云服务

部署在亚马逊云服务平台 (AWS) 的 Thermo Scientific SampleManager LIMS 软件

概述

Thermo Scientific™ SampleManager LIMS™ 软件可部署在本地或亚马逊云服务 (AWS) 平台中。客户可根据其基础架构标准管理本地部署或客户自有云托管服务部署。

与赛默飞世尔科技签约管理其在 AWS 中云部署的客户可获得端对端的支持。赛默飞会提供云服务，安装 SampleManager LIMS 软件，并维护此部署。

以下为 SampleManager LIMS 软件部署到 AWS 的部分功能和优势：

- 在全球范围内所选择的 AWS 区域中，进行全面托管的部署。
- 对 AWS 数据中心和网络的物理访问会受到严格控制、监控及审核。
- 基础架构的访问需要使用多重身份验证、身份识别与访问管理 (IAM)、细粒度权限控制。
- 使用专用服务器和逻辑隔离网络对您的数据进行隔离。
- 采用行业标准加密方法，确保您的动态和静态数据的安全。
- 通过在防火墙和策略/程序级别上的严格控制，保护您的数据，防止遭到未经授权的访问或泄露。
- 将您的数据备份后保存在一个有效期 30 天的滑动窗口中。
- 利用一体化的硬件故障自动恢复功能进行系统管理。
- 服务可用性达 99.5%（同时可选择可用性为 99.9% 的服务）。
- 实时入侵检测和预防。
- 基础架构和用户活动的记录和监控。
- 24 小时恢复时间目标 (RTO)。
- 24 小时恢复点目标 (RPO)。

下面几节概述了应用于 SampleManager LIMS 软件的安全策略和程序。有关 AWS 所提供的安全信息，另请参阅 AWS 云安全网站。

ThermoFisher SCIENTIFIC

设施安全

SampleManager LIMS 软件的 AWS 部署应用于所有客户系统；在赛默飞办事处现场没有安装任何系统。严格控制对赛默飞设施的访问。

系统安全

SampleManager LIMS 软件客户系统在 AWS 的部署和管理按照 AWS 云安全网站中概述的安全策略进行。对公司和客户系统的访问受到控制，且限定为特定的已认证员工。赛默飞的技术运营团队利用多重身份验证来保障系统访问的安全性。

网络安全

客户系统在专用的虚拟私有云 (VPC) 中进行配置和管理。VPC 为外部世界与托管实例之间，以及内部基础架构组件之间的网络交互提供了细粒度权限控制和监控。对每个客户实行的安全策略定义了数据如何流动和谁有权访问系统的所有规则。

入侵检测和预防系统保障了 SampleManager LIMS 软件所驻留网络的安全。该系统安全等级高，具有主动监控、入侵检测和预防功能。对 IDS 进行配置，可在检测到恶意活动时向相应人员发出警报，并自动更新 IDS 签名。

SampleManager LIMS 软件具有专门的高度受控的虚拟专用网络 (VPN)，用于访问 SampleManager LIMS 软件网络。VPN 仅供员工使用，同时会进行主动监控，以确保其使用得当。

数据安全

SampleManager LIMS 软件采用了行业标准 AES-256 加密算法，加密静态数据。所有驻留在数据库或文件系统中的数据都经过加密。

SampleManager LIMS 软件采用行业标准 256 位加密法和 2048 位公钥对传输中的数据进行加密，确保与托管实例的所有通讯都是安全的。限制对存储在客户数据库中的数据进行直接访问。

应用访问

SampleManager LIMS 软件提供了健全的身份验证、授权和记帐 (AAA) 功能。客户可以根据自己的具体需求确立 AAA 策略。赛默飞建议使用可提供最高安全级别的 AAA 策略。

SampleManager LIMS 软件客户可以选择通过设置 IP 限制来限制对其应用程序实例的访问，或允许进行网络访问。

安全编码实践

SampleManager LIMS 软件所利用的安全编码实践是基于开放式 Web 应用程序安全项目 (OWASP) 规定的最佳实践。

SampleManager LIMS 软件利用各种工具来评估代码的安全性，并将安全编码审核用作代码审查的一部分。

日志记录

SampleManager LIMS 软件利用日志管理系统来记录 IT 基础架构活动、用户活动，包括成功和失败的用户身份验证尝试。日志管理系统用于审查已记录的活动，并在发现可疑活动时向技术运营团队发出警报。日志数据最多保留一年。

监控

赛默飞的软件使用多种商业工具主动监控所有系统、网络、应用程序和配套基础架构。使用 AWS CloudWatch、AWS GuardDuty、AWS CloudTrail、入侵防/检测服务、云治理和报警工具对托管服务的安全和健康状况进行监控、记录，并向技术运营团队成员发出警报。

技术运营团队负责对 SampleManager LIMS 软件进行漏洞评估。赛默飞的企业信息安全（CIS）项目用于指导、监督、持续审查，并改进赛默飞所管理的 SampleManager LIMS 软件的云部署的安全控制。

变更管理

赛默飞采用变更管理策略来记录系统和基础架构的变更。对变更进行审查以减少风险，并加以记录，以用于会计核算。赛默飞利用 CloudTrail 记录所有与 AWS 上基础架构相关的活动，包括通过 AWS 管理控制台、AWS SDK、命令行工具和其他 AWS 服务执行的操作。

灾难恢复

SampleManager LIMS 软件具有标准化的部署架构和相关程序。这种标准化允许技术运营团队根据需要轻松建立新的环境。

赛默飞可为跨多个 AWS 区域和可用性区域（参考“区域和可用性区域”）的客户提供服务管理。

赛默飞保留独立于部署环境的所有客户服务的备份（请参阅本文档的“备份和恢复”部分）。

在发生灾难的情况下，赛默飞将评估事件的风险和影响，并联系受影响的客户。技术运营团队将制定恢复服务的计划，重点关注风险和对客户的影响。客户将收到该计划的通知。技术运营团队将执行恢复服务的计划。

备份和恢复

SampleManager LIMS 软件利用亚马逊完善的基础架构执行备份和恢复过程，以维护所有托管系统的系统可用性。

- 系统和数据按照标准的时间表进行备份，并与系统分开存储。
- 由数据或系统损坏或丢失而导致的恢复可视为一个事件，并根据事件管理策略进行管理。
- 技术运营团队将恢复系统和数据，以解决不可恢复的系统故障、数据损坏或数据丢失。
- 在计划执行系统或数据恢复之前，通知客户的利益相关者。
- 赛默飞将验证恢复的系统和数据。客户需要验证恢复情况是否符合他们的期望。
- 将执行所有恢复程序。

赛默飞是 AWS“生命科学合格合伙人项目”中唯一的 LIMS 供应商，赛默飞自 2008 年以来一直在使用 AWS 的服务。

更多信息，请访问 **thermofisher.com/digitalscience**