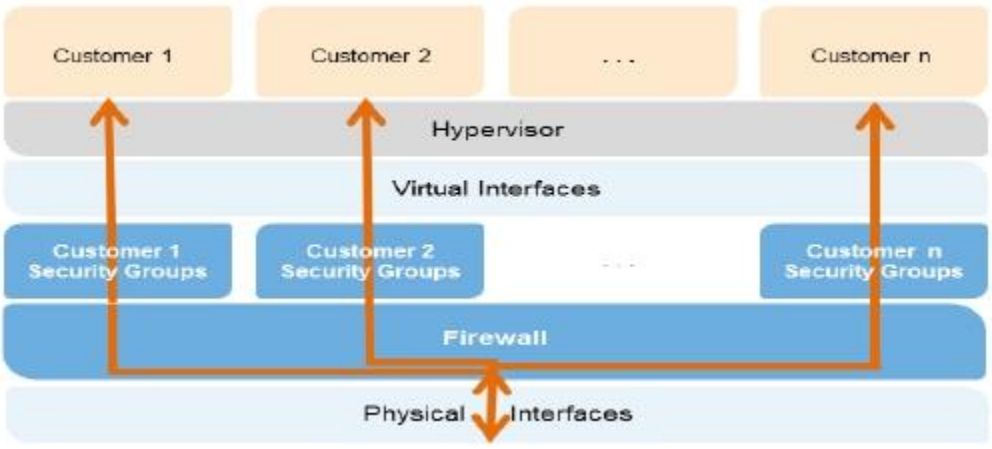
Amazon EC2 目前利用一套高度定制化 Xen 虚拟机管理程序版本，其能够充分发挥半虚拟化（在使用 Linux 访客系统的情况下）的固有优势。由于半虚拟化访客系统需要利用虚拟机管理程序为常规权限访问提供支持，因此访客系统本身并不会直接接入 CPU。CPU 提供四种独立的权限模式：0-3，且以“环（ring）”为单位。0 环代表最高权限，而 3 环代表最低权限。主机操作系统以 0 环权限运行。然而，相较于大部分操作系统的 0 环执行要求，访客操作系统则运行在权限更低的 1 环层级，应用程序则以权限最低的 3 环层级运行。这种明确的物理资源虚拟化方案将访客系统与虚拟机管理程序加以严格区分，从而为二者提供额外的安全隔离机制。

实例隔离

运行在同一物理设备上的不 同实例通过 Xen 虚拟机管理程序实现彼此隔离。AWS 在 Xen 社区当中一直高度活跃，而该社区则负责提供各类最新开发成果。另外，AWS 防火墙亦立足于该虚拟机管理层之内，位于物理网络接口与实例虚拟接口之间。全部数据包必须经由此层，因此各相邻实例之间绝对无法经由其它互联网主机访问到与之无关的物理主机。物理内存亦以同样的机制进行分区。

客户实例无法直接访问原始磁盘设备，而是接入虚拟磁盘。另外，分配给访客系统的内存亦会在实际分配之前由虚拟机管理程序加以清理（重新归 0）。这部分刚刚分配的内存不会被纳入资源池，直到其内容彻底清理完毕。

AWS 建议客户利用其它方案对自身数据加以进一步保护。此类建议方案之一在于立足 虚拟化磁盘设备运行加密文件系统：



图三：Amazon EC2 多安全层结构

主机操作系统: 因职能要求而需要访问管理面板的管理员需要利用多因素验证以接入对应的管理主机。这些管理主机属于经过特定设计、构建、配置与强化的系统，旨在保护各相关云资源的管理面板。全部相关访问皆会进行记录与审计。当员工不再 需要访问该管理面板时，其相关权限与主机访问能力皆会被立即撤销。

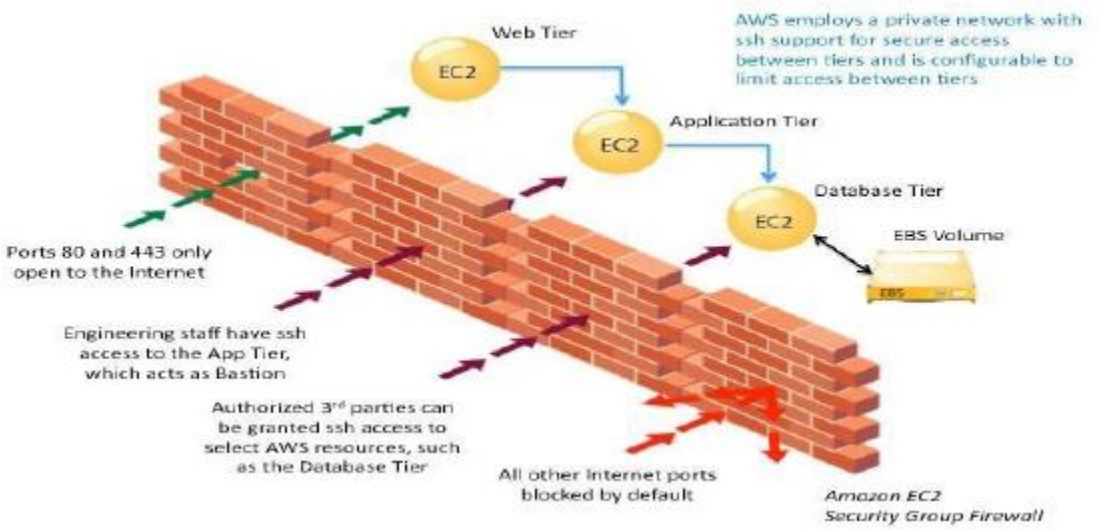
访客操作系统: 虚拟实例完全由客户负责控制。大家对于各账户、服务及应用程序拥有完整的 root 访问与管理能力。AWS 无权访问您的实例或者访客操作系统。AWS 建议大家采取基础性安全最佳实践，具体包括禁用纯密码访客系统访问机制，同时利用多因素验证方案以接入具体实例（或者至少使用基于证书的 SSH Version 2 连接）。另外，大家还应当采取权限升级机制并以每个用户为单位进行日志记录。举例来说，如果目标访客操作系统为 Linux，则大家应利用基于证书的 SSHv2 接入该虚拟实例，同时禁用远程 root 登录、使用命令行登录并使用“sudo”权限进行操作。大家还应当生成自己的密钥对，同时确保其不会为其他客户或者 AWS 所共享。

AWS 还支持利用安全 Shell（简称 SSH）网络协议以安全登录至您的 UNIX/Linux EC2 实例。AWS 利用公钥/私钥对实现 SSH 验证，旨在降低未授权访问对客户实例造成的潜在风险。大家也可以为自己的实例启用 RDP 证书，从而利用远程桌面协议（简称 RDP）远程接入 Windows 实例。

大家还需要控制访客操作系统的更新与补丁安装工作，其中包括各类安全更新。AWS 提供基于 Windows 与 Linux 的 AMI 功能，可用于定期实现最新补丁更新，这意味着大家不必再自行处理 Amazon AMI 实例中的数据保留或者定制化工作，即可顺利利用最新 AMI 重启新实例。另外，Amazon Linux AMI 还通过 Amazon Linux yum 库提供各相关更新补丁。

防火墙: Amazon EC2 提供一套完整的防火墙解决方案; 这套入站防火墙默认配置为拒绝一切模式，且 Amazon EC2 客户必须明确开启必要端口方可接收入站流量。这部分流量可由协议、服务端口以及源 IP 地址（个别 IP 或者无类别域内路由（简称 CIDR）块）等指标加以限制。

这套防火墙可通过配置对各实例进行分类，并为其执行不同的管理规则。举例来说，我们假定需要处理一款传统的三层 Web 应用程序。其中 Web 服务器组将面向互联网开放端口 80（HTTP）以及/或者端口 443（HTTPS）。而应用服务器组则仅向 Web 服务器组开放端口 8000（应用特定）。数据库服务器组将仅向应用服务器组开放端口 3306（MySQL）。全部三个分组皆可在端口 22 上提交管理访问（SSH），但仅限客户的企业网络。对安全性要求更高的其它应用程序可部署更为详尽的管理机制，具体示意图如下：



图四：Amazon EC2 安全组防火墙

该防火墙并非由访客操作系统负责控制; 相反，其要求使用客户的 X.509 证书及密钥以进行变更授权，从而添加额外安全层。AWS 支持立足不同管理功能对实例与防火墙进行细粒度访问控制，因此大家能够通过职能划分的方式进一步提升安全保障效果。防火墙所能实现的安全性水平取决于您所开放的端口及其持续时间与作用。防火墙的默认状态会拒绝一切入站流量，大家应当在构建并保护应用程序时谨慎规划所开放的端口。另外，各个实例皆需要配合良好的流量管理与安全设计方案。AWS 还鼓励大家在各实例中引入额外的主机防火墙过滤机制，具体包括 IP 表或者 Windows 防火墙及 VPN。这能够进一步对入站及出站流量加以限制。

API 访问: 用于启动及终止实例、变更防火墙参数以及执行其它功能的 API 调用全部需要由 Amazon 保密访问密钥进行签名许可——这一密钥可由 AWS 账户保密访问密钥充分，亦可使用用户利用 AWS IAM 创建的保密访问密钥。如果未能访问您的保密访问密钥，Amazon EC2 API 调用将无法完成既定操作。另外，API 调用亦可利用 SSL 进行加密，从而进一步提升安全保障。AWS 建议大家始终使用 SSL 保护下的 API 端点。

权限: AWS IAM 还允许大家控制用户权限之内所能使用的具体 API。

Elastic Block Storage (即弹性块存储，简称 Amazon EBS) 安全性: Amazon 弹性块存储（简称 EBS）允许大家创建容量在 1 GB 到 16 TB 区间的存储分卷，并由 Amazon EC2 实例作为设备进行挂载。各存储分卷的运行方式与原始未格式化块存储设备一致，用户需要为设备提供名称及块设备接口。大家可以立足于 Amazon EBS 分卷创建一套文件系统，或者直接将其作为块存储设备（例如磁盘驱动器）加以使用。Amazon EBS 分卷访问仅限于创建该分卷的 AWS 账户进行，同时亦允许该 AWS 账户所创建的各 AWS IAM 用户加以使用。除此之外，任何其它 AWS 账户及用户皆无权限查看或者访问该分卷。

存储在 Amazon EBS 分卷当中的数据以冗余方式存在于多个物理位置，这一设计亦作为常规服务运营的既有组成部分，不产生任何额外费用。然而，Amazon EBS 副本必须存储在同一可用区之内，而无法跨多个可用区; 因此，我们强烈建议大家定期将快照存储至 Amazon S3 当中以保障数据的长期持久性。对于那些利用 EBS 构建复杂事务数据库的客户，我们建议您将数据库备份至 Amazon S3 并通过数据库管理系统加以执行，从而确保分布式事务与日志得到定期检查。AWS 不会将所持有的数据备份复制到任何运行在 Amazon EC2 实例上的虚拟磁盘当中。

大家可以向其它 AWS 账户公开自己的 Amazon EBS 分卷快照，从而作为创建其它分卷的基础素材。与其它 AWS 账户共享 Amazon EBS 分卷快照并不需要具备对原始快照进行修改或者删除的高权限，这部分权限仅提供给创建该分卷的初始 AWS 账户。EBS 快照相当于一份面向完整 EBS 分卷的块级别视图。需要注意的是，这部分数据无法通过分卷上的文件系统进行查看，因此文件系统中已经被删除的文件可能仍然存在于 EBS 快照当中。如果大家希望创建共享快照，则应谨慎加以处理。如果一套分卷中包含有敏感数据或者部分文件已经被删除，那么应当创建另一套新的 EBS 分卷。共享快照中包含的数据应当被直接复制到新分卷当中，并利用新分卷再次创建完整的快照。

对敏感数据进行加密无疑是一项良好的安全实践，而 AWS 允许大家利用 AES-256 算法对 EBS 分卷及其快照进行加密。这一加密操作执行于托管 EC2 实例的服务器之上，负责在数据在 EC2 实例与 EBS 存储之间往来迁移时进行加密。为了能够高效、低延迟完成这一加密流程，EBS 加密功能只适用于配置较高的 EC2 实例类型当中（例如 M3、C3、R3 以及 G2）。

当一台存储设备接近其使用寿命终点，AWS 会自动执行清退，这是为了避免客户数据由于设备故障而发生丢失。

Auto Scaling 安全性

Auto Scaling 允许大家以自动化方式根据预先定义的条件对 Amazon EC2 容量规模进行伸缩，这意味着大家实际使用的 Amazon EC2 实例会随着资源需求量的提升而无缝增加，旨在维持稳定的性能表现; 而当资源需求降低时，其会自动进行规模收缩以降低使用成本。

与其它 AWS 服务一样，Auto Scaling 同样会对所有指向其控制 API 的请求进行验证，从而保证仅授权用户可以访问并管理 Auto Scaling。各要求由请求计算出的 HMAC-SHA1 签名以及用户私钥进行认证。然而，对于大规模或者弹性规模化集群来说，利用凭证经由 Auto Scaling 启动新 EC2 实例会变得非常困难。为了简化这一流程，大家可以使用 IAM 中的角色，确保每个实例在启动时都被分配予一个角色，进而自动实现凭证交付。当大家利用 IAM 角色启动一个 EC2 实例时，AWS 会为其提供临时性安全凭证以对应与操作任务相关的权限，这部分凭证亦通过 Amazon EC2 实例元数据服务可用于您的应用程序。该元数据服务将创建新的临时性安全凭证，其会在原有凭证过期之前对其加以替换，从而确保当前实例始终拥有操作权限。另外，该临时安全凭证还会以每天数次的频率进行自动轮换，旨在进一步提升安全性。大家可以利用 AWS IAM 在 AWS 账户之下创建更多用户，同时控制这些用户所能调用的 Auto Scaling API 权限，从而细化 Auto Scaling 的控制方式。

网络服务

Amazon Web Services 提供多种网络服务，旨在帮助大家创建一套自行定义且指向 AWS 云的专有隔离网络连接，同时配合高可用性与可扩展 DNS 服务，并以低延迟配合高数据传输速度的内容交付服务向最终用户交付内容。

Amazon Elastic Load Balancing 安全性

Amazon Elastic Load Balancing （即 Amazon 弹性负载均衡）用于管理 Amazon EC2 实例集群上的流量，将流量分发至单一服务区内各可用区上的实例。弹性负载均衡服务拥有内部负载均衡器的全部优势，外加以下安全性增强要素：

- 帮助 Amazon EC2 实例承担加密与解密任务，以集中化方式在负载均衡器上对此加以管理。
- 为客户提供单一联系点，亦可作为应对网络攻击活动的第一道屏障。
- 在 Amazon VPC 当中使用时，支持利用弹性负载均衡服务创建并管理安全分组，从而提供额外的网络与安全选项。
- 支持利用 TLS（此前为 SSL）在使用安全 HTTP（HTTPS）连接的网络之上对端到端流量进行加密。在使用 TLS 时，用于终止客户连接的 TLS 服务器证书可在负载均衡器当中进行集中管理，而不再需要立足各独立实例加以调整。

HTTPS/TLS 使用一条长期密钥以生成短期会话密钥，后者可在服务器与浏览器之间用于创建加密信息。Amazon 弹性负载均衡服务会利用 TLS 协商中使用的预定义加密集配置负载均衡器，从而确保客户端与负载均衡器间建立连接时，其始终受到加密保护。这套预定义加密集能够兼容多种客户端，且采用强大的加密算法。然而，部分客户可能需要仅由客户端指定加密与协议（例如 PCI、SOX 等等），从而确保满足特定标准。在这种情况下，Amazon 弹性负载均衡服务亦提供其它选项，其中包含

多种 TLS 协议与加密配置方案。大家可以根据自身实际需求选择启用或者禁用对应加密。

为了确保在建立安全连接时使用更新且更为强大的加密套件，大家可以配置该负载均衡器，要求其在客户端-服务器协商阶段进行加密套件选择。当选择“服务器选择优先”时，负载均衡器会根据服务器的加密套件倾向进行加密套件选择——而非客户端倾向。通过这种方式，大家将能够进一步控制客户接入负载均衡器时的安全性水平。

为了进一步提升通信隐私，Amazon 弹性负载均衡服务还允许大家使用完全转发保密，其使用的临时性会话密钥不会被实际保存在任何位置。这种作法能够避免被捕获数据受到解密，即使长期密钥本身已经遭到泄露。

Amazon 弹性负载均衡服务允许大家识别出接入服务器的客户端的原始 IP 地址——无论其实际使用 HTTPS 抑或是 TCP 负载均衡机制。一般来讲，客户端接入信息，例如 IP 地址与端口，会在请求通过负载均衡器进行代理时丢失。这是因为负载均衡器会将请求发送至客户端指定的服务器，这意味着负载均衡器就成了客户端请求来源。如果大家需要了解应用程序访客的更多信息，从而借此进行连接统计、流量日志分析或者 IP 地址白名单管理，那么掌握原始客户端 IP 地址无疑非常重要。

Amazon 弹性负载均衡服务会访问包含有负载均衡器所处理的各项 HTTP 与 TCP 请求信息的对应日志。其中包含请求客户端的 IP 地址与端口、处理该请求的实例的后端 IP 地址、请求与响应大小以及来自客户端的实际请求行（例如 GET http://www.example.com: 80/HTTP/1.1）。所有发送至该负载均衡器的请求皆会被记录下来，其中包含那些从未抵达后端实例的各项请求。

Amazon Virtual Private Cloud (简称 Amazon VPC)

安全性

一般来讲，大家启动的每个 Amazon EC2 实例都会在 Amazon EC2 地址空间内被随机分配予一个公共 IP 地址。Amazon VPC 允许大家创建一个 AWS 云隔离分区，并根据您所选定的地址范围（例如 10.0.0.0/16）启动具备私有（RFC 1918）地址的 Amazon EC2 实例。大家可以在 VPC 之内定义子网、根据 IP 地址区间对类型相似的实例进行分组，而后设置路由与安全机制以控制相关实例及子网的传入及传出流量。

AWS 提供多种 VPC 架构模板，其中包含负责提供各种公共访问级别的配置选项：

· **VPC 配合单一公共子网。**大家的实例运行在 AWS 云中的一套私有隔离分区当中，且能够直接访问互联网。网络 ACL 与安全组机制可用于对指向相关实例的入站及出站网络流量进行严格控制。

· **VPC 配合公共与专有子网。**除了包含一套公共子网之外，这套配置还添加了一套专有子网，其中各实例无法经由互联网接入。专有子网中的各个实例可利用网络地址转换（简称 NAT）功能经由公共子网建立指向互联网的出站连接。

· **VPC 配合公共与专有子网，外加硬件 VPN 访问。**这套配置在您的 Amazon VPC 与数据中心之间添加了一套 IP 安全 VPN 连接，能够在将数据中心有效扩展至云端的同时，继续为 Amazon VPC 内的公共子网实例提供指向互联网的直接连接通道。在这套配置当中，客户可在自己的企业数据中心端添加一台 VPN 设备。

· **VPC 配合纯专有子网外加硬件 VPN 访问。**大家的实例运行在包含一套专有子网的 AWS 云内专有隔离分区当中，且其无法直接经由互联网加以访问。大家可以经由一条 IP 安全 VPN 通道将此专有子网与企业数据中心相对接。

大家还可以利用专有 IP 地址对两套 VPC 加以对接，这种作法使得两套 VPC 中的各个实例能够在处于同一网络环境中时彼此通信。大家可以在您自己的 VPC 之间或者与同一服务区内另一 AWS 账户下的 VPC 之间创建对等连接。

Amazon VPC 中的安全功能包括安全分组、网络 ACL、路由表以及外部网关。每项功能都以补充性方式提供一套安全且具备隔离性的网络环境，且能够扩展至互联网直连或者经由专有连接指向其它网络。运行在 Amazon VPC 当中的 Amazon EC2 实例能够享受到多种安全收益，包括访客操作系统保护以及数据包嗅探预防。

不过需要注意的是，大家必须为自己的 Amazon VPC 创建特定 VPN 安全组; 大家所创建的任何 Amazon EC2 安全组都无法在 Amazon VPC 之内起效。另外，Amazon VPC 安全组还拥有一些 Amazon EC2 安全组所不具备的额外功能，其中包括在实例启动后变更安全组以及同时使用多种标准协议（而非单纯使用 TCP、UDP 或者 ICMP）的能力。

每个 Amazon VPC 在云环境中皆属于一套独特且孤立的网络; 各 Amazon VPC 之间的网络流量彼此隔离，相互间完全不存在干扰。在创建时，大家需要为每个 Amazon VPC 选定 IP 地址区间。大家可以创建并接入一套互联网网关、虚拟专有网关或者二者皆用，从而建立起一套能够完成以下控制任务的外部连接。

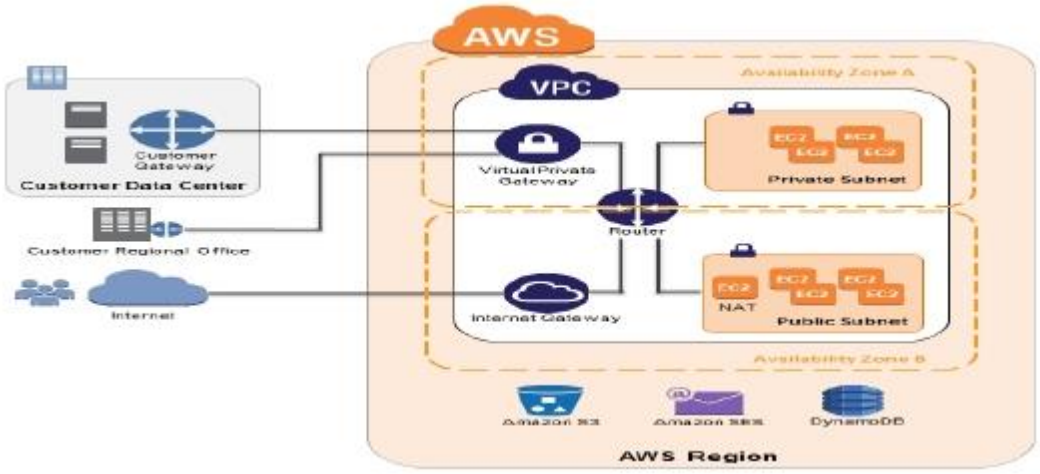
API 访问: 用于创建及删除 Amazon VPC、变更路由、安全组与网络 ACL 参数，以及执行其它功能的调用全部需要利用 Amazon 保密访问密钥进行签名——这一密钥可由 AWS 账户的保密访问密钥或者用户在 AWS IAM 中创建的保密访问密钥充当。如果不具备保密访问密钥，Amazon VPC API 调用将无法正确执行您的命令。另外，API 调用亦可利用 SSL 进行加密，从而保障其机密性。Amazon 建议大家始终使用受 SSL 保护的 API 端点。AWS IAM 还允许客户进一步控制新近创建的用户有权执行哪些 API 调用操作。

子网与路由表: 大家可以在每套 Amazon VPC 之内创建一套或者多套子网; 该 Amazon VPC 之内启动的每个实例都会接入其中一套子网。包括 MAC 嗅探与 ARP 嗅探在内的各类传统二级安全攻击都会被屏蔽。

Amazon VPC 中的每套子网都与一份路由表相关联，且离开该子网的全部网络流量都由该路由表负责处理，旨在确定其目的地。

防火墙（安全组）: 与 Amazon EC2 类似，Amazon VPC 同样支持完整的防火墙解决方案，可用于对任一实例的入站与出站流量进行过滤。默认分组允许来自同一组的各内部成员间通信，同时放行前往任意目的地的出站通信。大家可以利用 IP 协议、服务端口以及源/目的地 IP 地址（独立 IP 或者无类别域间路由（简称 CIDR）块）对流量进行限制。

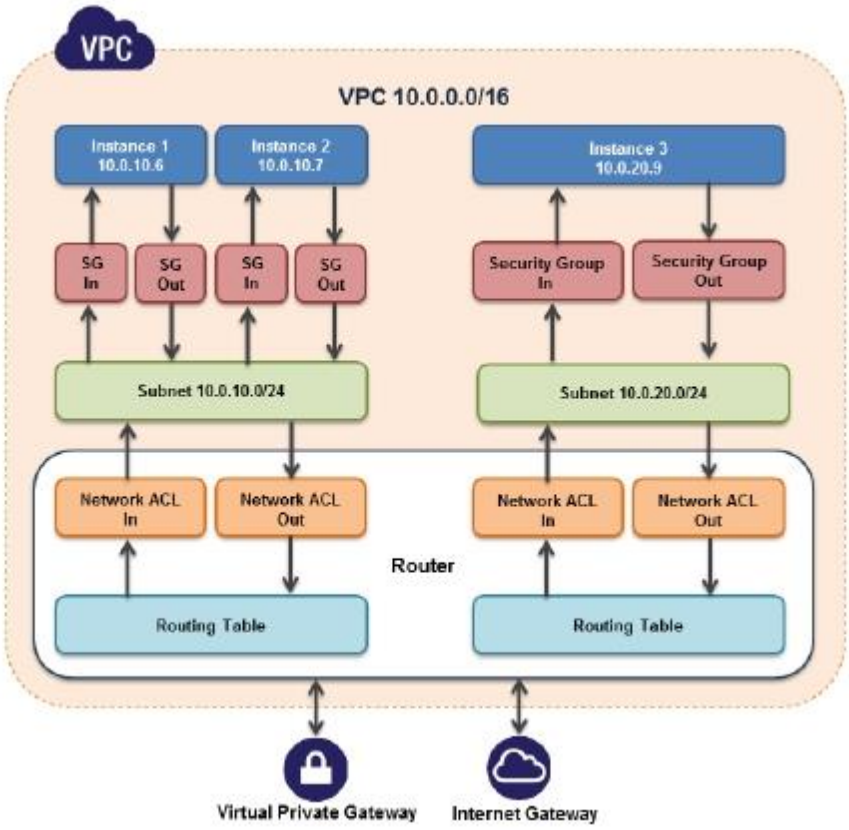
这套防火墙不会受到访客操作系统的控制; 相反，其只能经由 Amaozn VPC API 进行修改。AWS 允许大家以细粒度方式对实例上的不同管理功能与防火墙加以访问，这意味着用户能够通过职责划分实现额外的安全性保障。防火墙所能提供的安全性水平取决于您开放的端口及其持续时长与用途。另外，我们还需要在每个实例当中使用经过良好定义的流量管理与安全设计。AWS 亦鼓励大家在基于主机的防火墙（例如 IP 表或者 Windows 防火墙）当中应用其它每实例过滤机制。



图五：Amazon VPC 网络架构

网络访问控制列表: 为了在 Amazon VPC 之内添加更多安全层，大家可以配置网络 ACL。这些控制列表属于无状态流量过滤器，适用于 Amazon VPC 内目标子网的全部入站或者出站流量。这些 ACL 能够包含各类预设规则，从而根据 IP 地址、服务端口以及来源/目标 IP 地址放行或者拒绝对应流量。

与安全组类似，网络 ACL 同样通过 Amazon VPC API 实现管理，同时通过职责划分添加额外的保护层及安全机制。以下示意图展示了互连体系之上的安全控制机制如何在保证灵活网络拓扑结构的同时，提供面向网络流量流程的完整控制。



图六：灵活的网络拓扑结构

虚拟专有网关：利用一套虚拟专有网关建立 Amazon VPC 与其它网站间的专有连接。各虚拟专有网关内的网络流量会与其它虚拟专有网关中的网络流量彼此隔离。大家可以建立 VPN 连接以将该虚拟专有网关接入佻内部环境下的网关设备。每条连接都受到注入有客户网关设备 IP 地址的预共享密钥的严格保护。

互联网网关：大家可以将互联网网关接入至 Amazon VPC，从而实现其与 Amazon S3、其它 AWS 服务以及互联网之间的直连通道。每个需要实现这种访问能力的实例都必须被分配以弹性 IP 或者通过 NAT 实例进行流量路由。另外，网络路由亦可通过配置（详见上图）以将流量直接导入该互联网网关。AWS 提供多川参考 NAT AMI，大家可以借此执行网络日志记录、深度数据包检测、应用层过滤或者其它安全控制操作。

这一访问仅可通过调用 Amazon VPC API 进行修改。AWS 支持细粒度访问控制功能，即将不同管理功能与特定实例及互联网网关相匹配，从而帮助大家通过职责划分实现额外的安全性提升。

专用实例：在一套 VPC 当中，大家可以启动多个 Amazon EC2 实例并确保其与主机硬件层之间进行物理隔离（即其运行在单租户硬件之上）。一套 Amazon VPC 可以“专用”租户身份进行创建，这意味着在该 Amazon VPC 之内启动的全部实例都将符合这一特性。另外，大家也可以“默认”租户完成 Amazon VPC 创建，但同时为将其中启动的实例指定为“专用”租户。

弹性网络接口：每个 Amazon EC2 实例都拥有一套默认的网络接口，其会被分配以 Amazon VPC 网络上的一个专有 IP 地址。大家可以为 Amazon VPC 内的任意 Amazon EC2 实例创建并附加一个额外的网络接口，即弹性网络接口（简称 ENI），从而确保单一实例拥有总计两个网络接口。将超过一个网络接口附加至实例能够帮助大家在 Amazon VPC 之内创建管理网络、使用网络与安全设备，或者利用不同子网上的工作负载/角色创建双归属实例。一条 ENI 属性，其中包含专有 IP 地址、弹性 IP 地址以及 MAC 地址，将随同 ENI 一同附加至单一实例，亦可脱离该实例并重新附加至另一实例。欲了解更多 Amazon VPC 相关信息，请参阅 AWS 网站上的对应页面：

http://aws.amazon.com/vpc/

利用 EC2-VPC 实现其它网络访问控制

如果大家在从未使用过的新服务区内启动实例，AWS 会启动新的 EC2-VPC 功能（亦被称为默认 VPC 功能），意味着全部实例都会被自动配置为可随时使用的默认 VPC。大家可以选择创建更多 VPC，或者根据其它已经包含已有实例的可用区实例进行 VPC 创建。

如果大家利用常规 VPC 进行 VPC 创建，则需要为其指定 CIDR 块、创建子网、为这些子网输入路由与安全性规则，且在需要子网接入互联网时为其配置互联网网关或者 NAT 实例。在 EC2-VPC 之内启动 EC2 实例时，大部分上述任务都将自动完成。在利用 EC2-VPC 在默认 VPC 内启动实例时，我们会为您承担以下设置任务：

- 在每个可用区内创建一套默认子网。
- 创建一套互联网网关并将其接入您的默认 VPC。
- 利用规则为您的默认 VPC 创建一套主路由表，负责将全部指向互联网的流量引导至互联网网关。
- 创建一套默认安全组并将其与您的默认 VPC 相关联。
- 创建一套默认网络访问控制列表（简称 ACL）并将其与您的默认 VPC 相关联。
- 将您 AWS 账户的默认 DHCP 选项集与您的默认 VPC 相关联。

除了确保默认 VPC 拥有自己的专有 IP 区间之外，在默认 VPC 之内启动的各 EC2 实例还将获得一个公共 IP。

以下表格汇总了 EC2-Classic（即默认 VPC 中启动的实例）与非默认 VPC 内启动实例间的区别。

特性	EC2-Classic	EC2-VPC(默认 VPC)	常规 VPC
公共 IP 地址	您的实例会获得一个公共 IP 地址。	启动于默认子网中的实例会默认收到一个公共 IP 地址，除非您在启动过程中进行特殊指定。	您的实例不会默认获得公共 IP 地址，除非您在启动过程中进行特殊指定。
专有 IP 地址	您的实例会在每时启动时从 EC2-Classic 区间内获得一个专有 IP 地址。	您的实例会从默认 VPC 的地址区间内获得一个静态专有 IP 地址。	您的实例会从 VPC 的地址区间内获得一个动态专有 IP 地址。
多专有 IP 地址	我们会为您的实例选择一个单一 IP 地址。不支持多 IP 地址。	大家可以为您的实例分配多个专有 IP 地址。	大家可以为您的实例分配多个专有 IP 地址。
弹性 IP 地址	在终止实例时，其对应 EIP 将取消关联。	当终止实例时，其对应 EIP 将继续关联。	当终止实例时，其对应 EIP 将继续关联。
DNS 主机名称	DNS 主机名称默认启用。	DNS 主机名称默认启用。	DNS 主机名称默认禁用。
安全组	安全组可引用归属于其它 AWS 账户的现有安全组。	安全组仅可引用您 VPC 内部的现有安全组。	安全组仅可引用您 VPC 内部的现有安全组。
安全组分配	您必须终止当前实例以变更其安全组。	您可在实例运行的同时变更其安全组。	您可在实例运行的同时变更其安全组。
安全组规则	您只能为入站流量添加规则。	您可以为入站及出站流量添加规则。	您可以为入站及出站流量添加规则。
租户	您可以在共享硬件或者单租户硬件之上运行实例。	您的实例运行在共享硬件之上;	您可以在共享硬件或者单租户硬件之上运行实例。

需要注意的是，EC2-Clasic 中的实例安全组与 EC2-VPC 中的实例安全组略有不同。举例来说，大家只能为 EC2-Classic 添加入站流量规则，但却可以为 EC2-VPC 的入站与出站流量同时添加规则。在 EC2-Classic 当中，大家无法在实例启动之后变更其安全组; 但在 EC2-VPC 当中，大家可以在实例启动完成后随时变更其安全组分配。另外，大家无法利用 VPC 内各实例的安全组创建 EC2-Classic 安全组设置。大家必须在 VPC 内为各实例具体指定安全组。大家在 VPC 安全组内创建的规则无法直接引用至 EC2-Classic 内的安全组，反之亦然。

Amazon Route 53 安全性

Amazon Route 53 是一项具备高可用性与扩展性的域名系统（简称 DNS）服务，可用于应答 DNS 查询、将域名转换为 IP 地址以确保各计算机间能够彼此通信。Route 53 可用于将用户请求与运行在 AWS 内或者之外的基础设施对接——例如 Amazon EC2 实例或者 Amazon S3 存储桶。

Amazon Route 53 允许大家对自己域名进行 IP 地址（记录）列表管理，同时应答请求（查询）以将特定域名转换为对应 IP 地址。指向域名的查询始终会被自动路由至最近 DNS 服务器，从而确保提供最低的使用延迟。

Route 53 允许大家通过一整套路由类型完成流量的全局管理，其中包括基于延迟路由（简称 LBR）、地理 DNS 以及加权循环（简称 WRR），这些机制皆可与 DNS 故障转移相结合以建立低延迟、高容错架构。其中 Amazon Route 53 提供的故障转移算法不仅会确保流量被路由至运行正常的端点处，同时亦有助于避免由错误配置的状态检查与应用、端点过载乃至分区故障所引发的灾难场景。

Route 53 还提供域名注册服务——大家可以在这里购买并管理域名，而 Route 53 则会自动为您的域名配置默认 DNS 设置。大家可以随意选择各国顶级域名（简称 TLD）并根据需要进行购买、管理与转换。在注册过程中，大家可以选择为域名启用隐私保护机制。此选项在启用之后，会将大部分个人信息隐藏以来以避免恶意活动及垃圾邮件的侵扰。

Amazon Route 53 立足于 AWS 的高可用性与可靠性基础设施。AWS DNS 服务器的天然分布式特性能够确保大家始终有能力将最终用户路由至应用程序。Route 53 还提供运行状态检查与 DNS 故障转移功能，有助于确保网站可用性。大家能够轻松配置 Route 53 以定期检查网站运行状态（即使是仅可经由 SSL 访问的安全网站），同时在主站无法响应时将流量引导至备份站点。

与其它 AWS 服务一样，Amazon Route 53 会对指向其控制 API 的请求进行验证，意味着仅有授权用户能够访问并管理 Route 53。各 API 请求会通过请求及用户 AWS 保密访问密钥计算出的 HMAC-SHA1 或者 HMAC-SHA256 签名进行认证。另外，Amazon Route 53 控制 API 还仅可通过 SSL 加密端点进行控制。其仅支持 IPv4 与 IPv6 路由功能。

大家可以在自己的 AWS 账户当中利用 AWS IAM 创建用户以访问 Amazon Route 53 DNS 管理功能，同时控制这些用户所能执行的 Route 53 操作权限。

Amazon CloudFront 安全性

Amazon CloudFront 允许客户轻松便捷地将内容分发至最终用户，且保证低延迟与高数据传输速度效果。其提供动态、静态与流式内容交付方式，且利用一套全球边缘位置网络。与客户目标相关的请求会被自动路由至距离最近的边缘位置，从而保证内容以最佳性能进行交付。Amazon CloudFront 还针对与其它 AWS 服务的协作需求进行了优化，具体包括 Amazon S3、Amazon EC2、弹性负载均衡以及 Amazon Route 53。其亦能够与任意存储有原始文件版本的非 AWS 服务器无缝对接。

Amazon CloudFront 要求指向其控制 API 的各项请求接受验证，因此只有授权用户能够对自己的 Amazon CloudFront 发布机制进行创建、修改或者删除。各请求利用请求及用户私钥计算出的 HMAC-SHA1 签名进行认证。另外，Amazon CLoudFront 控制 API 还仅接受经由 SSL 交付的端点访问。

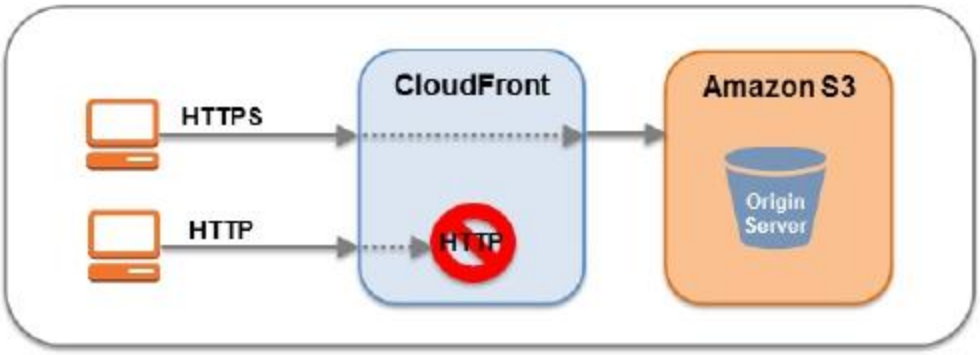
Amazon CloudFront 边缘位置中保留的数据不提供持久性承诺。该项服务会在相关对象访问频率较低时将其从边缘位置移除。持久性保障由 Amazon S3 负责实现，其可作为 Amazon CloudFront 的源服务器存储由后者交付的原始对象、最终对象或者对象副本。如果大家希望控制能够从 Amazon CloudFront 处下载内容的用户类型，则可启用该服务的专有内容功能。这项功能包含两大组成部分：其一负责控制内容如何从 Amazon CloudFront 边缘位置被交付至互联网上的用户处。其二则控制 Amazon CLoudFront 如何访问存储在 Amazon S3 中的对象。CloudFront 还支持地理限制功能，其能够根据访问者的地理位置限制其对内容的查看。

为了控制对 Amazon S3 内原始对象副本的访问，Amazon CloudFront 允许大家创建一项或者多项“原始访问身份”，并将其与您的分发机制进行关联。当一项原始访问身份与某种 Amazon CloudFront 分发机制相关联后，该分发机制将利用此身份从 Amazon S3 中获取对象。大家随后可利用 Amazon S3 的 ACL 功能限制指向该原始访问身份的访问操作，从而确保其原始对象副本无法进行公开查看。

为了控制可从 Amazon CLoudFront 边缘位置下载对象的用户身份，该服务使用了一套 URL 签名验证系统。要使用这套系统，大家首先需要创建公钥-私钥对，并将公钥通过 AWS 管理控制台上传至您的账户。接下来，大家配置自己的 Amazon CloudFront 分发机制以指定授权访问的具体账户——大家可以最多将 5 个 AWS 账户添加为受信对象。第三，大家被要求创建用于指定 Amazon CloudFront 内容交付的策略说明文档。这些策略文档可指定所要请求的对象名称、请求的日期与时间、发出请求之客户端的原 IP（或者 CIDR 区间）等等。在此之后，大家计算策略文档的 SHA1 哈希值并利用私钥对其进行签署。最后，大家在引用对象时将编码策略文档与签名作为查询客串参数。当 Amazon CloudFront 接收到一条请求时，其会利用大家的公钥进行签名解码，而 Amazon CloudFront 只会响应通过策略文档验证与签名匹配的输入请求。

需要注意的是，专有内容属于大家在设置 CloudFront 分发机制时必须启用的一项可选功能。如果不借此加以限制，您交付的内容将面向互联网公开。

Amazon CloudFront 提供该选项以通过加密连接（HTTPS）进行内容传输。在默认情况下，CloudFront 会接收来自 HTTP 以及 HTTPS 协议的全部请求。然而，大家也可以配置 CloudFront 以要求其仅接收 HTTPS 请求或者将指向 CloudFront 的 HTTP 请求重新定向至 HTTPS。大家甚至能够配置 CloudFront 分发机制以允许 HTTP 访问部分对象，同时要求经由 HTTPS 访问其它对象。



图七：Amazon CoudFront 加密传输流程

大家可以一个或者多个 CloudFront 来源，以供 CloudFront 借此获取对象并使用访问者在访问对象请求中使用的同一协议。举例来说，当大家使用此 CloudFront 设置时，使用 HTTPS 的访问者向 CloudFront 请求某一对象，CloudFront 也会利用 HTTPS 将该请求转发至数据来源。

Amazon CloudFront 在 CloudFront 与自定义原始 Web 服务器之间的 HTTPS 中支持 TLSv1.1 与 TLSv1.2 协议（亦支持 SSLv3 与 TLSv1.0），同时允许大家选择自己需要的加密套件，具体包括椭圆曲线 DIffie-Hellman 临时（简称 ECDHE）协议。ECDHE 允许 SSL/TLS 客户实现完全转发保密，即使用临时性且不会存储于任何位置的会话密钥。这有助于避免未授权第三方对捕获的数据进行解码——即使长期密钥本身已经遭到泄露。

需要注意的是，如果大家所设定的数据来源并非自有服务器，则应当在访问者与 CloudFront 以及 CloudFront 与来源之间使用 HTTPS 连接。在这种情况下，大家必须在 HTTP 服务器上安装一套有效 SSL 证书，并确保其由第三方证书颁发机构提供签名——例如 VeriSign 或者 DigiCert。

在默认情况下，大家可以利用 URL 中的 CloudFront 分发域名经由 HTTPS 向访问者交付内容; 举例来说，https://dxxxxx.cloudfront.net/image.jpg。如果大家希望利用自有域名及 SSL 证书经由 HTTPS 进行内容交付，则可使用 SNI 自定义 SSL 或者专用 IP 自定义 SSL。利用服务器名称标记（简称 SNI）自定义 SSL，CloudFront 可使用 TLS 协议的 SNI 扩展，目前大多数现代网络浏览器且对其提供支持。然而，部分用户可能由于使用不支持 SNI 的陈旧浏览器而无法访问您的内容。而使用专用 IP 自定义 SSL，CloudFront 能够为各 CloudFront 边缘位置的 SSL 证书分配 IP 地址，从而确保 CloudFront 能够将输入请求与对应的 SSL 证书关联起来。

Amazon CloudFront 访问日志中包含一整套与内容请求相关的信息集，具体包括所请求对象、请求的日期与时间、用于响应请求的边缘位置、客户端 IP 地址、引用以及用户代理。要启用访问日志，大家只需要在配置 Amazon CloudFront 发布机制时为其指定存储日志所用的 Amazon S3 存储桶名称即可。

AWS Direct Connect 安全性

利用 AWS Direct Connect，大家可以在内部网络与 AWS 服务区之间建立一条高能量专用连接。通过这种方式，客户能够降低网络使用成本、改善数据吞吐能力或者提供更为稳定的网络使用体验。利用这条专用连接，大家可以创建直接指向 AWS 云的虚拟接口（例如指向 Amazon EC2 以及 Amazon S3）。

在 AWS Direct Connect 的帮助下，大家可以绕开网络路径中的互联网服务供应商。大家能够在 AWS Direct Connect 位置内建立机架空间，并部署周边设备。部署完成之后，大家可以通过跨越连接将该设备接入 AWS Direct Connect。每个 AWS Direct Connect 位置都能够与距离其最近的 AWS 服务区相连。大家可以访问此服务区内可用的全部 AWS 服务。美国本土的 AWS Direct Connect 位置亦可经由公共虚拟接口访问其它 AWS 服务区中的公共端点。

利用行业标准 802.1q VLAN，该专有连接可被拆分成多个虚拟接口。如此一来，大家就能够利用同一连接访问多种公共资源，具体包括利用公共 IP 地址空间存储在 Amazon S3 中的对象，外加利用专有 IP 空间运行在 Amazon VPC 内部的 Amazon EC2 实例等专有资源，同时继续保持公共与专有环境之间的网络隔离性。

AWS Direct Connect 要求使用边界网关协议（简称 BGP）配合自主系统编号（简称 ASN）要建立一个虚拟接口，大家可以利用 MD5 加密密钥进行信息授权。MD5 会利用您的保密密钥创建一条密钥散列。AWS 能够自动生成一条 BGP MD5 密钥，大家也能够自行提供此密钥。

存储服务

Amazon Web Services 提供多种具备高持久性与可用性的低成本数据存储服务。AWS 提供的各存储选项可用于备份、归档、灾难恢复以及块与对象存储。

Amazon Simple Storage Service (Amazon S3)

安全性

Amazon Simple Storage Service 即 Amazon 简单存储服务，简称 S3）允许大家随时在任意网络位置进行数据上传与检索。Amazon S3 将数据以对象形式存储在存储桶当中。每个对象可代表任意类别的文件，具体包括文本文件、图片以及视频等等。当大家向 Amazon S3 当中添加文件时，可以选择同时包含该文件的元数据并设置相关访问权限。对于各个存储桶，大家可以控制指向存储桶的访问（哪些用户能够在存储桶中创建、删除及查看各对象）、查看存储桶访问日志及其对象，并选择 Amazon S3 存储桶及其内容的所在地理位置。

数据访问

对 Amazon S3 内数据进行的访问操作默认受到限制; 只有存储桶与对象的拥有者能够查看其创建的 Amazon S3 资源（请注意，这里的存储桶/对象拥有者即 AWS 账户拥有者，而非实际创建该存储桶/对象的用户）。大家可以利用多种方式控制对存储桶及对象的访问操作：

· **身份与访问管理（简称 IAM）策略。** AWS IAM 允许企业中的多名员工在单一 AWS 账户之内创建并管理多个用户。IAM 策略会被附加至这些用户处，从而在 AWS 账户之内启用集中化权限控制，用于规划存储桶或者对象访问行为。在 IAM 策略的帮助下，大家只需要为 AWS 账户内各用户设定权限即可对 Amazon S3 资源访问活动加以管理。

· **访问控制列表（简称 ACL）。**在 Amazon S3 当中，大家可以使用 ACL 为用户组提供对存储桶或者对象的读取或写入权限。利用 ACL，大家只需要为其他 AWS 账户（而非特定用户）提供访问自有 Amazon S3 资源的权限。

· **存储桶策略。**Amazon S3 中的存储桶策略可用于添加或者拒绝单一存储桶之内的部分或者全部对象操作权限。这些策略可被附加至用户、分组或者 Amazon S3 存储桶，从而实现权限的集中化管理。利用存储桶策略，大家能够对自有 AWS 账户之内或者其他 AWS 账户中的用户提供对 Amazon S3 资源访问的权限。

访问控制类型	是否提供 AWS 账户层级控制？	是否提供用户层级控制？
IAM 策略	否	是
ACL	是	否
存储桶策略	是	是

大家可以基于特定条件对部分资源进行严格控制。举例来说，大家可以要求请求时间（日期条件）、请求是否使用 SL 发送（Boolean 条件）、请求方 IP 地址（IP 地址条件）或者根据 请求方客户端应用（字符串条件）限制访问行为。要识别这些条件，大家需要使用公钥。欲了解更多 Amazon S3 中提供的特定行为公钥功能，请参阅 Amazon 简单存储服务开发者指南。

Amazon S3 还为开发者提供多种选项，用于查询字符串身份，其允许通过特定时段内有效的 URL 共享 Amazon S3 对象。查询字符串身份适用于为 HTTP 或者浏览器提供资源访问权限等用例。此查询字符串需要使用签名以保障请求安全。

数据传输

为了最大程度实现安全性保障，大家可以通过 SSL 加密端点随意面向 Amazon S3 进行数据上传/下载。该加密端点可接受来自互联网以及 Amazon EC2 内部的访问，意味着数据可以安全方式在 AWS 之内以及 AWS 之外进行传输。

数据存储

Amazon S3 提供多种选项，旨在对闲置数据进行保护。对于倾向于自行管理加密机制的客户，大家可以使用 Amazon S3 加密客户端到客户端加密库，在数据被上传至 Amazon S3 之前对其进行加密。另外，大家也可以使用 Amazon S3 服务器端加密（简称 SSE），从而将加密任务交由 AWS 负责处理。数据由 AWS 生成或者客户自行提供的密钥进行加密，具体取决于您的实际需求。利用 Amazon S3 SSE，大家可以轻松通过在写入对象时添加额外请求头的方式在数据上传时进行加密。加密会在数据进行检索时自动完成。

需要注意的是，大家包含在对象中的元数据不会进行加密。因此，AWS 建议客户不要将敏感信息添加到 Amazon S3 元数据当中。

Amazon S3 SSE 使用目前最为强大的块加密方案之一——即 256 位先进加密标准（简称 AES-256）。利用 Amazon S3 SSE，每个受保护对象都会利用惟一的加密密钥进行加密。此对象密钥本身随后亦会利用定期轮换的主密钥进行加密。Amazon S3 SSE 会将加密数据与加密密钥存储在不同主机之上，从而进一步提升安全性水平。Amazon S3 SSE 还允许大家强制执行加密要求。举例来说，大家可以创建并应用相关存储桶策略，要求只将加密后的数据上传至存储桶当中。

对于长期存储内容，大家可以自动将自己的 Amazon S3 存储桶内容归档至 AWS 的归档服务——即 Amazon Glacier。另外，大家可以在 Amazon S3 当中创建生命周期规则，通过设定哪些内容何时被归档至 Glacier 实现整个流程的自动化执行。作为数据管理策略的重要组成部分，大家也可以指定 Amazon S3 以怎样的时间周期对其中保存的对象进行清理。

当某一对象被从 Amazon S3 中删除时，来自公共名称指向该对象的映射亦会被立即移除，且整个过程在分布式系统内只需要数秒即可完成。一旦映射被移除，指向该被删除对象的全部远程访问将立即失效，对应的底层存储区域则重新可由系统进行分配。

数据持久性与可靠性

Amazon S3 在设计当中考虑到在一年周期内实现存储对象的 99.999999999%持久性与 99.99%可用性。各对象以冗余方式存储在同一 Amazon S3 服务区内跨越多套设施的多台设备当中。为了实现这一持久性水平，Amazon S3 会首先跨越多套设施对客户数据进行同步 PUT 与 COPY 操作，直到其返回 SUCCESS 结果。在存储完成后，Amazon S3 能够快速检测并修复任何丢失的数据内容，从而持续维护对象持久性。Amazon S3 还会定期利用和校验机制对所存储数据的完整性进行验证。如果发现数据内容损坏，则利用冗余数据进行修复。另外，Amazon S3 还会对全部网络流量进行和检验计算，从而在数据存储或者检索时检测数据包是否存在损坏。

Amazon S3 还通过版本控制功能实现进一步保护。大家可以利用版本控制机制对存储在 Amazon S3 存储桶内的各个对象进行保留、检索与恢复。利用版本控制机制，大家可以轻松解决由意外用户操作及应用故障造成的数据破坏。在默认情况下，各请求将直接检索最近写入的数据版本。对象的早期版本可通过指定特定版本号的请求操作进行检索。大家能够利用 Amazon S3 版本控制的 MFA 删除功能对各对象版本加以进一步保护。一旦在 Amazon S3 存储桶内启用版本控制功能，各项版本删除请求即必须包含由多因素验证设备提供的六位数字编码及序列号。

访问日志

大家可以对 Amazon S3 存储桶加以配置，允许对存储桶及其内部对象进行日志访问。该访问日志中包含与各项访问请求相关的细节信息，具体包括请求类型、所请求资源、请求方 IP 以及请求发生的时间与日期。当在存储桶中启用日志记录功能时，各日志记录会定期被整理为日志文件，同时被交付至特定 Amazon S3 存储桶以备日后查询。

跨域资源共享(简称 CORS)

利用 Amazon S3 托管静态网络页面或者存储其它网页所使用的对象的 AWS 客户，可以通过将 Amazon S3 存储桶配置为接受跨域请求实现安全的内容加载效果。现代浏览器使用同源策略以防止 JavaScript 或者 HTML 5 允许来自其它站点或者域的加载内容，旨在借此确保不会从低信誉来源处加载恶意内容（例如跨站点脚本攻击）。而在启用了跨域资源共享（简称 CORS）策略之后，存储在 Amazon S3 存储桶中的各类资产——例如字体与图片——能够安全地为外部网页、样式布局以及 HTML 5 应用所引用。

Amazon Glacier 安全性

与 Amazon S3 一样，Amazon Glacier 服务同样提供低成本、安全且持久性良好的存储资源。不过与专门针对快速检索的 Amazon S3 不同，Amazon Glacier 主要作为访问频率较低数据的归档方案——其检索过期往往需要数个小时。

Amazon Glacier 会在存储库内将文件作为归档进行存储。各归档可属于任何数据类型，例如图片、视频或者文件，且每一归档可包含一个或者多个文件。大家可以在单一存储库内保留任意数量的归档，且每服务区最多可容纳 1000 套存储库。每个归档最多可容纳 40 TB 数据。

数据上传

要将数据传输至 Amazon Glacier 存储库，大家可以一次性或者分拨对归档进行上传。在单一上传操作中，大家可以上传最大达 4 GB 的归档数据。然而，客户也可以使用 Multipart Upload API，从而在上传超过 100 MB 的归档时获得更理想的使用体验。在 Multipart Upload API 的帮助下，大家能够最多上传高达 40 TB 的归档数据。Multipart Upload API 调用在设计上充分考虑到大型归档的上传体验，其会对各数据部分进行并发独立上传。如果其中某项上传操作失败，大家只需要重新上传对应的失败部分即可，而不会影响到完整的归档数据。

当大家向 Amazon Glacier 上传数据时，必须计算并提供一条树状哈希值。Amazon Glacier 会针对数据进行哈希值检查，从而确保数据上传路径未受到篡改。数据中每 1 MB 大小的区块皆可计算一条对应的哈希值，而后将各值组合起来形成树状结构，用于反映数据增长过程中各区块的相邻关系。

作为 Multipart Upload 功能的替代方案，大家在将超大规模数据上传至 Amazon Glacier 时也可以考虑使用 AWS Import/Export 服务，用以代替网络传输。AWS Import/Export 利用便携式存储设备将大规模数据传输至 AWS 当中。AWS 会直接利用内部高速网络直接接入客户存储设备，并将存储装置以邮寄形式发回对应服务区设施，从而绕过互联网这一传输载体。

大家也可以设置 Amazon S3，从而通过特定的时间间隔将数据迁移至 Amazon Glacier。大家可以在 Amazon S3 的生命周期规则中描述哪些对象应在何时被传输至 Amazon Glacier。另外，大家还可以指定 Amazon S3 中的部分数据在驻留多久之后即应被自动删除。

为了实现更理想的安全水平，大家可以通过 SSL 加密端点与 Amazon Glacier 之间进行数据上传/下载。各加密端口可通过互联网或者 Amazon EC2 内部连接进行访问，因此数据传输过程在 AWS 之内或者之外皆拥有良好的安全保障。

数据检索

要对 Amazon Glacier 中的归档进行检索，大家首先需要启动检索任务，其大概需要 3 到 5 个小时方可完成。大家随后即可通过 HTTP GET 请求访问对应数据。这部分数据将在接下来的 24 小时内供您随时查看。

大家可以检索完整归档或者仅检索单一归档内的部分文件。如果大家仅希望对归档内的部分子集进行检索，则可使用一条检索请求以指定包含所需要文件的归档范围，或者启动多项检索请求且每条请求都对应不同的检索区间。大家也可以通过过滤归档的创建日期范围或者设定项目最大值以限定检索项目的数量。无论选择哪种实现方法，在对归档中的部分内容进行检索时，大家都可以使用和校验机制确保对应文件的完整性同整体归档的树状哈希值相匹配。

数据存储

Amazon Glacier 会自动利用 AES-256 对数据进行加密，并以恒定形式对其进行持久存储。Amazon Glacier 的设计目标旨在提供高达 99.999999999%的归档持久性。其会将每个归档存储在多套设施的多台设备当中。与需要进行大量数据验证与手工修复的传统存储系统不同，Amazon Glacier 会定期对内部数据的完整性进行检查，同时执行自动修复操作。

数据访问

只有您的账户才能访问 Amazon Glacier 中的自有数据。要对 Amazon Glacier 内的数据进行访问控制，大家可以使用 AWS IAM 以指定账户下的哪些用户有权对特定存储库进行操作。

AWS Storage Gateway 安全性

AWS Sotrage Gateway 负责将内部软件与云存储资源相对接，从而在 IT 环境与 AWS 存储基础设施之间提供无缝化及高安全性集成效果。此项服务允许大家将数据安全上传至 AWS 中具备高可扩展性、可靠性及安全性的 Amazon S3 存储服务当中，旨在实现极具成本效益的备份与快速灾难恢复功能。

AWS Storage Gateway 以透明方式将数据以 Amazon EBS 快照形式离站备份至 Amazon S3 处。Amazon S3 以冗余方式将这些快照存储在跨越多套设施的多台设备之上，同时检测并修复任何冗余数据丢失问题。Amazon EBS 快照能够提供时间点备份素材，可用于对内部环境进行恢复或者初始化新的 Amazon EBS 分卷。大家可将数据存储在您所指定的任何区域之内。

AWS Storage Gateway 提供以下三种选项：

· 网关存储分卷（其中云资源作为备份机制）。在这一选项中，大家的分卷数据会存储在本地，而后被推送至 Amazon S3，并在云端以冗余及加密的弹性块存储（简称 EBS）快照形式进行存储。当大家使用这一模式时，内部存储作为一级存储系统，负责为完整数据集提供低延迟访问支持; 而云存储则作为备份资源存在。

· 网关缓存分卷(其中云资源作为一级存储)。在这一选项中,大家的分卷数据会以加密方式被存储在 Amazon S3 当中,同时可通过一套 iSCSI 接口供企业网络进行查看。最近访问过的数据会被缓存在内部环境下以实现低延迟本地访问。当大家使用这一模式时,云存储将作为一级存储系统,但访问频率最高的数据将以缓存分卷形式驻留在内部环境中以加快访问速度。

· 网关虚拟磁带库(简称 VTL)。在这一选项中,大家可以在每套网关上配置最高 10 套虚拟磁带驱动器、1 套介质转换器以及多达 1500 个虚拟磁带卡。每套虚拟磁带驱动器都对 SCSI 命令集做出响应,因此大家的现有内部备份应用(无论是磁盘到磁带还是磁盘到磁盘再到磁带)都能够无需修改即直接与之对接。

无论大家具体选择哪种选项,数据都会以异步方式从内部存储硬件通过 SSL 传输至 AWS。Amazon S3 中存储的数据利用高级加密标准(简称 AES)256 进行加密——这是一项对称密钥加密标准,采用 256 位加密密钥。AWS Storage Gateway 只会将发生变更的数据上传至云端,旨在将经由互联网传输的数据量控制在最低水平。

AWS Storage Gateway 作为虚拟机运行,大家可以将其部署在运行有 VMware ESXi 虚拟机管理程序 v4.01 或者 v5,抑或是采用微软 Hyper-V(大家需要在设置过程中下载该 VMware 软件)的数据中心主机当中。大家也可以利用网关 AMI 将其运行在 EC2 实例之内。在安装与配置流程中,大家可以在每套网关上创建最多 12 套存储分卷、20 套缓存分卷或者 1500 个虚拟磁带卡。在安装完成后,各套网关都会自动下载、安装并部署更新及补丁。这部分操作立足于维护窗口进行,大家可以网关为基本单位进行规划设置。

iSCSI 协议 支持通过 CHAP(即质询握手身份验证协议)在目标与发起方之间进行身份验证。CHAP 能够定期对访问某存储分卷目标的 iSCSI 发起方进行身份验证,从而有效应对中间人与重放攻击。要设置 CHAP,大家必须同时在 AWS Storage Gateway 控制台以及用于接入目标的 iSCSI 发起方软件内对其进行配置。

在 AWS Storage Gateway 虚拟机部署完成之后,大家必须利用 AWS Storage Gateway 控制台对其进行激活。这一激活过程会将您的网关与 AWS 账户相关联。在建立这一连接后,大家即可立足 控制台对网关的几乎全部机制进行管理。在激活过程中,大家需要指定您的网关 IP 地址、网关名称、设置备份快照存储所在的目标 AWS 区以及网关时区。

AWS Import/Export 安全性

AWS Import/Export 是一项简单但安全的大规模数据物理传输方案,能够将数据快速迁移至 Amazon S3\EBS 或者 Amazon Glacier 当中。这项服务通常适用于迁移数据总量超过 100 GB 以及/或者互联网数据传输速度过慢的客户。利用 AWS Import/Export,大家可以自行准备一台便携式存储设备,用于将其中的数据直接邮寄至安全 AWS 设施。AWS 会利用内部高速网络将其中数据传输至自有基础设施,从而有效绕开承载能力有限的互联网路径。相反,大家也可以利用这种方式将数据从 AWS 中快速导出至本地设施。

与其它 AWS 服务一样，AWS Import/Export 服务同样要求大家自行挑选并验证您所用存储设备的安全性。在这种情况下，大家需要向 AWS 提交一条传输请求，其中包含您所使用的 Amazon S3 存储桶、Amazon EBS 区、AWS 访问密钥 ID 以及收货地址。在此之后，大家会收到一条请求标识信息，即用于验证您所用设备的数字签名，外加您需要将存储设备发送到的 AWS 地址。对于 Amazon S3，大家需要将该签名文件存放在存储设备的根目录位置。而对于 Amazon EBS，大家可以用胶带将该签名的条形码贴在设备外部。这一签名文件仅用于身份验证，而无需被上传至 Amazon S3 或者 EBS 当中。

以 Amazon S3 为例，大家可以指定作为数据加载目标的特定存储桶，从而确保账户对该存储桶拥有写入权限。大家还应当设置一套访问控制列表，用于指定各对象的目标加载 Amazon S3。

而在迁移至 EBS 时，大家应当为 EBS 导入操作指定目标区域。如果该存储设备的最大分卷容量小于等于 1 TB，则其内容可直接加载至 Amazon EBS 快照。如果存储设备的容量大于 1 TB，则设备镜像会被存储在特定 S3 日志存储桶当中。大家随后可以利用 Logical Volume Manager 等工具创建一套 Amazon EBS 分卷 RAID，同时将各镜像由 S3 复制到新分卷当中。

要进一步提升安全性水平，大家可以在将数据寄送至 AWS 之前，首先对其进行加密。对于 Amazon S3 数据，大家可以使用 PIN 码设备的硬件加密或者 TrueCrypt 软件实现数据加密。对于 EBS 以及 Amazon Glacier 数据，大家可以使用自己擎为任意加密方法，其中包括 PIN 码设备。AWS 会在将数据导入至 Amazon S3 之前，首先利用 PIN 码与/或客户提供的 TrueCrypt 密码进行加密。AWS 利用大家的 PIN 码以访问 PIN 码设备，但绝不会对需要导入至 Amazon EBS 或者 Amazon Glacier 的软件加密数据进行解密。

AWS Import/Export Snowball 采用安全性设计，其 Snowball 客户端能够加快 PB 级别数据与 AWS 设施之间的传入/传出速度。大家首先需要使用 AWS 管理控制台以创建一条或者多条请求，用于申请一台或者多台 Snowball 设备（具体取决于您需要传输的数据量），而后下载并安装 Snowball 客户端。在设备寄到之后，大家可以将其接入本地网络，手动或者利用 DHCP 设置 IP 地址，而后利用该客户端指定需要复制的目录。该客户端会自动进行数据加密与复制，同时在传输完成后向大家发出通知。

在导入完成后，AWS Import/Export 会擦除设备中的全部数据，以防其被其他客户所接触。AWS 会利用 0 将该存储设备上的全部可写入块进行覆盖。如果 AWS 无法擦除设备上的数据，则会安排将其销毁，我们的支持团队亦会通过随设备一同提供的邮件信息与您联系。

在对设备进行跨国运输时，某些海关及报关流程要求提供设备中存储的文件清单。AWS Import/Export 会利用大家提供的相关值进行入关验证并准备其它出关手续。相关选项包括是否对设备中的数据进行加密，以及所使用加密软件的具体类别。在将加密数据发出或者收入美国本土时，该加密软件必须符合美国出口管理条例 5D992 的要求。

数据库服务

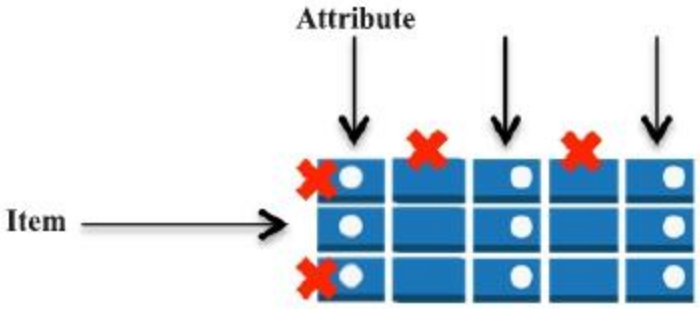
Amazon Web Services 为开发人员及企业提供多种数据库解决方案——从托管型关系数据库到 NoSQL 数据库服务，从内存内缓存即服务到 PB 级别数据仓储服务皆有涵盖。

Amazon DynamoDB 安全性

Amazon DynamoDB 是一项托管 NoSQL 数据库采取行动，其能够以无缝化扩展方式提供快速且可预测的性能表现。Amazon DYnamoDB 能够帮助大家摆脱对分布式数据库的操作与规模控制负担，这意味着大家无需为硬件选择、设置与配置、复制、软件补丁安装或者集群规模调整而分神。

大家可以创建一套数据库表，用于存储及检索任意规模的数据，同时响应任意水平的请求流量。DynamoDB 能够自动将表内的数据与对应流量传播至大量服务器之上，从而在为所指定数量的数据进行存储的同时，继续保持其一致性与理想的性能表现。全部数据条目皆被存储在固态存储驱动器（简称 SSD）之上，且以自动化方式在同一服务区内的各可用区间进行复制，旨在提供高可用性与数据持久性。大家可以利用 AWS Data Pipeline 中提供的特定模板设置自动化备份机制，其专门用于自动复制 DynamoDB 表。大家也可以选择将全部或者部分表内容备份至同一或者另一不同可用区。大家能够利用这一副本在发生故障时实现跨可用区灾难恢复，从而支持多可用区应用。

要控制用户对 DynamoDB 资源与 API 的使用，大家可以在 AWS IAM 当中设置对应权限。另外，为了控制 IAM 中的具体资源访问级别，大家也可以立足数据库层级进行访问控制——即根据具体应用需求创建数据库级权限，从而允许或拒绝对条目（行）以及属性（列）的访问。这些数据库级权限被称为细粒度访问控制，大家可以利用 IAM 策略创建此类控制规则以指定用户或者应用所能访问的具体 DynamoDB 表内容。该 IAM 策略可限制对表内特定条目、条目内特定属性或者二者兼有的访问活动。



大家可以选择使用网络身份联合对已经登录至 Amazon、Facebook 或者谷歌的应用用户进行访问控制。网络身份联合意味着我们不再需要分别创建 IAM 用户; 相反，大家可以登录至某一身份提供方，而后从 AWS 安全令牌服务（简称 AWS STS）处获取临时性登录凭证。AWS STS 会向该应用返回 AWS 凭证，从而允许用户访问特定 DynamoDB 表。

除了要求数据库与用户权限之外，每条指向 DynamoDB 服务的请求还必须包含一条有效的 HMAC-SHA256 签名，否则其会被直接拒绝。AWS SDK 会自动对请求进行签署; 然而，如果大家希望编写自己的 HTTP POST 请求，则必须在指向 Amazon DYnamoDB 的请求头中提供该签名。为了计算此签名，大家必须从 AWS 安全令牌服务处请求临时安全凭证。使用该临时安全凭证即可对您指向 Amazon DynamoDB 的请求进行签名。

Amazon DynamoDB 可通过 SSL 加密终端进行访问。各加密终端可通过互联网以及 Amazon EC2 内部网络进行访问。

Amazon Relational Database Service (简称 AmazonRDS) 安全性

Amazon RDS 允许大家快速创建一套关系型数据库实例，并灵活地对相关计算资源及存储容量进行规模伸缩，从而满足应用程序的实际需求。Amazon RDS 通过执行备份、处理故障转移并维护数据库软件等方式对数据库实例加以管理。目前，Amazon RDS 提供的相关数据库选项包括 Amazon Aurora、MySQL、PostgreSQL、甲骨文、微软 SQL Server 以及 MariaDB 等数据库引擎。

Amazon RDS 拥有多种特性，意在强化关键性生产数据库的可靠性水平，具体包括数据库安全组、权限、SSL 连接、自动备份、数据库快照以及多可用区部署等等。各数据库实例还能够部署在 Amazon VPC 当中以进一步实现网络隔离。

访问控制

当大家初次在 Amazon RDS 当中创建数据库实例时，大家需要创建一个用户账户，其仅在 Amazon RDS 内部用于控制对各数据库实例的访问。其中主用户账户属于本地数据库用户账户，允许大家以拥有全部数据库操作权限的方式登录至数据库实例。大家可以指定主用户名称及密码，并在创建数据库实例时将其关联至各必要数据库实例。数据库实例创建完成之后，大家将能够创建更多用户账户，并对其各自数据库实例访问能力加以限制。

利用 AWS IAM，大家可以进一步控制对 RDS 数据库实例的访问。AWS IAM 允许大家控制各 AWS IAM 用户所能实现的 RDS 操作调用权限。

网络隔离

要实现更为细化的网络访问控制，大家可以在 Amazon VPC 当中运行自己的数据库实例。Amazon VPC 允许大家指定所要使用的 IP 范围，同时经由行业标准加密的 IP 安全 VPN 接入现有 IT 基础设施，从而实现数据库实例隔离。在 VPC 当中运行 Amazon RDS 能够帮助大家确保数据库实例始终运行在专有子网当中。大家也可以设置一套虚拟专有网关，从而将您的企业网络延伸至 VPC 当中，旨在访问运行在其中的 RDS 数据库实例。欲了解更多细节信息，请参阅 Amazon VPC 用户指南。

部署在 Amazon VPC 当中的数据库实例可通过互联网或者 Amazon EC2 实例经由 VPN 或者在公共子网中启动的堡垒主机进行访问。要使用堡垒主机，大家需要设置一套公共子网，并利用 EC2 实例作为其 SSH 堡垒。这套公共子网必须拥有一套互联网网关及对应路由规则，负责将流量路通过该 SSH 主机进行定向——SSH 主机随后会将请求转发至 Amazon RDS 数据库实例的专有 IP 地址处。

数据库安全组可用于帮助大家确保 Amazon VPC 内各数据库实例的安全性。另外，输入及输出各子网的网络流量亦可通过网络 ACL 进行放行或者拒绝。全部通过 IP 安全 VPN 连接出入大家 Amazon VPC 的网络流量都可接受内部已部署安全基础设施的检查，具体包括网络防火墙以及入侵检测系统。

加密

大家可以利用 SSL 对应用程序与数据库实例之间的连接进行加密。对于 MySQL 与 SQL Server，RDS 服务会创建一份 SSL 证书并在实例配置流程中将该证书安装至数据库实例当中。对于 MySQL，大家需要利用—ssl_ca 参数启动 mysql 客户端，从而引用公钥以加密各条连接。对于 SQL Server，大家需要下载公钥并将证书导入至您的 Windows 操作系统。甲骨文 RDS 采用甲骨文的原生网络加密机制保护数据库实例。大家只需要在选项组中添加原生网络加密，而后将其关联至该数据库实例的选项组中即可。在加密连接建立完成后，数据库实例与客户应用程序之间的传输数据将在传输过程中进行加密。大家也可以要求自己的数据库实例仅接受加密连接。

Amazon RDS 支持对 SQL Server（SQL Server 企业版）以及甲骨文（甲骨文企业版中提供部分高级安全选项）进行透明数据加密（简称 TDE）。TDE 功能会自动对数据进行加密，而后才将其写入存储介质；而在将其读取出存储介质时，数据会首先进行解密。如果大家需要仅对数据库中的“闲置”MySQL 数据进行加密，大家的应用程序必须自行管理数据的加密与解密任务。

需要注意的是，SSL 在 Amazon RDS 当中支持应用程序与数据库实例间的连接加密，这部分任务不需要数据库实例自行处理。

尽管 SSL 提供诸多安全优势，但需要注意的是 SSQL 加密是一种计算资源密集型任务，且会给数据库连接带来延迟提升。欲了解更多 SSL 与 MySQL 间的协作细节信息，大家可以直接参阅 MySQL 说明文档。卻了解更多 SSL 与 SQL Server 间的协作细节信息，大家可以参阅 RDS 用户指南。

自动备份与数据库快照

Amazon RDS pro 提供两种不同的数据库实例备份与恢复方法：自动备份与数据库快照（DB Snapshots）。

作为默认启用的选项，Amazon RDS 服务的自动备份功能为大家的数据库实例提供恢复时间点。Amazon RDS 会备份您的数据库与事务日志，并由用户对其保留时长进行设置。通过这种方式，大家可以在保留期间随意对数据库实例进行恢复，且最长时耗仅为 5 分钟。大家的自动备份保留周期可最多设置为 35 天。

在备份窗口当中，存储 I/O 可能会由于数据备份操作而被暂停。这种 I/O 暂停状况通常持续数分钟。大家可以利用多可用区数据库部署避免这一暂停问题，因为应用可从备份副本处读取数据。

数据库快照是由用户启动的数据库实例备份。这些完整的数据库备份由 Amazon RDS 负责存储，直到大家明确要求将其删除。大家可以在各 AWS 公共区间对任意规模的快照进行并发复制与移动。在此之后，大家可以立足于任一数据库快照创建一套新的数据库实例。

数据库实例复制

Amazon 云计算资源被托管在全球范围内不同区域中的高可用性数据中心当中，且各服务区皆包含多个不同地理位置，其被称为可用区。各个可用区可彼此配合以实现故障转移，同时为同一服务区内的其它可用区提供低成本、低延迟网络连接。

Amazon RDS 利用多可用区部署为数据库实例提供高可用性与故障转移支持。多可用区部署适用于采用 Amazon 技术的甲骨文、PostgreSQL、MySQL 以及 MariaDB 等数据库实例，不过 SQL Server 数据库实例采用的则为 SQL Server Mirroring。需要注意的是，Amazon Aurora 会将同一数据库集群内的各数据副本存储在同一服务区内的各可用区当中——无论数据库集群中的各实例是否跨越多个可用区。在多可用区部署中，Amazon RDS 会在另一可用区内自动配置并维护同步待用副本。一级数据库实例会在不同可用区间进行同步复制，旨在实现数据冗余、避免 I/O 卡顿并在系统备份时将延迟控制在最低水平。当数据库实例或者可用区发生故障，Amazon RDS 会自动面向待用区进行故障转移，从而确保数据库能够尽快恢复正常运转，且整个过程无需管理操作介入。以高可用性方式运行数据库实例能够增强系统可用性，同时帮助大家的数据库免受数据库实例故障以及可用区中断的影响。

Amazon RDS 还利用 PostgreSQL、MySQL 以及 MariaDB 数据库引擎中的内置复制功能为数据库实例创建一种立足于源数据库实例的特殊副本类型，即“读取副本”。针对源数据库实例的更新会被同步复制至各读取副本。大家可以将来自应用程序的读取查询路由至读取副本，从而降低源数据库实例的负载强度。读取副本允许大家超越单一数据库实例规模限制，面向读取密集型数据库工作负载进行向外扩展。

自动软件补丁安装

Amazon RDS 能够确保您部署在其中的关系型数据库软件始终保持在最新版本。在必要时，各更新补丁亦可在您能够控制的维护窗口之内集中进行安装。大家可以将 Amazon RDS 维护窗口视为一种对数据库实例修改（例如扩展数据库实例类别）及软件补丁安装时间点的控制机制，并以请求或者必要时以事件形式触发。如果“维护”事件被规划为每周执行一次，则其会按照大家指定的时间段在 30 分钟维护窗口内完成。

极少数会导致 Amazon RDS 将数据库实例带入离线状态的维护事件包括对计算操作进行规模伸缩（其从开始到结束大约需要数分钟时间）或者必要软件补丁更新。必要补丁安装会经过规划，确保其仅在与安全性及持久性相关时才加以执行。此类补丁很少出现（通常数月出现一次），且基本应当在大家的维护窗口之内。如果大家在数据数据库实例时并未指定首选每周维护窗口，则其时长会默认设定为 30 分钟。如果大家希望修改该设置，则可在 AWS 管理控制台中或者使用 ModifyDBInstance API 完成相关调整。大家的每套数据库实例都可采用不同的偏好维护窗口，具体取决于大家的实际选择。

将数据库实例运行为多可用区部署方案可进一步降低维护事件带来的影响，因为 Amazon RDS 会通过以下步骤处理维护事件：1）在待用实例上执行维护；2）将待用实例切换为主实例；3）在原有主实例上执行维护，而后将其作为新的待用实例。

当 Amazon RDS 数据库实例检测到 API（DeleteDBInstance）运行时，该数据库实例会被标记为删除。一旦该实例不再被标记为“删除”状态，则代表其已经被移除。这时，该实例不再接受访问而且除非使用最新快照副本，否则将无法恢复且不会在工具或者 API 中被列出。

事件通知

大家可以收取 RDS 实例之上发生的各类重要事件的相关通知，例如该实例是否被关闭、备份操作开始、发生故障、安全组发生变更或者存储空间不足。Amazon RDS 服务会将各事件按类别进行分组，大家可进行结果订阅以在对应类别的事件发生时得到通知。大家能够订阅的事件类别的对象包括数据库实例、数据库快照、数据库安全组或者数据库参数组。RDS 事件会通过 AWS SNS 进行发布，并以邮件或者短信形式发送给用户。欲了解更多 RDS 通知事件分类的细节信息，请参阅 RDS 用户指南。

Amazon Redshift 安全性

Amazon Redshift 是一项 PB 级别 SQL 数据库仓储服务，其运行在经过高度优化与管理的 AWS 计算与存储资源之上。该服务的架构设计不仅能够快速实现规模伸缩，同时亦能够面向超大规模数据库集实现显著的查询提速。为了提升性能，Redshift 采用了列式存储、数据压缩以及区域映射等多项技术，用于降低执行查询所必需的 IO 数量。其还拥有一套大规模并发处理（简称 MPP）架构，能够并行分发 SQL 操作以充分发挥可用资源的全部优势。

在创建一套 Redshift 数据仓库时，大家需要配置单一节点或者多节点集群，指定节点的具体数量与类型并完成集群构建。节点类型决定了各节点的存储容量内存与 CPU 资源。每套多节点集群当中包含一个管理节点与两个或者更多计算节点。管理节点负责管理连接、解析查询、构建执行规划并管理各计算节点中的查询执行。而各计算节点则负责存储数据、执行计算并运行由管理节点指定的查询。其中各套集群中的管理节点可通过 ODBC 以及 JDBC 端点进行访问，且使用标准 PostgreSQL 驱动程序。各计算节点则运行在一套独立的隔离网络当中，且永远无法进行直接访问。

在集群配置完成之后，大家即可上传自己的数据集并利用基于常规 SQL 的工具与商务智能应用进行数据分析查询了。

集群访问

在默认情况下，大家创建的集群不会向任何人开放。Amazon Redshift 允许大家配置各类防火墙规则（安全组），从而控制指向数据仓库集群的网络访问。大家也可以在 Amazon VPC 之内运行 Redshift，从而将自己的数据仓库集群隔离在自有专有网络之内，并经由行业标准加密 IP 安全 VPN 将其接入现有 IT 基础设施。

用于创建该集群的 AWS 账户具备该集群的全部访问权限。在大家的 AWS 账户当中，您可以利用 AWS IAM 创建用户账户并对其具体权限加以管理。通过使用 IAM，大家能够对为用户分配不同权限，保证其仅能执行与工作内容相关的集群操作。

与其它数据库一样，大家必须在 Redshift 当中立足数据库层级进行权限分配，同时授予资源层级访问能力。能够接入数据库的数据库用户被称为用户账户，其在登录至 Amazon Redshift 时会进行身份验证。在 Redshift 当中，大家可以立足每集群为单位进行数据库用户权限分配，而非以数据库表为基础。在这种情况下，用户只能看到与其工作内容相关的表内特定行; 由其他用户创建的行将无法为其所查看。

用户创建的数据库对象归其自身所有。在默认情况下，只有超级用户或者对象拥有者能够对此对象进行查询、修改或者授予权限。对于那些使用对象的用户而言，他们必须为其或者其所在的组分配必要权限。另外，只有对象拥有者能够执行对象修改或者删除操作。

数据备份

Amazon Redshift 会将大家的数据分发至集群内的全部计算节点之上。当大家利用至少两台计算节点运行集群时，各节点上的数据将始终与彼此磁盘上的内容保持镜像关系，旨在降低数据丢失风险。另外，全部写入至集群内节点的数据都将持续以快照形式被备份至 Amazon S3 当中。Redshift 会将大家的快照按照用户定义的频度进行备份，具体可为 1 天到 35 天。大家也可以随时自行保存当前快照; 这些快照立足于全部现有系统快照，并在大家明确将其删除之前始终存在。

Amazon Redshift 会持续监控集群运行状况，同时自动将数据由故障驱动器甚至是故障节点当中复制出来。整个流程不会给大家的实际业务运行带来任何严重影响，不过大家可能会在重新复制时面对轻微性能下降。

大家也可以利用任何系统或者用户快照经由 AWS 管理控制台或者 Amazon Redshift API 对集群进行恢复。大家的集群将在元数据恢复完成后重新上线，这时大家可以正常运行查询，而用户数据仍在后台继续恢复。

数据加密

在创建一套集群时，大家可以选择对其进行加密，从而为闲置数据提供额外的安全保护。当在集群中启用加密功能时，Amazon Redshift 会以加密格式配合硬件加速 AES-256 块加密密钥将全部数据存储在用户创建的表当中。其中包括一切写入磁盘的数据以及备份内容。

Amazon Redshift 使用一套四层式、基于密钥的架构实现加密。这些密钥由数据加密密钥、数据库密钥、集群密钥以及主密钥共同构成：

- 数据加密密钥会在集群内对数据块进行加密。每个数据块会被分配予一条随机生成的 AES-256 密钥。这些密钥通过集群中的数据库密钥进行加密。

- 数据库密钥负责对集群内的数据加密密钥进行加密。数据库密钥属于一条随机生成的 AES-256 密钥。其存储在位于 Amazon Redshift 之外独立网络内的磁盘当中，同时由主密钥负责进行加密。Amazon Redshift 会通过安全通信进行数据库密钥传输，且将其保存在集群的内存当中。

- 集群密钥负责对 Amazon Redshift 集群内的数据库密钥进行加密。大家可以使用 AWS 或者硬件安全模块（简称 HSM）以存储此集群密钥。HSM 允许大家对密钥的生成与管理工作进行直接控制，同时确保密钥管理工作与其它应用及数据库不致相互干扰。

- 主密钥负责对存储在 AWS 当中的集群密钥进行加密。如果集群密钥存储在 HSM 当中，则主密钥则负责对由集群密钥加密的数据库密钥进行加密。

大家可以随时对加密集群中使用的加密密钥进行轮换。作为轮换流程中的组成部分，各密钥能够对各集群以自动以及手动方式生成的快照进行更新。

需要注意的是，在集群当中启用加密功能会对性能造成一定影响——尽管其已经配合硬件加速机制。加密机制亦适用于备份数据。在利用加密快照进行恢复时，新集群也将同时受到加密。

要在将表加载数据文件上传至 Amazon S3 时对其进行加密，大家可以使用 Amazon S3 的服务器端加密机制。而在从 Amazon S3 中加载数据时，COPY 命令会在数据加载至表中时对其进行解密。

数据库审计日志

Amazon Redshift 会记录全部 SQL 操作，其中包括连接尝试、查询以及数据库内容变更。大家可以利用 SQL 查询对系统表进行日志访问，或者将其下载至安全的 Amazon S3 存储桶。在此之后，大家可以使用这些审计日志来监控集群，从而实现安全保障及故障排查等效果。

自动软件补丁安装

Amazon Redshift 负责管理与数据仓库相关的各类设置、操作与规模伸缩任务，具体包括配置容量、监控集群以及针对 Amazon Redshift 引擎应用补丁与升级。各补丁只会在指定的维护窗口之内进行安装。

SSL 连接

要对 AWS 云之内中转的数据进行保护，Amazon Redshift 采用硬件加速 SSL 以保障 Amazon S3 或者 Amazon DynamoDB 中的 COPY、UNLOAD、备份以及恢复等操作的相关通信流程。大家可以在客户端与集群之间通过在与集群相关联的参数组内指定 SSL 实现连接加密。为了确保您的客户端同样对 Redshift 服务器进行验证，大家也可以在自己的客户端上为 SSL 证书安装公钥（.pem 文件），同时利用该密钥接入对应集群。

Amazon Redshift 提供更新、更为强大的加密套件，其利用椭圆曲线 Diffie-Hellman 临时（简称 ECDHE）协议实现加密。ECDHE 允许 SSL 客户端提供客户端与 Redshift 集群之间的完全转发保密机制。完全转发保密机制利用临时性会话密钥进行加密，其不会被保存在任何位置，这就避免了未授权第三方对所捕获的数据进行解密——即使其已经掌握有长期密钥。大家不需要在 Amazon Redshift 内进行任何设置即可启用 ECDHE; 如果大家利用 SQL 客户端工具进行接入，且该工具利用 ECDHE 加密客户端与服务器间的通信内容，则 Amazon Redshift 会利用由其提供的加密列表建立对应的连接。

Amazon ElastiCache 安全性

Amazon ElastiCache 是一项 Web 服务，可帮助大家在云端轻松实现分布式内存内缓存环境的设置、管理与规模伸缩。该服务允许大家利用速度更快的托管型内存内缓存系统进行信息检索，从而绕过速度较慢的磁盘数据库，旨在有效改善 Web 应用程序性能水平。其可用于显著改善高读取强度应用程序工作负载（例如社交网络、游戏、媒体共享以及常见问题查询门户）或者计算密集型工作负载（例如推荐引擎）的延迟表现及数据吞吐能力。

缓存机制可将关键性数据片段保存在内存中以提供更低访问延迟，从而改善应用程序性能。适合由缓存处理的信息包括 I/O 敏感型数据库查询结果或者计算敏感型结果。

Amazon ElastiCache 服务能够对内存内缓存环境进行自动化时间消耗任务管理，具体包括补丁管理、故障检测以及恢复等等。其可与其它 Amazon Web Services 配合起效（例如 Amazon EC2、Amazon CLoudWatch 以及 Amazon SNS 等），旨在提供更加安全、性能更出色且全面托管型内存内缓存方案。举例来说，运行在 Amazon EC2 实例中的应用程序可安全访问同一区域内的 Amazon ElastiCache 集群，且享受极低延迟水平。利用 Amazon ElastiCache 服务，大家可以创建一套缓存集群，其中汇聚了一套或者多套缓存节点。单一缓存节点相当于大小固定的安全、网络接入型内存资源池。各个缓存节点皆运行有 Memcached 或者 Redis 协议兼容性服务实例，且拥有自己的 DNS 名称与端口。

AWS 支持多种缓存节点类型，其中每一种都拥有不同的关联内存容量。缓存集群可包含特定数量的缓存节点，同时由一套缓存参数组负责控制各缓存节点的属性。单一缓存集群中的全部缓存节点皆需要属于同一种节点类型，且共享同样的参数与安全组设置。

Amazon ElastiCache 允许大家利用缓存安全组机制对指向缓存集群的访问加以控制。缓存安全组的运作方式类似于防火墙，其负责控制指向缓存集群的网络访问。在默认情况下，指向缓存集群的网络访问会被全部拒绝。如果大家希望应用程序访问自己的缓存集群，则必须在特定 EC2 安全组中明确启用主机访问许可。一旦入口规则配置完成，同样的规则将适用于全部与该缓存安全组相关联的缓存集群。

要接纳指向缓存集群的网络访问，大家需要创建一套缓存安全组并将其与必要的 EC2 安全组对接（此 EC2 安全组负责指定允许通过的 EC2 实例）。大家可以在创建缓存集群时将其与缓存安全组相关联亦可在 AWS 管理控制台中使用“Modify（修改）”选项。目前缓存集群尚不支持基于 IP 范围的访问控制功能。指向缓存集群的全部客户端必须人性于该 EC2 网络，且通过缓存安全组进行授权。

面向 Redis 的 ElastiCache 机制提供备份与恢复功能，大家可以借此为特定时间点中的整体 Redis 集群创建一套快照。大家亦可以规划每天自动保存快照，或者随时手动保存当前快照。对于自动化快照方案，大家需要指定其轮换周期; 手动快照则将在大家明确将其删除前始终存在。各快照存储在 Amazon S3 当中并具备极高持久性，可随时用于启动、备份与归档。

应用服务

Amazon Web Services 提供一系列托管型服务，可配合大家的应用程序共同起效，其功能具体包括提供应用流、查询、通知推送、邮件交付、搜索乃至转码等等。

Amazon CloudSearch 安全性

Amazon CloudSearch 是一项云端托管服务，能够帮助大家简化自有网站的设置、管理与规模伸缩。Amazon CLoudSearch 允许大家对各类大规模数据集合进行搜索，其中包括网页、文档文件、论坛帖子或者产品信息等等。在它的帮助下，大家能够向网站当中快速添加搜索功能，而无需雇用搜索技术专家或者对硬件进行配置、设置与维护。随着数据与流量规模的不断提升，Amazon CLoudSearch 会自动进行规模调以满足您的实际业务需求。

一个 Amazon CLoudSearch 域封装有大家需要搜索的全部数据集合、负责处理搜索请求的搜索实例，同时提供一套配置方案以控制如何对数据进行索引与搜索。大家需要为接受搜索的每套数据集合创建一个独立的搜索域。在各个域中，大家需要配置索引选项以描述目录中所应包含的字段、这些字段的使用方式、用于定义特定域停用词的文本选项、搜索结构、自定义同义词搜索方法、结果排序方法、域文件访问控制策略以及搜索端点等等。

指向搜索域端点的访问根据 IP 地址进行限制，这意味着只有授权主机能够提交文档并发送搜索请求。IP 地址授权机制仅适用于对指向文档及搜索端点的访问控制场景。全部 Amazon CloudSearch 配置请求必须利用标准 AWS 认证机制进行审查。

Amazon CloudSearch 提供多个独立端点，用于访问配置、搜索与文档服务：

- 大家可以利用配置服务创建并管理自己的搜索域。各区域限定配置服务端点皆以“cloudsearch.region.amazonaws.com”形式存在，例如“cloudsearch.us-east-1.amazonaws.com”。欲了解受支持区域的当前列表，请参阅 AWS 常规参考中的区域与端点页面。该文档服务端点可用于向域内提交索引用文档，同时通过域特定端点 http://doc-domainname-domainid.us-east-1.cloudsearch.amazonaws.com 接受访问。

- 搜索端点用于向域提交搜索请求，且可通过域特定端点进行访问：http://search-domainname-domainid.us-east-1.cloudsearch.amazonaws.com

需要注意的是，如果大家不具备静态 IP 地址，则必须在 IP 地址发生变化时对计算机进行重新授权。如果大家的 IP 地址以动态形式分配，则可能意味着您将该地址共享给了网络中的其它计算机。这意味着当大家授权该 IP 地址时，所有共享该地址的计算机都能够访问您的搜索域文档服务端点。

与其它 AWS 服务一样，Amazon CloudSearch 同样利用其控制 API 对各项请求进行授权，意味着只有授权用户能够访问并管理大家的 CloudSearch 域。API 请求以 HMAC-SHA1 或者 HMAC-SHA256 进行签名，其由请求本身以及用户的 AWS 保密访问密钥计算得出。另外，Amazon CloudSearch 控制 API 通过 SSL 加密端点进行访问。大家可以在您的 AWS 账户之下利用 AWS IAM 创建用户，从而控制指向各 Amazon CloudSearch 管理功能的访问请求，同时管理对应用户具备执行哪些操作的权限。

Amazon Simple Queue Service (简称 Amazon SQS)

安全性

Amazon SQS 是一项具备高可靠性与可扩展性的消息队列服务，负责实现应用程序当中各分布式组件之间的异步式通信。各组件可作为计算机或者 Amazon EC2 实例，抑或是二者兼有的形式存在。利用 Amazon SQS，大家可以立足任何组件向 Amazon SQS 队列中随时发送任意数量消息。各消息可由同一组件、不同组件或者随后（14 天之内）进行检索。消息数据亦具备高持久性; 每条消息将得到永久存储以实现高可用性、高可靠性队列。多个进程可同时指向 Amazon SQS 队列进行读取/写入，且不会造成相互影响。

Amazon SQS 访问基于 AWS 账户或者由 AWS IAM 创建的用户实现。一旦通过验证，AWS 账户将能够完全访问全部用户操作。然而，AWS IAM 用户则只能访问到其通过策略被分配到的对应权限之内的操作与队列。在默认设置下，所有指向单一队列的访问都仅限于创建该队列的 AWS 账户。不过，大家也可以使用 SQS 生成的策略或者自行编写的策略允许其它队列访问请求。

Amazon SQS 通过 SSL 加密端点接受访问。各加密端点可经由互联网或者 Amazon EC2 之内实现访问。存储在 Amazon SQS 之内的数据不会由 AWS 进行加密; 不过，用户可以在将其上传至 Amazon SQS 之前进行数据加密，意味着由应用程序本身提供加密机制并在检索消息时进行解密。

在将消息上传至 Amazon SQS 之前对其进行加密，有助于保护相关敏感性内容免受未授权个人——包括 AWS ——的访问。

Amazon Simple Notification Service (简称 AmazonSNS) 安全性

Amazon Simple Notification Service （即 Amazon 简单通知服务，简称 Amazon SNS）是一项用于简化云端通知信息设置、操作与发送的 Web 服务。其为开发人员提供具备高度可护性、灵活性及成本效益的方式，用于立足 应用程序发布消息并立即将其交付至订阅用户或者其它应用。

Amazon SNS 提供一套简单的 Web 服务界面，可用于创建与必要通知应用（或者个人）对象相关的主题，可面向订阅客户、公开消息，且全部消息皆经由客户选定的协议（例如 HTTP/HTTPS、邮件等）进行交付。Amazon SNS 利用“推送”机制向客户发送通知，从而消除了对方定期检查或者“提取”新信息与更新内容的需要。Amazon SNS 可用于构建高可靠性事件驱动型工作流以及消息收发应用，且无需涉及复杂的中间件与应用管理任务。Amazon SNS 的潜在用例包括监控应用程序、工作流系统、时间敏感型信息更新、移动应用等等。Amazon SNS 还提供多种访问控制机制，确保各主题与消息不至受到未授权访问的影响。主题拥有方能够为其设置策略，从而指定哪些用户能够发布或者订阅特定主题。另外，主题拥有方还能够将交付机制指定为仅 HTTPS，从而实现传输加密。

Amazon SNS 访问可基于 AWS 账户或者由 AWS IAM 创建的用户进行授权。在经过验证之后，AWS 账户将拥有对全部用户操作的访问权限。不过 AWS IAM 用户将只能根据策略设置访问与其工作内容相关的操作与主题。在默认情况下，仅有创建主题的 AWS 账户能够对该主题进行访问。当然，大家也可以使用由 SNS 生成的策略或者自行编写的策略允许其它指向 SNS 的访问请求。

Amazon Simple Workflow Service (简称 Amazon SWF)安全性

Amazon Simple Workflow Service (即 Amazon 简单工作流服务，简称 SWF) 能够帮助大家轻松构建应用程序，确保其跨越各分布式组件进行协同工作。利用 Amazon SWF，大家可以在应用之内构建多个处理步骤，并将其作为“任务”用于驱动分布式应用之间的工作; Amazon SWF 会以可靠且可扩展模式对这些任务加以协调。Amazon SWF 可根据开发者的应用逻辑管理任务执行的依赖性、调度以及一致性。此项服务可存储各任务，将其拆分为应用组件，追踪具体进程并保持其始终处于最新状态。

Amazon SWF 提供简单的 API 调用方式，允许大家以任意语言编写代码并将其运行在 EC2 实例之上，亦可立足全球范围内任何接入互联网计算设备。Amazon SWF 可作为一套协调中枢，且能够与大家的应用主机进行交互。大家可利用其关联任务以及实际需要的任何条件性逻辑创建必要工作流，而后将其存储在 Amazon SWF 当中。

Amazon SWF 基于 AWS 账户或者由 AWS IAM 创建的用户进行授权。所有与工作流执行相关的对象——包括决策者、活跃工作人员、工作流管理员等——皆必须以 IAM 用户的形式归属于拥有该 Amazon SWF 资源的 AWS 账户之下。大家无法授权归属于其它 AWS 账户的用户访问自己的 Amazon SWF 工作流。另外，AWS IAM 用户也只能根据策略分配的权限访问对应的工作流与资源。

Amazon Simple Email Service (简称 Amazon SES)安全性

Amazon Simple Email Service（即 Amazon 简单邮件服务，简称 SES）立足于 Amazon 高可靠性与可扩展性基础设施的仅出站邮件发送服务。Amazon SES 能够帮助大家最大程度提升邮件交付能力，同时随时掌握邮件的交付状态。Amazon SES 可与其它 AWS 服务进行集成，从而简化由托管在各服务（例如 Amazon EC2）之上应用程序的邮件发送流程。

遗憾的是，其它电子邮件系统有可能作为垃圾邮件发送方篡改电子邮件标题并伪造其实际地址，从而使其看似来自其它来源。为了解决这些问题，Amazon SES 要求用户自行验证相关邮件地址或者域名，以防止其他未授权人士加以使用。要进行域名验证，Amazon SES 要求发件人提供由 Amazon SES 分配的 DNS 记录以作为对该域名拥有控制权的证明。Amazon SES 会定期审查域名有效性状态，同时撤销那些不再有效的用例。

Amazon SES 采取一系列主动举措以防止发送可疑内容，确保互联网服务供应商始终从我们的域处接收到高质量邮件，从而始终将 Amazon SES 视为受信邮件来源。以下为各项针对发件人的交付性与可靠性保障手段：

- Amazon SES 利用内容过滤技术帮助大家检测并屏蔽一切包含病毒或者恶意软件的消息，防止其被实际发出。

- Amazon SES 与各大互联网服务供应商保持着投诉反馈合作。各项投诉反馈所涉及的收件人发送内容将被标记为垃圾邮件。Amazon SES 允许大家访问这些交付指标，从而通过引导顺利设置发送策略。

· Amazon SES 利用一系列技术以衡量用户所发送内容的实际质量。这些机制可帮助大家识别并禁用计划之外的 Amazon SES 邮件，同时检测一切可能危及 Amazon SES、互联网服务供应商、邮件服务供应商以及反垃圾邮件服务声誉的异常发送模式。

· Amazon SES 支持多种验证机制，具体包括发送方策略框架（简称 SPF）以及域名密钥识别邮件（简称 DKIM）。当大家对邮件进行验证时，需要向互联网服务供应商提供证据以证明自己对域名的所有权。Amazon SES 能够帮助大家简化对邮件的验证。如果大家利用 Easy DKIM 配置账户，则 Amazon SES 会根据您的实际操作利用 DKIM 进行邮件签名，帮助大家将注意力集中在其它邮件发送策略身上。为了确保交付优化效果，我们建议大家对自己的邮件进行预先验证。

在配合其它 AWS 服务时，大家可以利用安全凭证以验证用户的真实身份及其是否拥有与 Amazon SES 进行交互的权限。欲了解更多凭证使用信息，请参阅配合 Amazon SES 使用凭证。Amazon SES 还能够与 AWS IAM 相集成，帮助大家指定用户所能执行的 Amazon SES API 操作。

如果大家选择通过其 SMTP 接口与 Amazon SES 进行通信，则必须利用 TLS 对自己的连接进行加密。Amazon SES 支持两种 TLS 加密连接建立机制：STARTTLS 与 TLS Wrapper。如果大家选择在 HTTP 之上进行 Amazon SES 通信，那么全部通信内容皆会经由 Amazon ESE 的 HTTPS 端点接受 TLS 的保护。在将邮件交付至最终目的地时，Amazon SES 会利用随机 TLS 对邮件内容进行加密——如果接收方支持这一机制的话。

Amazon Elastic Transcoder Service（即 Amazon 弹性转码服务）安全性

Amazon 弹性转码服务能够以自动化方式显著简化将媒体文件由一种格式、大小或者质量转换为另一种的复杂流程。弹性转码服务能够对标准分辨率（简称 SD）或者高分辨率（简称 HD）视频文件进行转码，同时亦支持音频文件。其从 Amazon S3 存储桶中读取输入数据，对其进行转码，而后将结果文件写入至另一 Amazon S3 存储桶。大家可以使用同一存储桶保存输入与输出结果，且各存储桶可处于任意 AWS 服务区。弹性转码服务可接受多川输入文件类型，包括各类网络、消费级与专业格式。输出文件类型则包括 MP3、MP4、OGG、TS、WebM、使用 MPEG-2 TS 的 HLS 外加 fmp4。另外，其可存储 H.264 或者 VP8 视频以及 AAC、MP3 或者 Vorbis 音频。

大家可使用一个或者多个输入文件，同时利用所谓转码通道对每个文件创建转码任务。在创建此通道时，大家需要指定输入与输出存储桶，外加 IAM 角色。每个任务必须引用一种媒体转换模板，即转码样式，其将提供一个或者多个输出文件。此样式告知弹性转码服务使用哪些设置以处理特定输入文件。大家可以在创建样式时指定多项设置内容，具体包括示采样率、码率、分辨率（输出视频的高度与宽度）、引用与关键帧数量、视频码率以及其它多种创建选项。

最理想的方式当然是按照提交顺序分步执行上述任务，但这种作法往往缺少灵活性且在遭遇问题时难以应对。因此，弹性转码服务允许大家随时暂停及恢复自己的转码执行流程。

弹性转码服务支持使用 SNS 通知服务，意味着当其开始及结束各项任务时会向用户发送通知，或者在检测到错误或者警告状况时发布提醒。SNS 通知参数会与各流程进行关联。其亦可利用“按状态列出任务”功能找到符合特定状态的任务（例如‘已完成’），或者使用“读取任务”功能以检索与特定任务相关的细节信息。

与其它 AWS 服务一样，弹性转码服务亦可与 AWS 身份与访问管理（简称 IAM）相集成，允许大家对指向服务及其它弹性转码必要 AWS 资源的访问加以控制，具体包括 Amazon S3 存储桶与 Amazon SNS 主题。在默认情况下，IAM 用户无法访问弹性转码服务或者其使用的对应资源。如果大家希望各 IAM 用户能够使用弹性转码服务，则必须明确为其分配权限。

Amazon 弹性转码服务要求所有指向其控制 API 的请求皆经过验证，因此只有授权进程或者用户能够对自身 Amazon 转码通道及样式设置进行创建、修改或者删除。各请求经过 HMAC-SHA256 签名，此签名则由请求本身外加用户保密密钥提供的密钥计算得出。另外，Amazon 弹性转码 API 仅可经由 SSL 加密端点进行访问。

持久性由 Amazon S3 负责保证，其中各媒体文件以冗余方式存储在同一 Amazon S3 服务区内多套设施中的多台设备之上。要避免用户不慎对媒体文件进行误删，大家还可以使用 Amazon S3 提供的版本控制功能以实现在存储桶内各对象各个版本的保留、检索与恢复能力。大家还可以利用 Amazon S3 版本控制 MFA 删除功能进一步保护各数据版本。在旦在 Amazon S3 存储桶中启用此功能，每项版本删除请求都需要输入六位数编码及来自多因素验证设备的序列号方可完成。

Amazon AppStream 安全性

Amazon AppStream 服务提供一套框架，用于运行流应用，特别是那些要求在移动设备上运行轻量化客户端的应用程序。其允许大家在云环境中立足强大的并发处理 GPU 存储并运行自己的应用程序，并将数据流输入及输出至任意客户端设备。大家可以对现有应用程序进行修改以确保其对接 Amazon AppStream，亦可立足 服务协作需求创建新的应用程序。

Amazon AppStream SDK 能够简化交互式流应用与客户端应用的开发流程。该 SDK 提供相关 API，用于将客户设备与应用程序直接对接，以近实时方式通过互联网进行音频、视频与流媒体内容的捕捉与编码，在客户端设备上进行解码并将用户输入结果返回至该应用程序。由于应用程序的处理流程完全在云环境下实现，因此其能够承载极为可观的计算负载。

Amazon AppStream 将流应用部署在 Amazon EC2 实例之上。当大家通过 AWS 管理控制台添加一款流应用时，该服务会创建托管应用及实现客户端应用可用性的必要 AMI。该服务能够根据需求对应用程序规模进行自动调整，从而确切满足实际资源用量。使用 Amazon AppStream SDK 的客户端会自动接入您的流应用。

在大多数情况下，大家需要确保运行该客户端的用户在获取会话 ID 并使用应用之前，首先获得正确授权。我们建议大家使用授权服务实现这一目标，由其负责验证客户并对指向应用程序的连接进行授权。在这种情况下，授权服务会调用 Amazon AppStream REST API 以创建一条新的客户端流会话。在会话创建完成之后，其会将该会话标识以一次性授权 URL 的形式返回至授权客户端。客户端随后即可使用此授权 URL 接入应用程序。大家可将授权服务托管在 Amazon EC2 实例或者 AWS Elastic Beanstalk 之上。

Amazon AppStream 利用一套 AWS CloudFormation 模板以自动完成 GPU EC2 实例的部署流程，其中安装有 AppStream Windows 应用与 Windows 客户端 SDK 库，且面向 SSH、RDC 或者 VPN 访问进行了配置; 另外，其亦被分配予一个弹性 IP 地址。通过使用此模板进行独立流服务器部署，大家只需要将应用程序上传至服务器并运行命令将其启动即可。在此之后，大家可以使用 Amazon AppStream 服务模拟工具以独立模式测试自己的应用，并在一切正常后将其部署至生产环境。

Amazon AppStream 还利用 STX 协议管理由 AWS 指向本地设备的应用程序数据流。Amazon AppStream STX 协议可用于在多种网络条件之下发布高质量应用视频流; 其会监控网络状况并自动适配视频流，确保其始终以低延迟与高分辨率方式交付至客户。这项协议能够将延迟控制在最低水平，实现音频与视频同步，同时从客户处捕捉输入内容并将其发送回运行在 AWS 当中的应用程序处。

分析服务

Amazon Web Services 提供一系列基于云的分析服务，旨在帮助大家对各种规模的数据进行处理与分析——具体适用场景包括托管 Hadoop 集群、实时流数据、PB 级别数据仓库以及编排任务。

Amazon Elastic MapReduce (简称 Amazon EMR)安全性

Amazon Elastic MapReduce (简称 Amazon EMR)是一项托管网络服务，允许大家将任意规模的工作负载与数据分发至多台服务器，同时运行 Hadoop 集群对其进行处理与分析。其利用一套经过强化且运行在 Amazon EC2 与 Amazon S3 基础设施之上的 Apache Hadoop 框架版本。大家可以轻松将自己的输入数据与数据处理应用上传至 Amazon S3 当 。Amazon EMR 随后会启动您所指定数量的 Amazon EC2 实例。该服务会首先执行任务流，同时从 Amazon S3 中提取输入数据并将其加载至刚刚启动的 Amazon EC2 实例当中。在任务流完成之后，Amazon EMR 会将输出数据传输回 Amazon S3，大家可在这里对结果进行检索或者将其作为其它任务流的输入结果。

在启动各任务流时，Amazon EMR 会设置两个 Amazon EC2 安全组：其一面向主节点，其二则面向从节点。其中主安全组开放一个端口，用于同该服务进行通信。其同时开放一个 SSH 端口，允许大家通过事先指定的 SSH 密钥接入该实例。各从节点则存在于另一安全组内，其仅接受来自主实例的交互请求。在默认情况下，这两套安全组皆被设置为不接受任何来自外部的访问，其中包括归属于其他客户的 Amazon EC2 实例。由于这些安全组存在于您的账户之内，因此大家可以使用标准 EC2 工具或者仪表板对其进行重新配置。为了保护客户的输入与输出数据集，Amazon EMR 会利用 SSL 进行指向 Amazon S3 的数据传入与传出操作。

Amazon EMR 提供多种方式，用于控制指向集群资源的访问。大家可以使用 AWS IAM 以创建用户账户及角色，同时配置其权限以指定各用户能够访问哪些 AWS 功能。在启动一套集群时，大家可以为其分配一套 Amazon EC2 密钥对，大家随后可利用此密钥对通过 SSH 接入该集群。大家也可以设置对应权限，允许 Hadoop 默认用户之外的使用者向集群提交任务。

在默认情况下，如果一位 IAM 用户启动了一套集群，那么该集群将不可为同一 AWS 账户下的其他 IAM 用户所见。这种过滤机制适用于全部 Amazon EMR 界面——包括控制台、CLI、API 以及 SDK，旨在帮助 IAM 用户免受其他 IAM 使用者的访问与变更影响。这种作法适用于仅支持单一 IAM 用户与主 AWS 账户进行查看的场景。大家也可以利用相关选择确保集群可供单一 AWS 账户下全部 IAM 用户查看及接入。

为了增加额外的保护层，大家也可以在 Amazon VPC 之内启动 EMR 集群的各 EC2 实例，即相当于在专有子网内构建这套体系。如此一来，大家即可对整套子网加以控制。大家也可以将集群启动于 VPC 当中，同时允许利用 VPN 连接的内部网络资源访问请求。大家可以在将输入数据上传至 Amazon S3 衫，利用任意常见数据加密工具对其进行加密。如果大家在上传前完成了数据加密，随后则需要在 Amazon Elastic MapReduce 从 Amazon S3 中获取这部分数据时添加对应的解密步骤。

Amazon Kinesis 安全性

Amazon Kinesis 是一项托管服务，专门用于处理大数据的实时数据流。其能够从任意数量的来源处接纳任意规模的数据，同时根据实际需求进行规模伸缩。大家可以利用 Kinesis 对超大规模实时数据进行收集与处理，具体包括服务器日志、社交网络或者市场数据，以及网络点击流数据等。

应用程序会以数据流方式面向 Amazon Kinesis 进行数据记录读取与写入。大家可以创建任意数量的 Kinesis 流，用于捕捉、存储及传输数据。Amazon Kinesis 能够自动管理必要的基础设施、存储、网络与配置任务，确保大家能够根据流应用程序的实际需求收集并处理数据。大家无需为实现数据实时捕捉与大规模存储所必需的硬件、软件或者其它服务带来的配置、部署或者持续维护而分神。Amazon Kinesis 还能够以同步方式将数据跨越同一 AWS 服务区中的三套设施进行复制，从而实现数据的高可用性与持久性。

在 Amazon Kinesis 当中，数据记录当中包含一条序列号、一条分段密钥以及一个数据 blob，后者为一条未解释且不可变序列。Amazon Kinesis 服务不会对 blob 中的任何数据进行检查、解释或者变更。数据记录只能在被添加到 Amazon Kinesis 流中的 24 小时之内接受访问，在此之后其会被自动丢弃。

大家的应用程序属于 Amazon Kinesis 流的消费者，其能够运行在一整套 Amazon EC2 实例之上。一款 Kinesis 应用程序使用 Amazon Kinesis 客户端库以从 Amazon Kinesis 流中读取数据记录。该 Kinesis 客户端库负责一系列细节任务的执行，具体包括故障转移、恢复以及负载均衡等等，允许大家的应用专注于处理各类可用数据。在记录处理完成之后，大家的消费应用代码可将其传递至另一 Kinesis 流; 随后写入至 Amazon S3 存储桶、Redshift 数据仓库或者 DynamoDB 表; 或者直接将其丢弃。连接器库则能够帮助大家将 Kinesis 与其它 AWS 服务（例如 DynamoDB、Redshift 以及 Amazon S3 等）乃至第三方产品（例如 Apache Storm）进行集成。

大家可以通过在 AWS 账户下利用 AWS IAM 创建用户的方式控制指向 Kinesis 资源及管理功能的逻辑访问，外加 Kinesis 允许这些用户执行的具体操作权限。要在 Amazon EC2 实例之上运行您的生产或者消费应用，大家可以将该实例同 IAM 角色加以关联。通过这种方式，反映至对应角色的 AWS 凭证将被分配至该实例中的应用程序内，意味着大家无需为其提供任何长期 AWS 安全凭证。各角色提供的临时性凭证会在短时间内过期，这就为大家的业务环境带来了额外的安全保障。欲了解更多与 IAM 角色相关的细节信息，请参阅 IAM 使用指南。

Amazon Kinesis API 只接受经由 SSL 加密端点（kinesis.us-east-1.amazonaws.com）进行的访问，旨在确保您的数据以安全方式传输至 AWS。大家必须接入该端点以访问 Kinesis，或者利用指向 AWS Kinesis 的 API 在 AWS 服务区内创建数据流。

AWS Data Pipeline 安全性

AWS Data Pipeline 服务能够帮助大家在不同数据源之间利用数据驱动型工作流及内置依赖性检查机制实现数据的处理与迁移。当创建这样一条通道时，大家需要定义数据源、预定条件、目的地、处理步骤以及操作规划。在定义并激活一条通道时，其将自动根据您所指定的规划实现运行。

> With AWS Data Pipeline, you don't have to worry about checking resource availability, managing inter-task dependencies, retrying transient failures/timeouts in individual tasks, or creating a failure notification system. AWS Data

利用 AWS Data Pipeline，大家不再需要费心检查资源可用性、管理任务间依赖性、对个别任务中的传输失败/超时进行重试或者创建故障通知系统。AWS Data Pipeline 会负责处理各类数据处理通道中必需的 AWS 服务与资源（例如 Amazon EC2 或者 EMR），同时将结果传输至存储端（例如 Amazon S3、RDS、DynamoDB 或者 EMR）。

当大家使用控制台时，AWS Data Pipeline 会创建必要的 IAM 角色及策略，其中包括一份受信工具列表。IAM 角色会检测您的通道所能访问的内容以及可以执行的操作。另外，当大家的通道创建一项资源，例如一个 EC2 实例，IAM 角色会检测该 EC2 实例所对应的资源与活动。在创建通道时，大家需要指定一个 IAM 角色以管理通道，并利用另一 IAM 角色管理通道所使用的资源（亦被称为‘资源角色’），当然二者也可以使用同一角色。作为最低权限安全最佳实践的组成部分，我们建议大家考虑仅为通道提供执行工作所必需的权限，并据此定义 IAM 角色。

与大多数 AWS 服务一样，AWS Data Pipeline 同样提供仅允许通过 SSL 安全（HTTPS）端口进行接入的选项。

部署与管理服务

Amazon Web Services .提供一系列工具，用以帮助大家开发及管理自己的应用程序。此类服务允许大家利用接入 AWS 服务的凭证创建各独立用户账户。其同时包含多项服务，用以创建及更新 AWS 资源堆栈、在此类资源之上部署应用程序同时监控其它 AWS 资源的运行状况。其它工具则能够帮助大家管理利用硬件安全模块生成的加密密钥以及用于安全及合规性保障的 AWS API 活动记录。

AWS 身份与访问管理(简称 AWS IAM)

AWS IAM 允许大家创建多个用户，同时在 AWS 账户当中对各个用户的操作权限进行管理。一个用户相当于配备有惟一安全凭证的身份（立足 AWS 账户之内），这部分凭证可用于访问各类 AWS 服务。AWS IAM 帮助大家摆脱了共享密码或者密钥的需求，且极大简化了对用户访问活动的启用与禁用流程。

AWS IAM 允许大家实现各类安全最佳实践，例如最低权限、在 AWS 账户之内对各用户进行权限分配以及仅为用户提供执行任务所必需的 AWS 服务与资源访问能力等。AWS IAM 默认安全，新用户直接被分配予适当权限方可对 AWS 进行访问。

AWS IAM 还与 AWS Marketplace 相集成，意味着大家能够控制企业中各位员工对 Marketplace 内软件与服务的订阅权限。由于 Marketplace 中的特定软件订阅需要配合 EC2 实例以运行该软件，因此这一访问控制能力拥有重要意义。利用 AWS IAM 控制对 AWS Marketplace 的访问，亦能够帮助 AWS 账户拥有者更为细化地对软件使用量及成本进行控制。

AWS IAM 允许大家以最低限度使用 AWS 账户凭证。一旦大家创建了 AWS IAM 用户账户，与 AWS 服务及资源间的全部交互都将利用这部分 AWS IAM 用户安全凭证实现。欲了解更多 AWS IAM 相关细节信息，请参阅 AWS 网站。

角色

一个 IAM 角色可利用临时性安全凭证，允许大家委派其访问平时并不需要涉及的 AWS 资源。角色相当于一组权限集合，用于访问特定 AWS 资源，但这部分权限并不会绑定至特定 IAM 用户或者群组。由授权实体（例如移动用户、EC2 实例等）消费角色并收取该角色定义中指向的资源授权相关凭证。临时性安全凭证能够提供更出色的安全保护效果，因为其存在周期较短（默认过期时长为 12 小时）且无法 在过期后进行恢复。这一设计特别适合特定状况下的受限、受控访问活动：

· 联合（非 AWS）用户访问。联合用户属于那些不归属于 AWS 账户的用户（或者应用程序）。利用角色，大家可以在特定时间段内允许其接入自己的 AWS 资源。这一设计特别适合那些需要进行授权但又不属于 AWS 用户的外部服务，例如微软 Active Directory、LDAP 或者 Kerberos。对应的临时性 AWS 凭证与角色配合以提供 AWS 与企业身份与授权系统内非 AWS 用户间的联合。

· 如果大家的企业支持 SAML 2.0（即安全断言标记语言 2.0），则可以将当前组织作为身份供应方（IdP），另一组织作为服务供应方，并在二者之间建立信任关系。在 AWS 当中，大家可以将 AWS 配置为服务供应方，并利用 SAML 为用户提供指向 AWS 管理控制台的联合单点登录（简称 SSO）机制，或者以联合方式接入并调用 AWS API。

· 各角色还能够帮助大家所创建的移动或者 Web 应用程序接入 AWS 资源。各 AWS 资源要求以编程化请求提供安全凭证; 不过，大家不应将长期安全凭证嵌入至应用程序当中，因为其可能会被应用用户所获取且难以轮换。相反，大家可以允许用户通过登录至 Amazon、Facebook 或者谷歌的方式登录应用程序，而后再利用其验证信息作为角色获取临时性安全凭证。

· 跨账户访问。对于那些利用多个 AWS 账户以管理自身资源的企业而言，大家可以设置多个角色为用户提供单一账户内访问另一账户资源所必需的权限。对于那些员工几乎不需要访问其它账户资源的企业，则可利用角色机制确保各安全凭证仅在必要时以临时方式提供。

· 运行在 EC2 实例之上且需要访问 AWS 资源的应用程序。如果某款应用程序运行在 Amazon EC2 实例之上且需要向 Amazon S3 存储桶或者 DynamoDB 表等 AWS 资源发出访问，则其必须具备安全凭证。利用角色而非创建单独 IAM 账户，能够帮助运行有大量实例或者使用 AWS Auto Scaling 进行自动规模伸缩的客户节约可观的操作时间。

临时性凭证包括安全令牌、访问密钥 ID 以及保密访问密钥。要为用户提供指向特定资源的访问能力，大家需要通过为其提供临时性凭证实现临时性访问。当用户向您的资源发起访问时，该用户需要提交令牌与访问密钥 ID，外加保密访问密钥所需要的签名。该令牌无法与其它访问密钥配对。根据 API 以及 AWS 产品版本的不同，用户利用令牌发起访问的具体方式也有所区别。欲了解更多信息，请参阅 AWS 上的临时性安全凭证部分。

使用临时性凭证意味着增加额外的保护能力，因为大家不必再为临时性用户管理或者分发长期凭证。另外，临时性凭证还能够自动加载至目标实例当中，意味着大家不需要以非安全方式将其嵌入至代码等位置。临时性凭证会自动轮换或者每天变更数次，无需任何人为介入，且默认以安全方式保存。

Amazon CloudWatch 安全性

Amazon CloudWatch 是一项网络服务，用于为 AWS 云资源提供监控机制，且首先以 Amazon EC2 为起点。其为客户提供对资源使用情况、运转性能以及各类总体需求模式的查看能力，具体包括 CPU 利用率、磁盘读取与写入以及网络流量等等。大家可以设置 CloudWatch 警报以确保在超过特定阈值时获得提醒，或者利用其它自动化操作解决对应问题，例如在启用 Auto Scaling 时自动添加或者移除 EC2 实例。

CloudWatch 能够面向 AWS 资源捕捉并整理各类原生使用量指标，但大家也可以将其它日志发送至 CloudWatch 加以监控。大家可以将自己的访客操作系统、应用程序以及安装在 EC2 实例上的应用程序的自定义日志文件发送至 CloudWatch，并根据需要将这部分信息进行存储。大家可以配置 CloudWatch 以监控符合给定特征的日志条目或者信息，并以 CloudWatch 指标的形式交付结果。举例来说，大家可以监控 Web 服务器日志文件中的 404 错误，用以检测故障入站链接，或者利用无效的用户消息检测未经授权的访客操作系统访问尝试。

与其它 AWS 服务一样，Amazon CloudWatch 亦要求全部指向其控制 API 的请求接受验证，从而确保不受未授权用户的访问与管理。各请求由 HMAC-SHA1 进行签名，签名由请求本身与用户的私钥共同计算得出。另外，Amazon CloudWatch 控制 API 仅接受来自 SSL 加密端点的访问。

大家可以通过在 AWS 账户下利用 AWS IAM 创建用户的方式进一步控制指向 Amazon CloudWatch 的访问活动，同时设置这些用户能够在 CloudWatch 中使用的具体操作权限。

AWS CloudHSM 安全性

AWS CloudHSM 服务为客户提供指向硬件安全模块（简称 HSM）设备的专有访问能力，这类设备用于立足反入侵且防篡改设备提供安全加密密钥存储及操作。大家可以生成、存储及管理用于进行数据加密的加密密钥，并保证其仅供您本人访问。AWS CloudHSM 服务专门用于安全存储及处理加密密钥素材，且适用于多种具体场景，包括数据库加密、数字化版权管理（简称 DRM）、公钥基础设施（简称 PKI）、验证与授权、文档签名以及交易处理等等。其支持多种最为强大的加密算法，具体包括 AES、RSA 以及 ECC 等等。

AWS CLoudHSM 服务专门用于配合 Amazon EC2 与 VPC，其负责在专有子网之内提供专有 IP。大家可以立足于 EC2 服务器通过 SSL/TLS 接入 CloudHSM，而这些连接利用双工数字化证书验证与 256 位 SSL 加密以提供安全的通信通道。

大家应当在同一服务区内选择 CloudHSM 服务以降低 EC2 实例的网络延迟，从而提升应用程序性能。大家也可以在 EC2 实例之上配置一套客户端，确保您的应用程序利用由 HSM 提供的 API，具体包括 PKCS#11、MS CAPI 与 Java JCA/JCE（即 Java 加密架构/Java 加密扩展）。

在着手使用 HSM 之前，大家必须至少在设备上设置一个分区。一个加密分区相当于一种逻辑与物理安全边界，用于限制对密钥内容的访问，这意味着只有大家自己能够对密钥以及 HSM 执行的操作进行控制。AWS 为该设备提供管理凭证，但这些凭证仅可用于管理该设备，而非设备上的 HSM 分区。AWS 利用这些凭证监控并维持该设备的正常运行及可用性。AWS 无法提取您的密钥，亦不会利用您的密钥执行任何加密操作。

HSM 设备拥有物理与逻辑篡改检测与响应机制，并会在发现篡改活动时擦除加密密钥素材并生成事件日志。HSM 的设计方案能够检测 HSM 设备是否受到物理入侵。另外，在利用 HSM 管理员凭证对 HSM 分区进行三次访问尝试且均告失败后，HSM 设备会直接擦除其 HSM 分区。

当大家的 CloudHSM 订阅到期，且确认 HSM 中的全部内容皆不需要保留，则必须删除其中的各个分区、对应内容以及日志记录。作为清退流程的一部分，AWS 能够将该设备归零，即永久抹除一切关键性信息。

移动服务

AWS 移动服务能够帮助大家更为轻松地面向移动设备构建、发布、运行、监控、优化以及规模调整各类云支持型应用程序。这些服务还能够帮助大家验证用户身份，从而控制移动应用访问、同步数据并收集与分析应用使用情况。

Amazon Cognito

Amazon Cognito 为移动与 Web 应用程序提供身份与同步服务。其能够显著简化用户身份验证任务，同时轻松实现跨越多台设备、平台以及应用的数据存储、管理及同步任务。其提供临时性受限权限凭证，允许大家无需管理任何后端基础设施即对授权及非授权用户进行管理。

Cognito 能够与多家知名服务供应商顺利对接，其中包括谷歌、Facebook 以及 Amazon，用于验证移动及 Web 应用程序的最终用户身份。大家可以充分发挥这些服务提供的身份与授权机制，而无需自行构建及维护相关系统。大家的应用程序会利用对应 SDK 对以上几项服务进行身份验证。当最终用户以这种方式完成验证后，由供应方提供的 OAuth 或者 OpenID Connect 令牌会由应用程序交付至 Cognito，再由后者为用户提供一条新的 Cognito ID 以及一组临时性受限权限 AWS 凭证。

要使用 Amazon Cognito，大家需要通过 Amazon Cognito 控制台创建一套身份池。这套身份池用于存储指向 AWS 账户的特定用户身份信息。在身份池的创建过程中，大家需要创建一个新的 IAM 角色或者为最终用户选取现有角色。IAM 角色相当于一组权限集合，用于访问特定 AWS 账户，但这些权限不会被绑定至特定单一 IAM 用户或者群组。一个授权实体（例如移动用户或者 EC2 实例）会消费一个角色并接收相关临时性安全凭证，用于访问该角色定义中指向的 AWS 资源。临时性安全凭证能够提供安全性水平，因为其生命周期较短（默认过期时长为 12 小时）且在过期之后无法恢复。大家选定的角色会对最终用户利用临时性凭证能够实际访问到的 AWS 服务造成影响。在默认情况下，Amazon Cognito 会利用受限权限创建一个新角色——最终用户只能借此访问 Cognito Sync 服务以及 Amazon Mobile Analytics。如果大家的应用需要访问其它 AWS 资源，例如 Amazon S3 或者 DynamoDB，则需要直接在 IAM 管理控制台中对当前角色进行修改。

利用 Amazon Cognito，大家不再需要为每一位访问 AWS 资源的 Web/移动应用最终用户创建独立 AWS 账户或者 IAM 账户。利用 IAM 角色，移动用户能够以安全方式访问 AWS 资源与各类应用程序功能，甚至能够将数据保存在 AWS 云当中，而无需创建账户或者进行登录。然而，如果他们选择稍后再行使用角色，则 Cognito 会将数据与身份信息加以合并。

由于 Amazno Cognito 会同时对数据进行本地与服务内存储，因此最终用户能够在离线状态下继续与其数据进行交互。其离线数据可能版本较为陈旧，但任何被添加至数据库集中的内容皆可立即在上线或者离线状态下进行检索。客户端 SDK 负责管理本地 SQLite 存储，因此应用程序能够在未联网状态下继续正常运作。SQLite 存储功能以缓存方式存在，同时亦成为全部读取与写入操作的指向目标。Cognito 的同步工具能够对数据的本地版本与云端版本进行比较，而后根据需要推送或者提取更新内容。需要注意的是，为了在不同设备之间完成数据同步，大家的身份池必须支持身份验证，否则数据同步无法顺利完成。

利用 Cognito，大家的应用程序能够直接与受支持公共身份供应方（包括 Amazon、Facebook 以及谷歌等）直接通信，从而实现用户身份验证。Amazon Cognito 并不需要接收或者存储用户凭证——而仅从身份供应方处获取 OAuth 或者 OpenID Connect 令牌。当 Cognito 接收到令牌之后，其会为用户返回一条新的 COgnito ID 以及一组临时性受限权限 AWS 凭证。

每个 Cognito 身份都仅能访问自身对应的同步数据存储，而且这部分数据在存储时会经过加密。另外，全部身份数据皆经由 HTTPS 进行传输。设备上的惟一 Amazon Cognito 标识存储在 iOS 钥匙串当中。用户数据会在设备沙箱环境下的本地 SQLite 数据库内进行缓存; 如果大家需要进一步提升安全性，则可利用应用内的加密机制对本地缓存中的身份数据进行加密。

Amazon Mobile Analytics

Amazon Mobile Analytics （即 Amazon 移动分析）是一项专门用于收集、可视化及理解移动应用使用情况数据的服务。它能够帮助大家追踪客户行为、整理指标并在移动应用中发现有意义模式。Amazon Mobile Analytics 能够对从运行对应应用的客户端设备处获取到的数据进行计算与更新，同时将结果显示在控制台当中。

Amazon Mobile Analytics 与您的应用程序加以集成，且无需应用用户利用身份供应方（例如谷歌、Facebook 或者 Amazon）进行验证。对于这部分未经验用户，Amazon Mobile Analytics 会利用 Amazon Cognito 为其提供临时性受限权限凭证。为了实现这一目标，大家首先需要在 Cognito 当中创建一套身份池。该身份池将利用 IAM 角色，后者属于一组未绑定至任何特定 IAM 用户或者群组的权限集合，允许大家利用其访问特定 AWS 资源。其会消费 IAM 角色并接收临时性安全凭证，用于接入角色中定义的对应 AWS 资源。在默认情况下，Amazon Cognito 会创建一个具备受限权限的 IAM 角色——最终用户只能借此访问 Cognito Sync 服务与 Amazon Mobile Analytics 。如果大家的应用程序需要访问其它 AWS 资源，例如 Amazon S3 或者 DynamoDB，则可直接在 IAM 管理控制台中修改您的角色。

大家可以将 AWS Mobile SDK for Android 或者 iOS 整合至您的应用程序当中，或者使用 Amazon Mobile Analytics REST API 发送来自任何联网设备或者服务的事件，同时在报告中对数据进行可视化处理。Amazon Mobile Analytics API 仅可通过受到 SSL 加密保护的端点进行接入。

应用

AWS 应用属于托管服务，可帮助大家立足于云环境为用户提供安全的集中化存储及工作区。

Amazon WorkSpaces

Amazon WorkSpaces 属于一项托管桌面服务，允许大家快速为用户配置基于云的桌面系统。只需要选择能够满足用户需求的 Windows 7 捆绑包以及需要启动的 WorkSpaces 数量即可。当 WorkSpaces 准备就绪之后，用户会收到一封电子邮件，提醒其如何下载相关客户端并登录至 WorkSpaces。他们随后能够通过多种终端设备访问自己的云桌面，具体包括 PC、笔记本以及移动设备。不过，大家的企业数据永远不会被发送或者存储至最终用户设备，这是因为 Amazon WorkSpaces 使用 PC-over-IP（即 PCoIP），其提供的是交互式视频流而非实际进行数据传输。PCoIP 协议会对用户桌面的计算资源使用体验进行压缩、加密与编码，同时仅在标准 IP 网络与最终用户设备之间发送“像素”信息。

要访问您的 WorkSpaces，用户必须利用一组惟一的凭证集合或者常规 Active Directory 凭证进行登录。当大家将 Amazon WorkSpaces 与自己的企业 Active Directory 进行整合时，每个 WorkSpaces 都会加入您的 Active Directory 域，并可与企业内的其它桌面一样接受管理。这意味着大家可以利用 Active Directory 组策略管理用户的 WorkSpaces，包括指定用于控制该桌面的配置选项。如果大家不打算使用 Active Directory 或者其它内部目录类型来管理自己的用户 WorkSpaces，则可在 Amazon WorkSpaces 当中创建一套私有云目录，并将其用于管理工作。

要提供额外的安全性保障，大家也可以要求用户利用多因素验证登录，从而以硬件或者软件令牌的形式实现登录。Amazon WorkSpaces 支持利用内部远程验证身份验证拨入用户服务（简称 RADIUS）服务器或者任何支持 RADIUS 验证机制的服务实现 MFA。其目前支持 PAP、CHAP、MS-CHAP1 以及 MS-CHAP2 协议，同时亦支持 RADIUS 代理。

每套 WorkSpaces 皆与匹配的 EC2 实例运行在同一 VPC 当中。大家可以在已经启动的 VPC 当中创建 WorkSpaces，亦可利用 WorkSpaces Quick Start 选项自动创建 WorkSpaces 服务。在使用 Quick Start 选项时，WorkSpaces 不仅会创建对应 VPC，同时亦将执行其它各项设定与配置任务，具体包括为该 VPC 配置互联网网关、在 VPC 之内设置用于存储用户及 WorkSpaces 信息的目录、创建一个目录管理员账户、创建特定用户账户并将其添加到目录当中，以及创建 WorkSpaces 实例。大家也可以经由安全 VPN 连接将 VPC 接入至内部网络，从而允许用户直接访问现有内部 Active Directory 以及其它内网资源。大家可以将在 Amazon VPC 内创建的安全组添加至全部归属于 Directory 的 WorkSpaces 当中。通过这种方式，大家能够控制一切来自 Amazon WorkSpaces 并接入 Amazon VPC 以及内部网络中其它资源的请求。

WorkSpaces 的持久性存储由 Amazon EBS 负责提供，且以每天两次的频度自动备份至 Amazon S3。如果 WorkSpaces Sync 在 WorkSpaces 当中得到启用，则用户选定的文件夹将持续备份并存储在 Amazon S3 当中。大家也可以在 PC 或者 Mac 之上利用 WorkSpaces Sync 将文档同步至 WorkSpaces，从而确保在任意桌面计算设备上访问相关数据。

由于属于托管服务，AWS 会负责承担备份及补丁安装等各类日常安全与维护任务。更新会以自动化方式每周一次交付至您的 WorkSpaces。大家可以控制用户 WorkSpaces 的具体补丁配置方式。在默认情况下，Windows Update 处于启用状态，但大家也可以对具体设置进行自定义，或者使用备选补丁管理方案。在底层操作系统方面，Windows Update 在 WorkSpaces 中默认启用，且配置为每周安装一次更新补丁。大家可以利用其它备选补丁管理方案或者配置 Windows Update 以指定补丁的具体安装周期。

大家可以利用 IAM 控制团队中的各些成员拥有管理权限，例如创建或者删除 WorkSpaces，抑或是设置用户目录。大家亦能够设置一套 WorkSpace 用于目录管理，安装您所熟悉的 Active Directory 管理工具，同时创建组织单位及组策略以简化各 WorkSpaces 用户的 Active Directory 变更应用流程。

Amazon WorkDocs

Amazon WorkDocs 是一项托管型企业存储与共享服务，且拥有反馈功能以实现用户协作。用户能够将任意类型的文件存储在 WorkDocs 文件夹当中，并允许他人进行查看与下载。特定文件类型还支持评论与注释功能，例如微软 Word 文件，且无需启动文件初始创建时所使用的相关应用。WorkDocs 会通过电子邮件向用户通常注释活动及过期时间，且可利用 WorkDocs Sync 应用对文件版本进行同步。

用户信息被存储在一个 Acitve Directory 兼容型网络目录当中。大家可以在云端创建一个新目录，或者将 Amazon WorkDocs 与您的内部目录相对接。在利用 WorkDocs 快速启动设置创建云目录时，其同时亦会创建一个目录管理员账户，并将管理员邮箱作为用户名。这时其会向您的管理员发送一封邮件，用于确认以完成注册过程。管理员随后即可利用此账户管理对应目录。

在利用 WorkDocs 快速启动设置创建云目录时，其同时亦会利用该目录创建并配置一套 VPC。如果大家需要对目录配置进行细化控制，则可选择标准设置流程，其允许大家指定您自己的目录域名，同时可利用现有 VPC 使用该目录。如果大家希望使用现有 VPC，则该 VPC 必须拥有互联网网关且至少具备两套子网。每套子网都必须位于不同的可用区内。

利用 Amazon WorkDocs 管理控制台，管理员们能够查看审计日志，从而根据时间、IP 地址以及设备追踪文件与用户活动，同时选择是否允许用户将文件共享至组织之外的使用者。在此之后，用户能够控制哪些对象能够访问其共享内容中的个别文件，或者禁用文件下载。

所有数据皆由行业标准 SSL 进行加密传输。WorkDocs Web 与移动应用及桌面同步客户端会利用 SSL 直接将文件传输至 Amazon WorkDocs。WorkDocs 用户亦能够在相关组织部署有 Radius 服务器的前提下使用多因素验证机制，简称 MFA。MFA 会使用以下因素：用户名、密码以及 Radius 服务器支持的各项方法。目前受支持的协议包括 PAP、CHAP、MS-CHAPv1 与 MS-CHAPv2。

大家需要选择各 WorkDocs 站点内文件存储所在的 AWS 区。Amazon WorkDocs 目前可用于美国东部（弗吉尼亚州）、美国西部（俄勒冈州）以及欧洲（爱尔兰）AWS 区。存储在 WorkDocs 内的全部文件、评论及注释都会自动利用 AES-256 进行加密。

附录——术语词汇表

访问密钥 ID:一条客串，由 AWS 分发以作为各 AWS 用户的惟一身份标识; 这是一条与保密访问密钥相关联的字母加数字令牌。

访问控制列表(简称 ACL): 一份权限或者规则列表，用于访问某一对象或者网络资源。在 Amazon EC2 当中，安全组作为实例层级的 ACL 发挥作用，负责控制哪些用户拥有访问特定实例的权限。在 Amazon S3 当中，大家可以利用 ACL 为用户组分配指向特定存储桶或者对象的读取或写入操作权限。在 Amazon VPC 当中，ACL 作为网络防火墙起效，负责在子网层级进行访问控制。

AMI: 一套 Amazon Machine Image（即 Amazon 机器镜像，简称 AMI）属于一套存储在 Amazon S3 当中的加密机器镜像，其中包含客户软件实例引导所必需的全部信息。

API: 应用程序编程接口（简称 API）是一种计算机科学概念中的接口机制，用于定义应用程序能够以请求方式调用库以及/或者操作系统中的哪些服务。

归档: Amazon Glacier 中的一份归档代表一个需要存储的文件，亦属于 Amazon Glacier 的基本存储单位。其可容纳任意数据类型，包括图片、视频或者文档。每份归档都拥有惟一 ID 外加一条可选描述。

验证: 验证代表的是判断某人或者某物的声明身份与实际身份是否相符的流程。除了用户需要接受验证之外，每款需要利用 AWS API 进行功能调用的程序也同样需要进行验证。AWS 要求大家利用由加密散列功能生成的数字化签名对每一条请求进行验证。

Auto Scaling: 一项 AWS 服务，允许客户以自动化方式根据预先定义的条件对 Amazon EC2 容量进行规模伸缩。

可用区: Amazon EC2 的位置由服务区与可用区共同构成。可用区作为独立位置，在设计上用于隔绝各可用区间的故障影响并提供低成本、低延迟网络连接，因此能够实现同一服务区内各可用区间的顺畅对接。

壁垒主机: 一台在配置上专门用于抵御攻击影响的计算机，通常位于非军事区（简称 DMZ）外部/公共区域或者防火墙之外。大家可以通过将一套公共子网设置为 Amazon VPC 组成部分，从而将 Amazon EC2 实例设置为 SSH 壁垒。

存储桶: Amazon S3 当中的对象存储容器。每个对象皆被承载于存储桶当中。举例来说，如果某个名为 photo/puppy.jpg 的对象被存储在 johnsmith 存储桶当中，那么其即可利用以下 URL 进行寻址：http://johnsmith.s3.amazonaws.com/photos/puppy.jpg。

证书: 证书为 AWS 产品用于验证 AWS 账户及用户的依据。亦被称为 X.509 证书。该证书需要与一条私钥进行匹配。**CIDR 块**: IP 地址的无类别域间路由块。

客户端加密: 在将数据上传至 Amazon S3 之前，立足于客户端对其进行加密。

CloudFormation: 一款 AWS 配置工具，允许客户记录运行应用程序所必需的 AWS 资源基准配置信息，从而以按序且可预测方式完成配置与更新工作。

Cognito: 一项 AWS 服务，用于简化用户身份验证以及数据在各设备、平台与应用程序之间存储、管理与同步的流程。其可与多家现有身份供应方对接，同时亦支持未验证访客用户机制。

凭证: 用户或者进程必须具备的条目，用于在其访问 AWS 目标服务时对其身份进行验证。AWS 凭证当中包含密码、保密访问密钥、X.509 证书以及多因素令牌。

专用实例: 指在主机硬件层面进行物理隔离的 Amazon EC2 实例（即始终运行在单租户硬件之上）。

数字签名: 数字签名代表一种加密方法，用于证明数字信息或者文档的验证结果。一条有效的数字签名代表对应信息由认证发送者创建，且在传输过程中未受篡改。数字签名允许客户对指向 AWS API 的请求进行签名，并将其作为验证流程的组成部分。

Direct Connect 服务: 一项 Amazon 服务，允许大家在内部网络与 AWS 服务区之间利用一条高通量专用连接建立直连关系。利用此专用连接，大家随后可直接面向 AWS 云（例如指向 Amazon EC2 以及 Amazon S3）与 Amazon VPC 创建逻辑连接，从而在网络路径中绕过互联网服务供应商。

DynamoDB Service: 一项由 AWS 提供的托管型 NoSQL 数据库服务，用于提供高速可预测性能及无缝化规模扩展能力。

EBS: Amazon Elastic Block Store（即 Amazon 弹性块存储，简称 EBS）提供块级存储分卷，以供各 Amazon EC2 实例使用。Amazon EBS 分卷为实例关联型存储，其持久性取决于对应实例的具体生命周期。

ElastiCache: 一项 AWS Web 服务，允许大家在云环境下设置、管理及规模调整各分布式内存内缓存环境。此项服务允许大家立足于速度更快的托管内存内缓存系统进行信息检索，而非依靠速度更慢的磁盘数据库，旨在显著提升 Web 应用程序性能水平。

Elastic Beanstalk: 一款 AWS 部署与管理工具，能够以自动化方式实现容量配置、负载均衡以及客户应用规模自动伸缩等功能。

弹性 IP 地址: 一条静态公共 IP 地址，大家可以将其分配给 Amazon VPC 之内的任一实例，从而实现实例公开。弹性 IP 地址亦能帮助大家将自己的公共 IP 地址快速映射至 VPC 中的任意实例，从而实现实例故障转移。

Elastic Load Balancing（弹性负载均衡）: 一项 AWS 服务，用于管理 Amazon EC2 实例群组上的相关流量，负责将全部流量引导至单一服务区内各可用区中的全部实例处。弹性负载均衡拥有内部负载均衡器的全部固有优势，同时亦提供多种安全性提升，例如对提取自 EC2 实例的工作内容进行加密/解密，并在负载均衡器上对其加以集中管理。

Elastic MapReduce (简称 EMR)服务: 一项 AWS 服务立足于 Amazon EC2 与 Amazon S3 构建起的网络规模基础设施运行托管 Hadoop 框架。Elastic MapReduce 允许客户以轻松易行且极具成本效益的方式处理超大规模数据（即‘大数据’）。

Elastic Network Interface（即弹性网络接口）: 在 Amazon VPC 当中，弹性网络接口属于次级可选网络接口，大家可以利用其接入 EC2 实例。弹性网络接口可用于创建管理网络，或者利用 Amazon VPC 内的网络或安全设备。其能够由实例所轻松识别，并随时重新附加至其它实例。

端点: 作为 AWS 服务入口点的一条 URL。为了降低应用程序的数据延迟，大多数 AWS 服务允许大家选择区域内端点以执行请求。部分 Web 服务还允许大家使用不隶属于特定服务区的通用型端点; 这些通用端点解析至服务的 us-east-1 端点。大家可以通过 HTTP 或者配合 SSL 的安全 HTTP（HTTPS）接入 AWS 端点。

联合用户: 当前尚未被验证且访问 AWS 服务的用户、系统或者应用程序，大家需要为其分配临时性访问权限。此类访问由 AWS 安全令牌服务（简称 STS）API 负责实现。

防火墙: 一类硬件或者软件组件，用于根据特定规则集合对输入及/或输出网络流量进行控制。要在 Amazon EC2 中使用防火墙规则，大家需要指定接入实例所必需的协议、端口及源 IP 地址范围。这些规则将指定哪些输入网络流量应被交付至您的实例（例如在端口 80 上接收网络流量）。Amazon VPC 支持一套完整的防火墙解决方案，可面向单一实例对入站及出站流量进行过滤。默认组策略允许同一组内其它成员的入站通信请求，同时允许一切指向任意外部目的地的出站通信。网络流量可根据 IP 协议、服务端口以及源/目的地 IP 地址（单一 IP 或者无类别域间路由（简称 CIDR）块）进行限定。

访客操作系统: 在虚拟机环境下，多套操作系统可能运行在同一硬件之上。其中每个实例皆可作为主机硬件上的一个访客，且拥有自己的操作系统。

哈希: 一项加密散列功能，用于为指向 AWS API 的请求进行数字签名计算。一条加密哈希属于一项单向功能，其根据输入结果返回惟一的哈希值。指向哈希功能的输入内容类型包括所请求内容文本以及保密访问密钥。哈希功能随后会返回一条包含请求内容的哈希值作为签名。

HMAC-SHA1/HMAC-SHA256: 在密码学概念当中，密钥控制型散列消息认证代码（简称 HMAC 或者 KHMAC）是一类消息验证代码（简称 MAC）类别，利用包含加密哈希功能配合保密密钥的特定算法计算得出。配合 MAC，其可用于对数据的完整性以及消息身份进行验证。任何一种迭代式加密哈希功能，例如 SHA-1 或者 SHA-256，皆可用于 HMAC 的计算; MAC 算法得出的计算取决于具体使用 HMAC-SHA1 或者 HMAC-SHA256。HMAC 的加密强度则取决于底层哈希功能的加密强度，具体体现为密钥大小、质量以及输出散列的实际长度。

硬件安全模块(简称 HSM): HSM 属于一套负责在反入侵硬件设备内提供安全加密密钥存储与操作功能的方案。HSM 的设计目标 在于以安全方式存储加密密钥素材并使用这些密钥素材，且不会将其暴露在加密边界之外。AWS CloudHSM 服务为客户提供指向 HSM 设备的专有、单租户访问能力。

虚拟机管理程序: 虚拟机管理程序（hypervisor），亦被称为虚拟机监控器（简称 VMM），属于一套软件/硬件平台虚拟化软件，允许多套操作系统并行运行在单一主机计算机之上。

身份与访问管理(简称 IAM): AWS IAM 允许大家为自有 AWS 账户内的每位用户创建多个用户与对应管理权限。

身份池: Amazon Cognito 中的用户身份信息存储体系，专门指向特定 AWS 账户。身份池使用 IAM 角色，后者包含未绑定至特定 IAM 用户或者群组的权限，负责根据角色定义提供指向 AWS 资源的临时性安全验证凭证。

身份供应方: 一项在线服务，负责为需要与 AWS 服务或者其它业务服务进行交互的用户提供身价信息。目前的知名身份供应方包括 Facebook、谷歌以及 Amazon。

Import/Export 服务: 一项 AWS 服务，用于以物理方式发送便携式存储设备以实现指向 Amazon S3 或者 EBS 存储体系的大规模数据传输。

实例：一个实例相当于一套虚拟服务器，同时亦可被称为虚拟机，其拥有自己的硬件资源与访客操作系统。在 EC2 中，一个实例代表的是运行中的一套 Amazon Machine Image（即 Amazon 机器镜像，简称 AMI）副本。

IP 地址: 一条互联网协议（简称 IP）地址属于一份数字型标签，其利用互联网协议分配至计算机网络中的具体设备，旨在实现各节点间的相互通信。

IP 欺诈: 利用伪造的源 IP 地址（即欺诈）创建 IP 数据包，旨在隐瞒发件人真实身份或者伪造计算系统身份。

密钥: 在密码学概念中，一条密钥代表的是一种加密算法（亦被称为散列算法）的计算结果。密钥对为一组安全凭证，大家可利用其验证电子身份，其由一条公钥与一条私钥组成。

密钥轮换: 对当前使用的加密数据或者数字签名进行定期自动变更的流程。与密码变更一样，密钥轮换能够在攻击者已经获得了密钥或者相关值的情况下，最大程度降低由此带来的损失。AWS 支持多条并发访问密钥与证书，允许客户按照预定周期进行密钥与证书轮换，且不会给应用程序造成任何停机时间。

Mobile Analytics: 一项 AWS 服务，用于对移动应用的使用情况数据进行收集、可视化处理与理解。其能够帮助大家追踪客户行为、整理指标并识别存在于移动应用程序当中的有意义模式。

多因素验证(简称 MFA): 利用两种或者更多验证因素进行身份验证。验证因素包括大家自身知晓（例如密码内容）或者实际掌握（例如生成的随机数字令牌）的信息。AWS IAM 允许大家在用户名与密码凭证之外，使用六位数字一次性编码进行身份验证。客户可通过物理或者虚拟设备获取这类一次性编码（例如物理令牌设备或者智能手机上的虚拟令牌应用）。

网络 ACL: 无状态流量过滤器，适用于 Amazon VPC 之内单一子网的全部入站或者出站流量。网络 ACL 可包含有序规则，用于根据 IP 协议、服务端口以及源/目的地 IP 地址进行流量放行或者拒绝。

对象: Amazon S3 当中的基本存储单位。对象当中包含对象数据与元数据。数据部分无法为 Amazon S3 所查看，而元数据则属于一组名称-值对，用于描述该对象。默认元数据中包含数据的上一次修改时间，外加内容类型等 HTTP 元数据。开发人员也可以在存储各对象时为其指定自定义元数据。

半虚拟化: 在计算学科当中，半虚拟化是一种虚拟化技术，代表将软件接入至虚拟机——其将虚拟机作为类似于但却不完全等同于底层硬件的运行基础。

对等: VPN 对等连接属于一种存在于两套 VPC 之间的网络连接，允许大家在二者之间利用专有 IP 地址进行流量路由。任一 VPC 中的实例皆能够与另一存在于同一网络内的实例进行通信。

端口扫描: 端口扫描属于一组消息序列，其发送方希望借此了解目标计算机内运行的网络服务，具体包括该计算机提供的“公开”端口编号。

服务区: 代表同一地理区域内的全部 AWS 资源集合。每个服务区由至少两个可用区构成。

副本: 来自数据库的持续数据副本结果，旨在保有该数据库的第二套版本，通常用于实现灾难恢复。客户可以利用多可用区实现其 Amazon RDS 数据库的副本保存，或者在使用 MySQL 的情况下选择读取副本（Read Replicas）服务。

关系型数据库服务(简称 RDS): 一项 AWS 服务，允许大家创建一个关系型数据库（简称 DB）实例并根据应用程序需求灵活调整其计算资源与存储容量规模。Amazon RDS 可用于 Amazon Aurora、MySQL、PostgreSQL、甲骨文、微软 SQL Server 以及 MariaDB 等数据库引擎。

角色: AWS IAM 中的一项实体，其拥有一组权限集合并可由其它实体进行消费。运行在 Amazon EC2 实例上的应用程序可利用角色实现对 AWS 资源的安全访问。大家可以为角色分配具体权限条目，利用该角色启动 Amazon EC2 实例，而后由 EC2 对运行在其上的应用程序自动进行 AWS 凭证管理。

Route 53: 一套权威 DNS 系统，负责为开发人员提供更新机制，用于管理自身公共 DNS 名称、回应 DNS 查询并将域名翻译为计算机可用于彼此通信的 IP 地址。

保密访问密钥: 大家在登录至 AWS 账户时，由 AWS 分配的一条密钥。要实现 API 调用或者使用命令行界面，每位 AWS 用户都需要保密访问密钥及访问密钥 ID。该用户需要利用保密访问密钥签名每条请求，同时在请求中包含访问密钥 ID。为了确保 AWS 账户的安全性，保密访问密钥仅可在创建过程中进行内容访问。大家必须保存此密钥（例如以文本文件形式进行安全存储），从而实现再次访问。

安全组: 一个安全组能够为大家提供对协议、端口及源 IP 地址范围的控制能力，并立足于此限制能够接入 Amazon EC2 实例的具体对象; 换句话来说，其为我们的实例进行防火墙定义。这些规则将指定哪些输入网络流量可被交付至您的实例（例如只接受端口 80 上的网络流量）。

安全令牌服务(简称 STS): AWS STS API 会返回临时性安全凭证，其中包含一条安全令牌、一个访问密钥 ID 以及一条保密访问密钥。大家可以利用 STS 为需要临时访问资源的用户分发安全凭证。这些用户可为前 IAM 用户、非 AWS 用户（即联合身份）、系统或者其它需要访问 AWS 资源的应用程序。

服务器端加密(简称 SSE): Amazon S3 存储中的一个选项，用于自动对闲置数据进行加密。利用 Amazon S3 SSE，客户能够通过在写入对象时添加额外的请求头以实现上传数据加密。解密会在数据接受检索时自动执行。

服务：经由网络提供的软件或者计算能力（例如 Amazon EC2 与 Amazon S3）。

片段: 在 Amazon Kinesis 当中，一个片段代表的是 Amazon Kinesis 流中的一组惟一数据记录。Kinesis 流由多个片段构成，每个片段都具备固定的容量单位。

签名: 即数字签名，属于确认数字消息验证情况的基本方式。AWS 使用的签名由一项加密算法与大家的私钥共同计算得出，用于验证指向至 Web 服务的请求。

简单数据存储库(简称 Simple DB): 一套非关系型数据存储系统，允许 AWS 客户通过 Web 服务请求实现数据条目的存储与查询。Amazon SImpleDB 能够创建并管理分布于多个地理位置的、以自动化方式生成的分布式客户数据副本，旨在实现高可用性与数据持久性。

简称邮件服务(简称 SES): 一项 AWS 服务，用于为企业及开发人员提供可扩展的批量与事务型邮件发送服务。为了最大程度提升发送内容的交付能力与可靠性，Amazon SES 会采取积极举措以预防发送异常内容，从而确保互联网服务供应商始终将 SES 服务视为可信邮件来源。

简单邮件传输协议(简称 SMTP): 一项互联网标准，用于跨越 IP 网络实现邮件传输。Amazon 简单邮件服务使用 SMTP，使用 Amazon SES 的客户亦可利用 SMTP 接口进行邮件发送，但必须通过 TLS 进行 SMTP 端点接入。

简单通知服务(简称 SNS): 一项 AWS 服务，旨在简化云环境下通知内容的设置、操作与发送。Amazon SNS 为开发人员提供由应用程序发布消息，并立即将其交付至订阅者或者其它应用的能力。

简单队列服务(简称 SQS): 一项由 AWS 提供的可扩展消息队列服务，能够以在同一应用的各分布式组件之间实现基于消息的异步式通信。各组件可为计算机设备、Amazon EC2 实例或者二者兼而有之。

简单存储服务(简称 Amazon S3): 一项 AWS 服务，能够为各对象文件提供安全存储支持。指向对象的访问操作可在文件或者存储桶层级进行控制，并进一步通过 IP 源、请求时间等具体条件加以限定。各文件还能够自动利用 AES-256 加密机制进行加密。

简单工作流服务(简称 SWF): 一项 AWS 服务，允许客户构建起能够协调分布式组件间工作流程的应用程序。利用 Amazon SWF，开发人员能够将单一应用程序中的各处理步骤设置为“任务 ”，从而驱动分布式应用的顺利运作。Amazon SWF 能够协议各相关任务、管理任务执行依赖性、实现调度并根据开发人员的应用逻辑进行并发运行。

单点登录: 一次登录即可访问多种应用程序及系统的功能。安全的单点登录功能可通过创建 URL 的方式为联合用户（包括 AWS 与非 AWS 用户）提供指向 AWS 管理控制台的临时性安全凭证。

快照: 一套面向客户的 EBS 分卷快照，可存储在 Amazon S3 当中; 亦可表现为一套面向客户的 RDS 数据库备份，存储于 Amazon RDS 当中。快照可用作新 EBS 分卷或者 Amazon RDS 数据库的起始点，亦可实现长期持久性与恢复能力以支持数据保护效果。

安全嵌套层(简称 SSL): 一项加密协议，用于经由互联网的应用层提供安全性保障。TLS 1.0 与 SSL 30 协议规范皆利用加密机制以建立安全 TCP/IP 连接的建立与维护。此安全连接可预防劫持、篡改或者消息伪造。大家可以通过 HTTP 或者配合 SSL 的安全 HTTP（HTTPS）接入 AWS 端点。

有状态防火墙: 在计算学科中，有状态防火墙（任何可执行有状态数据检测（简称 SPI）或者有状态检查的防火墙）是一套能够持续追踪网络连接状态（例如 TCP 数据流以及 UDP 通信）的防火墙。

Storage Gateway: 一项 AWS 服务，能够以安全方式利用在主机之上部署虚拟机，允许客户在其中运行 VMware ESXi 虚拟机管理程序，从而实现客户内部软件与 Amazon S3 存储间的对接。数据会以异步方式由客户内部存储硬件经由 SSL 传输至 AWS，而后再利用 AES-256 以加密方式存储在 Amazon S3 当中。

临时性安全凭证: AWS 负责提供临时性 AWS 服务接入权限的 AWS 凭证。临时性安全凭证可用于在自有身份与验证系统当中，在 AWS 服务与非 AWS 用户间建立身份联合。临时性安全凭证包含安全令牌、一条访问密钥 ID 以及一条保密访问密钥。

Transcoder: 一套转码（转换）系统，用于将媒体文件（包括音频与视频）从一种格式、大小或者质量转换为另一种。Amazon Elastic Transcoder 能够帮助客户轻松将视频文件转化为更具扩展性及成本效益的形式。

传输安全层(简称 TLS): 一项加密协议，用于经由互联网的应用层实现安全保护。使用 Amazon 简单邮件服务的客户必须经由 TLS 方可接入 SMTP 端点。

树状哈希: 一套树状哈希由以 1 MB 数据片段为基本单位计算得出哈希值组成。这些哈希值随后会以树状形式组成起来，用于表现数据间的具体相邻关系。Amazon Glacier 会面向此数据进行哈希检查，旨在确保内容未经过篡改或者路由。

存储库: 在 Amazon Glacier 当中，一套存储库代表的是用于存储各份归档的容器。当大家创建起一套存储库时，需要指定一条名称并选择创建该存储库的具体 AWS 服务区。每套存储库拥有一条惟一地址。

版本控制: Amazon S3 当中的每个对象皆拥有一条密钥与一个版本 ID。各对象可拥有同样的密钥，但配合不同的版本 ID 存储在同一存储桶当中。版本控制机制可利用 PUT Bucket 版本控制在存储桶层中启用。

虚拟实例: 当 AMI 启动完成后，由此运行的系统将被引用为一个实例。基于同一 AMI 的全部实例皆使用同样的信息，且各实例在终止或者发生故障后，信息将同时消失。

虚拟 MFA: 用户可利用自己的智能手机（而非实体令牌）获取一条六位数字 MFA 编码。MFA 可用于在用户名及密码之外，提供额外因素（一次性编码）实现身价验证。

虚拟专有云(简称 VPC): 一项 AWS 服务，允许客户在 AWS 云中配置一套隔离型分区，具体包括选择自己的 IP 地址范围、定义子网同时配置路由表及网络网关。

虚拟专有网络(简称 VPN): 能够在两个位置之间利用互联网等公共网络创建一条专有的安全网络连接。AWS 客户能够在其 Amazon VPC 与自有数据中心之间添加一条 IP 安全 VPN 连接，从而有效实现数据中心面向云端的延伸，同时允许公共子网实例经由互联网直接接入其 Amazon VPC。在这类配置情况下，客户可以在其企业数据中心侧添加一台 VPN 设备。

WorkSpaces: 一项 AWS 托管桌面服务，允许大家为用户配置基于云的桌面环境，并允许他们利用惟一凭证集合或者自有 Active Directory 凭证进行登录。

X.509: 在密码学概念中，X.509 是一项公钥基础设施（简称 PKI）标准，用于实现单点登录与权限管理基础设施（简称 PMI）。X.509 指定了公钥凭证、证书轮换列表、属性凭证以及证书路径验证算法的标准格式。部分 AWS 产品在特定接口上利用 X.509 证书取代了保密访问密钥机制。举例来说，Amazon EC2 在其查询接口上使用保密访问密钥，但在 SOAP 接口及命令行工具接口上则使用签名证书机制。

WorkDocs: 一项 AWS 托管型企业存储与共享服务，亦提供反馈功能以实现用户协作。

文档修订

2016 年 6 月

- 更新合规性计划
- 更新服务区

2014 年 11 月

- 更新合规性计划
- 更新共享安全责任模式
- 更新 AWS 账户安全功能
- 对服务归类进行重新调整
- 对以下服务进行了功能更新: CloudWatch, CloudTrail, CloudFront, EBS, ElastiCache, Redshift, Route 53, S3, Trusted Advisor 以及 WorkSpaces
- 添加 Cognito 安全性
- 添加 Mobile Analytics 安全性
- 添加 WorkDocs 安全性

2013 年 11 月

- 更新服务区
- 对以下服务进行了功能更新: CloudFront, DirectConnect, DynamoDB, EBS, ELB, EMR, Amazon Glacier, IAM, OpsWorks, RDS, Redshift, Route 53, Storage Gateway 以及 VPC
- 添加 AppStream 安全性
- 添加 CloudTrail 安全性
- 添加 Kinesis 安全性
- 添加 WorkSpaces 安全性

2013 年 5 月

- 更新 IAM，纳入角色与 API 访问
- 更新 MFA，包含指向客户特定权限操作的 API 访问机制
- 更新 RDS，添加事件通知、多可用区以及 SSL 接入 SQL Server 2012
- 更新 VPC，添加多 IP 地址、静态路由 VPN 以及默认 VPC
- 对以下服务进行了新功能更新: CloudFront, CloudWatch, EBS, ElastiCache, Elastic Beanstalk, Route 53, S3, Storage Gateway

- 添加 Glacier 安全性
- 添加 Redshift 安全性
- 添加 Data Pipeline 安全性
- 添加 Transcoder 安全性

☐ 添加 Trusted Advisor 安全性

☐ 添加 OpsWorks 安全性

☐ 添加 CloudHSM 安全性