AWS 安全简介

2020 年 1 月

通知

客户有责任对本文档中的信息进行单独评估。本文档：(a) 仅供参考；(b) 代表当前提供的 AWS 产品和实践，如有更改，恕不另行通知；并且 (c) AWS 及其附属机构、供应商或许可方不做任何承诺或保证。AWS 产品或服务“按原样”提供，不提供任何形式的保证、陈述或条件，无论是明示还是暗示。AWS 对其客户的责任和义务受 AWS 协议管控，本文档不是 AWS 与其客户之间的任何协议的一部分，也不会对其进行修改。

目录

摘要

Amazon Web Services (AWS) 推出了一个具有高可用性和高可靠性的可扩展云计算平台，为您提供运行各种应用程序所需的工具。帮助保护您系统和数据的机密性、完整性和可用性对 AWS 而言至关重要，同时这也有助于维系您对 AWS 的信任和信心。本文档旨在介绍 AWS 的安全方法，包括 AWS 环境中的控制措施，以及 AWS 为客户提供以实现您的安全目标的一些产品和功能。

AWS 基础设施的安全性

AWS 基础设施旨在成为当今市场上最灵活、最安全的云计算环境之一。它旨在提供一个可扩展性极强、高度可靠的平台，从而让客户能够快速安全地部署应用程序和数据。

此基础设施的构建和管理不仅要遵循安全最佳实践和标准，而且要考虑到云的独特需求。AWS 使用冗余和分层控制、持续验证和测试以及大量自动化，以确保全天候监控和保护底层基础设施。AWS 确保在每个新数据中心或服务中都有相同的控制措施。

所有 AWS 客户都会从旨在满足大多数安全敏感型客户要求的数据中心和网络架构中受益。这意味着您可以获得一个弹性基础设施，专为高安全性而设计，而无需传统数据中心的资本支出和运营开销。

AWS 采用共享安全责任模型运营，其中 AWS 负责底层云基础设施的安全，您负责保护您在 AWS (*图 1*) 中部署的工作负载。这为您提供了在 AWS 环境中为您的业务功能实施最适用的安全控制措施所需的灵活性和敏捷性。您可以严格限制对处理敏感数据的环境的访问，或者为要公开的信息部署不太严格的控制。

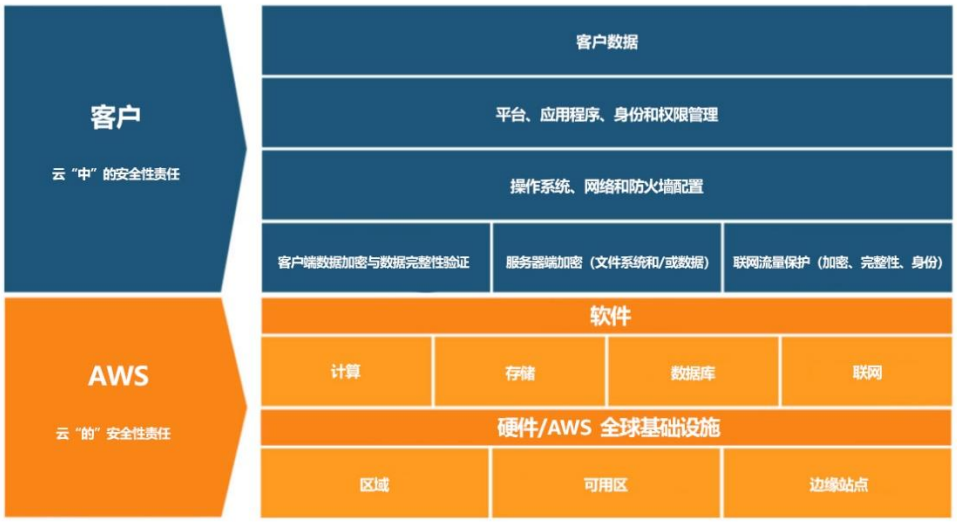

图 1：AWS 共享安全责任模式

安全产品和功能

AWS 及其合作伙伴提供各种工具和功能，以帮助您实现安全目标。这些工具可以镜像您在本地环境中部署的熟悉控制。AWS 提供的安全专用工具和功能涉及网络安全、配置管理、访问权限控制和数据安全这些领域。此外，AWS 还提供了监控和日志记录工具，让您可以全面了解环境中正在发生的情况。

基础设施安全性

AWS 提供了多种安全功能和服务，以增强隐私安全并控制网络访问。其中包括：

- Amazon VPC 内置的网络防火墙让您可以创建私有网络并控制对实例或应用程序的访问。客户可以通过 AWS 服务中的 TLS 控制动态加密。
- 支持从您的办公室或本地环境进行私有或专用连接的连接选项。
- 应用于第 3 层或第 4 层以及第 7 层的 DDoS 缓解技术。这些可作为应用程序和内容分发策略的一部分应用。
- 自动加密 AWS 安全设施之间的 AWS 全球和区域性网络上的所有流量。

库存和配置管理

AWS 提供了一系列工具，可让您在快速移动的同时确保云资源符合组织标准和最佳实践。其中包括：

- 部署工具，用于根据组织标准管理 AWS 资源的创建和删除。
- 库存和配置管理工具，用于识别 AWS 资源，然后追踪并管理这些资源在一段时间内发生的变化。
- 模板定义和管理工具，用于为 EC2 实例创建标准、预配置、强化的虚拟机。

数据加密

借助 AWS，您可以为云中的静态数据添加一层安全保护，并提供可扩展且高效的加密功能。其中包括：

- 大多数 AWS 服务中都提供静态数据加密功能，如 Amazon EBS、Amazon S3、Amazon RDS、Amazon Redshift、Amazon ElastiCache、AWS Lambda 和 Amazon SageMaker
- 灵活的密钥管理选项（包括 AWS Key Management Service）让您可以选择是让 AWS 管理加密密钥还是您自行完全控制自己的密钥
- 使用 AWS CloudHSM 的基于硬件的专用加密密钥存储，有助于让您满足合规性要求
- 加密的消息队列，用于针对 Amazon SQS 使用服务器端加密 (SSE) 来传输敏感数据

另外，AWS 还为您提供了相应的 API，用于将加密和数据保护与您在 AWS 环境中开发或部署的任意服务相集成。

身份和访问控制

AWS 使您能够定义、实施和管理各项 AWS 服务的用户访问政策。其中包括：

- AWS Identity and Access Management (IAM) 让您可以为各个用户账户定义对 AWS 资源的访问权限（特权账户的 AWS Multi-Factor Authentication），包括基于软件和硬件的身份验证器选项。通过 IAM，您可以使用您现有的身份验证系统（如 Microsoft Active Directory 或其他合作伙伴的产品）向员工和应用程序授予对 AWS 管理控制台和 AWS 服务 API 的联合访问权限。
- AWS Directory Service，让您可以与企业目录集成和联合，以便减少管理开销并提升最终用户体验。
- 利用 AWS Single Sign-On (AWS SSO)，您可以轻松在 AWS Organizations 中集中管理您所有账户的 SSO 访问和用户权限。

AWS 在多种 AWS 服务中提供原生 Identity and Access Management 集成，以及与您自己的任何应用程序或服务的 API 集成。

监控和日志记录

您可以通过 AWS 提供的工具和功能了解 AWS 环境中发生的情况。其中包括：

- 利用 AWS CloudTrail，您可以获取您账户的 API 调用历史记录，包括通过 AWS 管理控制台、AWS 开发工具包、命令行工具和更高级 AWS 服务进行的 API 调用，从而监控您在云上的 AWS 部署。您还可以确定哪些用户和账户为支持 CloudTrail 的服务调用了 AWS API、发出调用的源 IP 地址以及调用发生的时间。
- Amazon CloudWatch 提供可靠、可扩展且灵活的监控解决方案，让您可在短短几分钟内开始使用。您不再需要设置、管理和扩展监控系统和基础设施了。
- Amazon GuardDuty 是一种威胁检测服务，可持续监控恶意活动和未经授权的行为，从而保护您的 AWS 账户和工作负载。Amazon GuardDuty 通过 Amazon CloudWatch 公布通知，因此您可以触发自动响应或通知人工处理。
- Amazon Detective 会自动从您的 AWS 资源中收集日志数据并使用机器学习、统计分析和图论来构建一组关联的数据，让您能够轻松地进行更快、更有效的安全调查。

这些工具和功能可为您提供所需的可见性，使您能够在问题影响业务之前发现问题，并提升环境的安全水平，降低环境的风险。

AWS Marketplace 中的安全产品

组织将生产工作负载转移到 AWS，可以在维持安全环境的同时提高敏捷性、可扩展性，并实现创新和成本节省。AWS Marketplace 提供的产品具有行业领先的安全性，这些产品与您本地环境中的现有控制等效、相同或相集成。这些产品是对现有 AWS 服务的补充，使您可以部署综合的安全架构，并为您提供更加流畅的跨云和本地环境的无缝体验。

安全指导

AWS 通过 AWS 及其合作伙伴提供的在线工具资源、支持和专业服务为客户提供指导和专业知识。

AWS Trusted Advisor 是一款在线工具，类似于自定义的云专家，可帮助您配置资源，以遵循最佳实践。Trusted Advisor 会检查您的 AWS 环境来帮助弥补安全漏洞；并发现可以节省开支、提高系统性能和提升可靠性的机会。

AWS 客户服务团队会指定第一联系人，指导您进行部署和实施，并指引您找到正确的资源，解决您可能遇到的安全问题。

AWS 企业支持会在 15 分钟之内响应，并通过电话、聊天或电子邮件提供 24×7 全天候服务；此外，还有专门的技术客户经理。一对一服务可确保尽快解决客户的问题。

AWS 合作伙伴网络可提供数百个行业领先的产品，这些产品与您本地环境中的现有控制等效、相同或相集成。这些产品是对现有 AWS 服务的补充，让您能够部署综合的安全架构，并为您提供更加流畅的跨云和本地环境的无缝体验；同时，还可以在全球范围内提供数百家经过认证的 AWS 咨询合作伙伴，帮助您满足安全性和合规性要求。

AWS 专业服务可提供安全性、风险和合规性专业实践，可帮助您在将最敏感的工作负载迁移到 AWS 云时增添信心并提升您的技术能力。AWS 专业服务可帮助客户基于成熟的设计来开发安全策略和实践，并可以帮助确保客户的安全设计满足内外部合规性要求。

AWS Marketplace 是一种数字目录，收录了来自独立软件供应商的数千种软件产品，可让您轻松查找、测试、购买和部署在 AWS 上运行的软件。AWS Marketplace 安全产品是对现有 AWS 服务的补充，使您可以部署综合的安全架构，并为您提供更加流畅的跨云和本地环境的无缝体验。

AWS 安全公告可提供有关当前漏洞和威胁的安全公告，并使客户能够与 AWS 安全专家协同合作，解决报告滥用、漏洞和渗透测试等问题。我们还在线提供有关漏洞报告的资源。

AWS 安全性文档介绍了如何配置 AWS 服务，以满足您的安全性与合规性目标。AWS 客户可通过专为满足最关注安全性的企业或组织的要求而构建的数据中心和网络架构受益。

AWS 架构完善的框架可帮助云架构师为其应用程序构建安全、高性能且高效的弹性基础设施。AWS 架构完善的框架内含一个安全性支柱，主要用于保护信息和系统。关键主题包括：数据的机密性和完整性、识别和管理谁可以进行哪些权限管理工作、保护系统以及建立检测安全事件的控制措施。客户可以从控制台使用架构完善的服务，也可以使用某个 APN 合作伙伴的服务来为他们提供帮助。

AWS 架构完善的工具可帮助您检查工作负载的状态，并将其与最新的 AWS 架构最佳实践进行对比。进入 AWS 管理控制台，然后回答一系列有关卓越运营、安全性、可靠性、性能效率和成本优化的问题后即可使用此免费工具。然后，AWS Well-Architected Tool 将提供有关如何使用既有最佳实践针对云进行构建的计划。

合规性

AWS 合规性可帮助客户理解 AWS 在 AWS 云中用以维持安全和数据保护的可靠控制。在 AWS 云中构建系统时，AWS 和客户需共担合规性责任。我们持续对 AWS 计算环境进行审核，以获得跨地域和行业的各种认证机构的认证，包括 SOC 1/SSAE 16/ISAE 3402（前 SAS 70）、SOC 2、SOC 3、ISO 9001/ISO 27001、FedRAMP、DoD SRG 以及 PCI DSS Level 1。i 此外，AWS 还具有保障计划，该计划可提供模板和控制映射，以帮助客户确定其在 AWS 上运行的环境的合规性，有关该计划的完整列表，请参阅 AWS 合规性计划。

我们可以确认，根据 GDPR 可以使用所有 AWS 服务。这意味着，除了受益于 AWS 为维护服务安全而采取的所有措施之外，客户还可以将 AWS 服务作为其 GDPR 合规计划的一部分进行部署。AWS 可以提供符合 GDPR 规定的数据处理附录 (GDPR DPA)，让您遵守 GDPR 的合同义务要求。AWS GDPR DPA 已被纳入 AWS 服务条款，并且自动适用于全球所有需要符合 GDPR 规定的客户。Amazon.com, Inc. 已通过《欧盟-美国隐私护盾》认证且 AWS 也包含在此认证中。这有助于选择将其个人数据传输到美国的客户履行其数据保护义务。Amazon.com Inc. 的认证可在“欧盟-美国隐私护盾”网站上找到：https://www.privacyshield.gov/list

通过在经过审核的环境中进行操作，客户可以减少他们需执行的审核范围和成本。AWS 持续对其底层基础设施进行评估，包括其硬件和数据中心的物理和环境安全性，因此客户可以利用这些认证以及简单的内在控制。

在传统的数据中心中，常见的合规性活动通常是定期的人工活动。这些活动包括验证资产配置和报告管理活动。而且，结果报告甚至在发布之前就已过时。在 AWS 环境中进行操作时，客户可以利用 AWS Security Hub、AWS Config 和 AWS CloudTrail 等嵌入式自动化工具来验证合规性。由于这些任务变得日常化、持续化和自动化，因此这些工具减少了执行审核所需的工作。通过减少人工活动时间，可以帮助您将公司中的合规性角色从一种必要的管理负担演变为一种管理风险并改进安全状况的活动。

了解更多内容

有关更多信息，请参阅以下资源：

有关更多信息...	请参阅
AWS 上云安全性的关键主题、研究领域和培训机会	AWS 云安全性学习
将指南规划为六个重点领域的 AWS 云采用框架：业务、人员、治理、平台、安全性和运营	AWS 云采用框架
AWS 的特定控制；如何将 AWS 集成到现有框架中	Amazon Web Services：风险与合规性
有关如何在 AWS 环境中部署安全控制的最佳实践指南	AWS 安全最佳实践
AWS 架构完善的框架 – 安全性支柱	AWS 架构完善的框架 – 安全性支柱

文档修订

日期	描述
2020 年 1 月	已更新以反映最新的服务、资源和技术。
2015 年 7 月	首次发布。