AWS 安全性介绍

2015 年 7 月

目录

简介

Amazon Web Services (简称 AWS) 提供一套具备可扩展性的云计算平台，其可用性极为出色，能够提供运行各类应用程序所必需的工具方案。其能够帮助您系统与数据的保密性、完整性与可用性，并借此增强您的信任与信心。本份文件旨在提供一份与 AWS 安全性方案相关的指南资料，其中涵盖 AWS 环境控制机制以及部分产品与功能，AWS 希望利用它们帮助客户充分满足安全性保障目标。

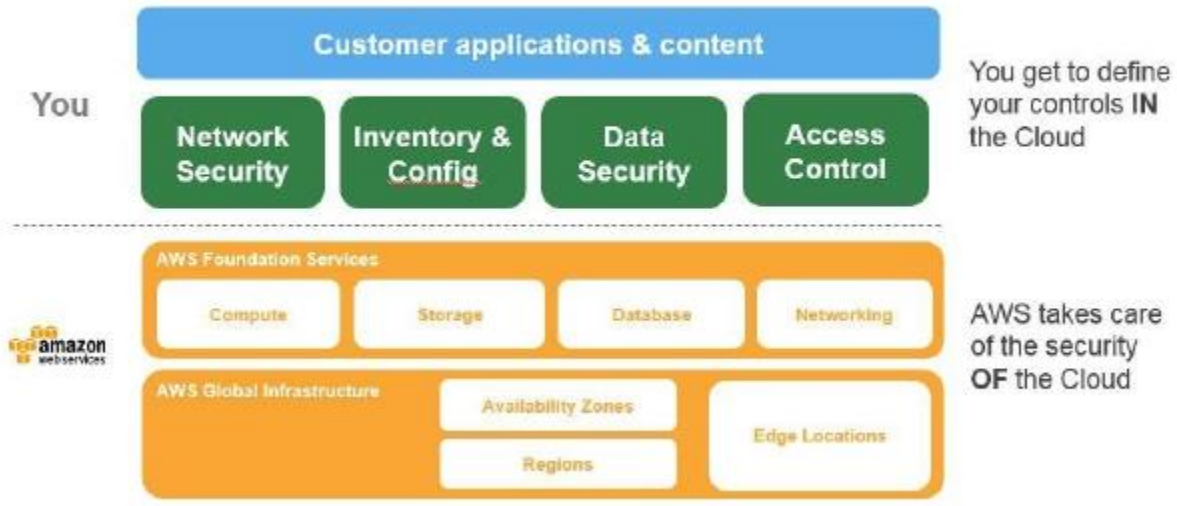
AWS 基础设施的安全性

AWS 基础设施在架构层面堪称当下最为灵活且安全性水平最高的云计算环境。其设计方案能够提供一套具备终极可扩展能力、超高可靠性的平台，帮助客户快速且安全地部署各类应用程序与数据。

这套基础设施在构建与管理当中不仅遵循各项最佳安全实践与标准，同时亦考虑到云环境下的各种特殊需求。AWS 采用冗余与分层控制、持续验证与测试以及一系列自动化机制，旨在确保底层基础设施受到 24 x 7 全天候监控与保护。AWS 亦确保这些控制机制能够复制至全部新建数据中心或者服务当中。

全部 AWS 客户皆能够享受到其数据中心与网络架构带来的优势，从而满足各类最为严苛的安全需求。这意味着您将拥有一套弹性基础设施，在设计中充分纳入高安全性要素，且不存在传统数据中心内所常见的高昂资本支出与运营开销。

AWS 采用一套安全责任分担模型，其中 AWS 负责底层云基础设施的安全保障工作，而身为客户的您则负责保护您部署在 AWS 中的工作负载安全（详见图一）。这种作法能够帮助大家在 AWS 环境当中获得实现业务功能安全控制所必需的灵活性与敏捷性。您可以严格限制指向敏感数据环境的访问活动，亦可在需要公开的一般信息层面使用较为宽松的访问控制手段。



图一：AWS 安全责任分担模型

安全产品与功能

AWS 及其合作伙伴提供一系列工具与功能选项，旨在帮助大家满足自己的具体安全目标。这些工具能够为大家提供与内部环境相对应的控制能力。AWS 还提供多种特定安全工具与功能，其涵盖范围包括网络安全、配置管理、访问控制以及

数据安全。另外，AWS 亦提供多种监控与日志记录工具，负责帮助大家确切把握环境之内发生的一切活动。

网络安全性

AWS 提供多项安全功能与服务，旨在提升隐私保护水平并控制网络访问活动。其中具体包括：

- 内置防火墙允许大家立足 AWS 之内创建专有网络，同时控制一切指向您实例与子网的网络访问。
- 利用 TLS 对全部服务间的数据传输进行加密。
- 多种网络连接选项可为来自您所在办公环境或者内部环境的连接提供专有或者专用通道。
- DDoS 攻击防护技术作为自动规模伸缩或者内容交付策略中的组成部分。

库存与配置管理

AWS 提供一系列工具，允许大家在快速实现业务迁移的同时，确保自身云资源符合企业内实施的标准与最佳实践。其中具体包括：

- 各类根据企业标准管理 AWS 资源创建与释放的部署工具。
- 库存与配置管理工具，用于识别 AWS 资源而后随时间推移追踪并管理与这部分资源相关的变更。
- 模板定义与管理工具用于创建标准化、预配置且强大的 EC2 实例虚拟机。

数据加密

AWS 允许大家为云环境中的闲置数据添加安全层，负责提供可扩展且高效的加密功能。其中具体包括：

- 可用于各 AWS 存储与数据库服务的数据加密功能，具体包括 EBS、S3、Glacier、Oracle RDS、SQL Server RDS 以及 Redshift 等等。
- 灵活的密钥管理选项，允许大家选择由 AWS 管理加密密钥，抑或是始终由您自己亲自加以控制。
- 客户可选择各类专用型、基于硬件的加密密钥，从而满足各类合规性要求。

除此之外，AWS 还为客户提供多种 API，用于将加密与数据保护机制同您开发或部署在 AWS 环境下的各类服务加以整合。

访问控制

AWS 为大家提供对各 AWS 服务内用户访问策略进行定义、执行与管理的能力。其中具体包括：

- 身份与访问管理功能，负责立足于各类 AWS 资源对个别用户账户及权限进行定义。

- 多因素验证，用于为账户分配权限，其中包括基于硬件的验证工具选项。
- 同企业目录集成与合并，旨在降低管理开销并提升最终用户体验。

AWS 为其大多数服务提供原生身份与访问管理机制，同时允许客户将 API 集成至您的任意应用程序或者服务当中。

监控与日志记录

AWS 提供多款工具与功能，帮助客户对 AWS 环境下的状况进行监控，其中具体包括：

- 对 API 调用的深层查看能力，包括由谁在何时调用了哪些 API，对应 API 又执行了何种操作。
- 日志聚合与多种功能选项，用于简化调查及合规性报告工作。
- 警报通知，在发生特定事件或者超过阈值时发出提醒。

这些工具与功能将帮助大家抢先了解重点问题，从而在其对业务造成影响之前加以解决，最终提升安全性水平并解决环境中的潜在风险。

AWS Marketplace

AWS Marketplace 负责提供数百款行业领先合作伙伴打造的产品，其可提供等同于现有内部环境控制手段的功能，或者将内部控制机制与云环境相结合。其中具体包括反恶意软件、Web 应用防火墙以及入侵防护等方案。

这些产品是对 AWS 工具与功能的一种强大补充，将帮助大家部署一套更为全面的安全架构，同时以高度无缝化方式跨越云环境与内部环境。

安全指南

AWS 为客户提供多种指南与专业知识资料，具体载体包括在线工具、资源、技术支持以及由 AWS 及合作伙伴提供的专业服务等。

AWS Trusted Advisor 是一款在线工具，其像是一位定制化云技术专家，能够帮助大家遵循最佳实践完成资源配置工作。Trusted Advisor 能够检查您的 AWS 环境，帮助消除安全漏洞并发现种种能够节约资金、提升系统性能及改善可靠性的潜在机遇。

AWS Account Teams 提供第一接触点，负责引导大家完成整个部署与实施流程，同时为您指明如何利用正确的资源处理对应的安全问题。

AWS Enterprise Support 承诺在 15 分钟内做出响应，且以 24 x 7 全天候方式接受电话、即时通讯或者邮件咨询; 另外，其还提供专门的技术客户经理为您服务。其能够确保客户的问题在尽可能短的时间内得到妥善处理。

AWS Professional Services 与 AWS Partner Network 都能够帮助客户根据经过确切验证的设计方案建立自己的安全策略与规程，同时有助于确保客户的安全设计真正满足内部与外部合规性要求。AWS Partner Network 当中包含来自全球范围的数百家认证 AWS 咨询合作伙伴，能够帮助客户解决各类安全与合规需求。

AWS 建议与公告。AWS 针对现有安全漏洞与威胁提供建议，并允许客户同 AWS 安全专家协作以应对种种安全问题，具体包括报告滥用、安全漏洞以及渗透测试等等。

合规性

AWS 计算环境接受持续审计，且得到全球各地区及行业认证机构的许可，具体包括 ISO 27001、FedRAMP、DoD CSM 以及 PCI DSS[1] 等。另外，AWS 还提供相关模板与控制映射方案，旨在帮助客户面向 20 多项标准对自己当前运行在 AWS 之上的环境进行合规性评估，其中包括 HIPAA、CESG（英国）以及新加坡多层云安全（简称 MTCS）标准等等。

AWS 亦完全遵循欧盟数据保护法规，且 AWS 数据处理协议亦结合其中第 29 条工作小组示范条款。这意味着 AWS 客户可根据需要将个人数据由欧盟经济区（简称 EEA）转移至其它国家，且其内容将始终受到与欧盟经济区同等水平的安全保护。

通过在认证环境中运营自身业务，客户能够显著降低审计工作的设计与实施成本。AWS 会持续评估自身底层基础设施——包括硬件乃至数据中心的物理与环境安全因素——从而确保客户充分享受到此类认证所带来的安全保障成效。

在传统数据中心之内，大部分常见合规举措需要以手动方式定期执行。这些举措包括验证资产配置与报告管理活动。另外，大部分结果报告可能在整理完成之前就已经过时。相比之下，将业务运行在 AWS 环境当中则允许客户利用 AWS Config 与 AWS CLoudTrail 提供的内置自动化工具顺利完成合规性验证任务。这些工具能够显著降低审计工作执行成本，因为此类任务将成为常规性持续性自动化流程的组成部分。相较于人为执行，其时间耗费将大幅缩短，同时亦将带来更出色的风险应对能力与安全性水平。

如何获取更多信息？

AWS 提供多份白皮书，其中囊括 AWS 环境下的各具体安全方案描述与量化标准。

欲了解更多与 AWS 安全性实践与产品功能相关的细节信息，请前往 http://d0.awsstatic.com/whitepapers/Security/AWS Security Whitepaper.pdf 下载 AWS 安全流程概述文件。

欲了解更多与 AWS 内特定控制机制及其如何同现有控制框架相结合的细节信息，请前往 https://media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf 下载 AWS 风险与合规性白皮书。

欲了解更多与 AWS 环境下如何部署安全控制机制的最佳实践指南信息，请前往 http://media.amazonwebservices.com/AWS_Security_Best_Practices.pdf 下载 AWS 安全最佳实践文档。

[1] 欲了解更多与 AWS 合规性计划相关的细节信息，请访问 http://aws.amazon.com/compliance