AWS 对重要合规性问题的回答

2017 年 1 月

版权声明

目录

摘要

本文档探讨与 AWS 相关的常见云计算合规性问题。对这些问题的回答可能在评估和运行云计算环境时非常有用，并且可以协助 AWS 客户轻松进行控制管理。

重要合规性问题和回答

类别	云计算问题	AWS 信息
控制所有权	什么人拥有哪些控制体系来管理已部署的云基础设施？	对于部署到 AWS 的部分，AWS 控制该技术的物理组件。客户拥有并控制其他所有部分，包括连接点和传输控制。为了帮助客户更好地了解我们现有哪些控制体系以及其运行效率如何，我们发布了 SOC 1 II 类报告，其中包括围绕 EC2、S3 和 VPC 定义的控制体系，并详细描述了物理安全和环境控制体系。这些控制体系的定义具有高水平的明确度，可满足大部分客户的要求。与 AWS 签订保密协议的客户可以申请一份 SOC 1 II 类报告。
审计 IT	如何完成对云提供商的审计？	对物理控制体系上的大部分层次和控制体系的审计仍然由客户负责。SOC 1 II 类报告中记录了 AWS 定义的逻辑和物理控制体系定义，该报告可供审计与合规性团队审查。AWS ISO 27001 和其他认证也可供审计师审查。
Sarbanes-Oxley 合规性	如果在云提供商环境中部署了范围内的系统，如何达到 SOX 合规性要求？	如果客户在 AWS 环境中处理财务信息，客户的审计人员可以确定有些 AWS 系统已在 Sarbanes-Oxley (SOX) 要求的范围。客户审计人员可以自行确定 SOX 的适用性。由于大部分逻辑访问控制体系是由客户自行管理的，因此客户是确定其控制活动是否达到相关标准的最佳人选。如果 SOX 审计师需要了解 AWS 物理控制体系的相关细节，则可参考 AWS SOC 1 II 类报告，其中详细阐述了 AWS 提供的控制体系。
HIPAA 合规性	是否可以既达到 HIPAA 合规性要求，同时又部署在云提供商的环境？	HIPAA 要求适用于 AWS 客户，并由客户自行控制。AWS 平台支持部署满足特定行业认证要求 (如 HIPAA) 的解决方案。客户可以使用 AWS 服务来维持相当于或高于要求的安全等级，保护电子医疗记录信息。客户已在 AWS 上构建了符合 HIPAA 安全隐私保密规定的医疗保健应用程序。AWS 在其网站上提供了有关 HIPAA 合规性的其他信息，包括有关此主题的白皮书。
GLBA 合规性	是否可以既达到 GLBA 认证要求，同时又部署在云提供商环境中？	大部分 GLBA 要求由 AWS 客户自行控制。AWS 为客户提供各种方法，帮助他们保护数据、管理权限以及在 AWS 基础设施上构建符合 GLBA 要求的应用程序。如果客户需要具体确保物理安全控制体系有效运行，则可参考 AWS SOC 1 II 类报告的相关内容。
联邦政府法规的合规性	美国政府机关是否可以遵从安全隐私保密法规，同时部署在云提供商的环境中？	美国联邦政府机关可能要遵从许多合规性标准，包括 2002 年版联邦信息安全管理法案 (FISMA)、联邦风险与授权管理计划 (FedRAMP)、联邦信息处理标准 (FIPS) 第 140-2 版和美国国际武器贸易条例 (ITAR)。可能还需遵从其他法律和法律条文，具体取决于相应法律设立的要求。

类别	云计算问题	AWS 信息
数据位置	客户数据驻存在何处？	AWS 客户指定其数据和服务器所处的物理位置。对于 S3 数据的数据元复制，则在存储数据的地区集群内进行，不会将数据复制到其他地区的数据中心集群。AWS 客户指定其数据和服务器所处的物理位置。除非应法律或政府部门的要求，否则 AWS 不会在未通知客户的情况下，从客户选择的区域移动客户的内容。有关区域的完整列表，请访问 aws.amazon.com/about-aws/global-infrastructure。
电子取证	云提供商是否能在电子取证程序和要求方面满足客户要求？	AWS 提供基础设施，而客户管理其他组件，包括操作系统、网络配置和安装的应用程序。客户负责响应其使用 AWS 存储或处理的数据的识别、收集、处理、分析以及生成电子文档方面所涉及的法律程序。如果客户需要 AWS 协助处理法律事宜，经客户请求，AWS 可以提供合作。
数据中心参观	云提供商是否支持客户参观数据中心？	否。我们的数据中心中托管了多个客户，这使 AWS 不支持客户参观数据中心，因为这样会导致许多客户遭到第三方物理访问。为了满足客户需要，作为 SOC 1 II 类报告审计流程的一部分，我们支持独立且有能力胜任的审计人员验证控制体系的存在和运行。这种第三方认证向客户提供有关现有控制体系有效性的独立观察结果，得到广泛认可。与 AWS 签订保密协议的客户可以申请一份 SOC 1 II 类报告。对数据中心物理安全的单独审查也是 ISO 27001 审计、PCI 评估、ITAR 审计和 FedRAMP^{sm} 测试计划的一部分。
第三方访问	是否支持第三方访问云提供商的数据中心？	AWS 严格控制对数据中心的访问，即使是内部员工也是如此。除非 AWS 相应数据中心经理按 AWS 访问政策明确批准，否则不会提供第三方访问 AWS 数据中心的权限。请参阅 SOC 1 II 类报告以了解与物理访问、数据中心访问授权相关的控制体系以及其他相关控制体系的具体信息。
特权操作	特权操作是否受到监视？	现有控制体系会限制对系统和数据的访问，并且约束和监视对系统和数据的访问权。另外，默认情况下，客户数据和服务器实例在逻辑上是与其他客户隔离的。在 AWS SOC 1、ISO 27001、PCI、ITAR 和 FedRAMP^{sm} 审计期间，特权用户访问控制由独立审计师审查。
内部访问	云提供商是否已解决内部不当访问客户数据和应用程序所带来的威胁？	AWS 提供了特定的 SOC 1 控制来解决不当的内部访问的威胁，本文档中公开的认证和合规性倡议解答了内部访问有关问题。所有资质证书和第三方认证评估了逻辑访问预防和检测控制体系。此外，定期风险评估也主要针对如何控制和监视内部访问。

类别	云计算问题	AWS 信息
多租户	是否已安全实施客户隔离？	AWS 环境是虚拟化的多租户环境。AWS 已实施旨在隔离每个用户的安全管理流程、PCI 控制体系和其他安全控制体系。AWS 系统旨在防止客户通过筛选虚拟软件访问未向其分配的物理主机或实例。该架构已通过 PCI 合格安全评估商 (QSA) 验证，符合 2015 年 4 月出版的 PCI DSS 2.0 版本的所有要求。 **注意**：AWS 也提供单一租户选项。专用实例是在您的 Amazon Virtual Private Cloud (Amazon VPC) 内启动的 Amazon EC2 实例，其中运行供单一用户专用的硬件。专用实例让您能够充分利用 Amazon VPC 和 AWS 云的优势，同时在硬件级别隔离您的 Amazon EC2 计算实例。
管理程序漏洞	云提供商是否已处理已知的管理程序漏洞？	Amazon EC2 目前采用高度自定义版 Xen 管理程序。内部和外部防窃取团队会定期评估该管理程序的新旧漏洞和攻击载体，非常适合维护虚拟客户机间的强隔离状态。在评估和审计期间，AWS Xen 管理程序安全由独立审计人员定期评估。请参阅 AWS 安全白皮书了解有关 Xen 管理程序和实例隔离的更多信息。
漏洞管理	是否会适当修补系统？	AWS 负责修补系统，例如管理程序和网络服务，以支持向客户交付服务。修补是按照 AWS 策略和 ISO 27001、NIST 和 PCI 要求进行的。客户自行控制其客户操作系统、软件和应用程序，因此也负责修补其自己的系统。
加密	所提供的服务是否支持加密？	是的。AWS 的几乎所有服务，包括 S3、EBS、SimpleDB 和 EC2，都支持客户使用自己的加密机制。VPC 的 IPSec 隧道也进行了加密。Amazon S3 还提供了服务器端加密，可供客户选择。客户也可以使用第三方加密技术。请参阅 AWS 安全白皮书了解更多信息。
数据所有权	云提供商对客户数据享用哪些权利？	AWS 客户保留控制和拥有其数据的权利。AWS 负责保护客户隐私权，并在判断遵从哪些执法部门的要求方面保持警惕。如果 AWS 认为执法部门发布的命令缺乏有力的根据，则会毫不犹豫地提出质询。
数据隔离	云提供商是否会充分地隔离客户数据？	由 AWS 代表客户存储的所有数据均享有强大的租户隔离安全和控制保护。Amazon S3 提供了高级数据访问控制体系。请参阅 AWS 安全白皮书了解有关特定数据安全性的更多信息。
合成服务	云提供商是否支持将其提供的服务与其他提供商的云服务配合使用？	AWS 不利用任何第三方云提供商向客户提供 AWS 服务。
物理和环境控制	这些控制体系是否由指定的云供应商运行？	是的。这些内容在 SOC 1 II 类报告中专门提供了概述。此外，AWS 还支持其他认证，如 ISO 27001 和 FedRAMP[sm]，这些认证需要物理和环境控制体系最佳实践。

类别	云计算问题	AWS 信息
客户端保护	云提供商是否支持客户保护并管理来自各种客户端的访问，如 PC 和移动设备？	是的。AWS 支持客户根据自身需要管理客户端和移动应用程序。
服务器安全	云提供商是否支持客户保护其虚拟服务器的安全？	是的。AWS 支持客户实施自己的安全架构。请参阅 AWS 安全白皮书了解有关服务器和网络安全的更多详情。
Identity and Access Management	该服务是否包含 IAM 功能？	AWS 具有一套身份和访问管理产品，支持客户集中管理用户身份、分配安全证书、整理组中的用户和管理用户权利。请参阅 AWS 网站了解更多信息。
计划维护停机	提供商是否指定何时停止系统进行维护？	AWS 不需要系统下线执行常规维护和系统修补。AWS 自身的维护和系统修补一般不会影响到客户。实例本身的维护由客户控制。
扩展功能	提供商是否支持客户扩展超出原始协议规定？	AWS 云具有分布式、高安全、高弹性的特点，提供客户进行大规模扩展的潜力。客户可以随意扩展或收缩，按使用情况付费。
服务可用性	提供商是否承诺提供高水平的可用性？	AWS 确实承诺在服务水平协议 (SLA) 内提供高水平可用性。例如，Amazon EC2 承诺在其工作年限内，正常运行时间至少达到 99.95%。Amazon S3 承诺月度正常运行时间百分比至少达到 99.9%。如果没有达到此可用性度量，AWS 将提供服务积分。
分布式拒绝服务 (DDoS) 攻击	提供商如何保护其服务免于 DDoS 攻击？	AWS 网络提供强大的保护功能，以应对传统网络安全性问题，而且客户还能实施进一步的保护。请参阅 AWS 安全白皮书了解有关此主题的更多信息，包括有关 DDoS 估攻击的讨论。
数据可移植性	是否可以按客户要求导出存储在服务提供商处的数据？	AWS 支持客户按照需要移动 AWS 存储上的数据。适用于 S3 的 AWS Import/Export 服务可使用便携式存储设备进行传输，加速将大量数据移入和移出 AWS。
服务提供商业务连续性	服务提供商是否运行业务连续性计划？	AWS 确实按业务连续性计划运营。请参阅 AWS 安全白皮书了解详细信息。
客户业务连续性	服务提供商是否支持客户实施业务连续性计划？	AWS 为客户提供了实施稳定的连续性计划的能力，包括频繁实施服务器实例备份、数据冗余复制以及多区域/多可用区部署架构。
数据持久性	数据的持久性是否由服务提供商指定？	Amazon S3 提供具有高持久性的存储基础设施。在 Amazon S3 地区，数据元以冗余方式存储在多个设施间的数个设备中。存储后，Amazon S3 通过快速检测和修复任何丢失的冗余数据，保持数据元的持久性。Amazon S3 还使用校验和定期验证所存储数据的完整性。如果检测到数据损坏，则使用冗余数据进行修复。将数据存储在 S3 中的目标是在指定年度内提供 99.999999999% 的持久性和 99.99% 的对象可用性。

类别	云计算问题	AWS 信息
备份	服务提供商是否提供磁带备份？	AWS 支持客户使用自己的备份服务提供商执行磁带备份。但是，磁带备份不是 AWS 提供的服务。Amazon S3 服务旨在通过存储冗余实现数据丢失率接近零，且数据持久性相当于采用多站点复制数据元所达到的效果。要了解有关数据持久性和冗余的信息，请参阅 AWS 网站。
提价	服务提供商是否会突然提价？	AWS 的一贯做法是随着提供这些服务所需成本的降低而一再降价。AWS 在过去数年里不断降低价格。
可持续性	服务提供商公司是否有长期持续的潜力？	AWS 是领先的云提供商，是 Amazon.com 公司的长期服务战略。AWS 具有非常高的长期持续性潜能。

延伸阅读

有关更多信息，请参阅以下资源：

- AWS 风险和合规性概述
- AWS 认证、计划、报告和第三方鉴证
- CSA 一致性评估倡议问卷

文档修订

日期	描述
2017 年 1 月	迁移到了新模板。
2016 年 1 月	首次发布