NetSuite数据中心情况说明书

企业级数据管理、安全、性能和可用性

作为世界上最大的云ERP供应商，NetSuite为超过20,000个组织提供支持、年请求处理量超过700亿条、年度研发投资额超过3800万美元、每季度独立访问量超400万次。NetSuite自1998年起开始为客户提供记录安全维护服务。

NetSuite数据中心的体系结构

NetSuite在加利福尼亚州和马萨诸塞州分别运营有两个独立的数据中心，均以活动模式运行。每一个数据中心都具备数据镜像、灾备数据恢复以及故障转移功能。如果其中一个数据中心发生故障，另外一个会自动启用。两个数据中心的设施由一家领先的配置提供商运营。这家配置提供商专门提供抗震设防、消防以及加热、冷却和备用电源设备。NetSuite应用程序采用多租户架构，所有服务器、存储和硬盘全部建立在多个冗余层之上。

NetSuite数据中心基础设施的相关情况

数据管理

- **冗余：**NetSuite系统中的许多层次实现多层次冗余。这种设计的优势在于，即便有某个或多个组件发生故障，服务也不会被中断。因为当组件发生故障时，在线的多个冗余系统会自动启用，代替失效组件处理数据。

- **灾备数据恢复：**通过内部设立的专有复制机制，复制加利福尼亚州数据中心和马萨诸塞州数据中心的数据并将它们同步至其他数据中心。倘若主数据中心发生故障，所有操作故障转移至次数据中心。我们以每年两次的频率对此故障转移程序进行测试并实施现场验证。故障转移属自动程序，按钮方式即可触发。为了在各种灾难场景中实现故障转移，NetSuite在多地配备有操作工程师和数据中心。
- **可扩展性：**在截至2014年1月的12个月里，NetSuite共计为超过20,000个组织提供支持，每月客户请求处理量超过600万条。NetSuite已对各系统进行设计，使其能够适应使用激增和峰值情况，并且能够稳步向上扩展，以处理更多数据和交易。

应用安全

- **加密：**用户唯一ID和密码以及由此产生连接中所有数据的传输，均按行业标准SSL进行加密。
- **仅限于访问应用程序：**系统分为多个层次，这些层次能够将数据从NetSuite应用程序本身中分离出来。应用程序用户只能访问应用程序功能，但无权访问基本数据库或者其他基础设施组件。
- **角色级别访问和闲置断开：**客户可为每个最终用户分配一个特定角色，这种角色具有特定权限，只能查看并使用与其工作相关的功能。基于用户登录信息跟踪每笔交易的变动并对每次变动作出时间标识，即可进行完整的审查跟踪。此外，系统还可在发现闲置连接时，自动锁定浏览器界面，以防止无人值守的计算机屏幕对其进行未经授权访问。
- **IP地址限制：**可强行限制特定计算机和/或位置访问NetSuite账户。对于那些担心谁会访问以及从哪里可以访问到自己NetSuite账户的客户来说，这种功能非常实用，因为它大幅降低了未经授权第三方访问用户账户的风险。
- **强有力的密码策略：**NetSuite的密码配置选项设置精细（从用户密码长度，到用户密码按需到期设置）。

客户可以制定严格的密码策略，确保新密码不同于先前的密码，且密码的构成足够复杂（同时包含数字、字母和特殊字符）。此外，密码多次输错，账户会自动锁定。NetSuite还提供使用简单物理标记的多因素身份验证，以满足客户对于访问控制的更高要求。除了输入自己的密码之外，用户还必须有随机生成一次性密码的物理标记。这些加密后的鲁棒密码可以防止键盘记录器、窃码者、非法钓客以及密码破译器访问用户账户。

操作安全

- **连续监视：**NetSuite采用大量入侵检测系统（IDS）识别试图访问其网络的恶意流量。阻止未经授权试图访问数据中心的企图，记录并调查任何未经授权的连接尝试。同时安装有企业级防病毒软件，防止特洛伊木马、蠕虫、病毒和其他恶意软件影响企业软件及应用程序。
- **职责分离：**除了强制性核实NetSuite业务各级员工的背景之外，NetSuite奉行职责分离原则。具体来讲，NetSuite遵循最小权限原则（POLA），也就是只向员工分配履行自身职责所需的权限。
- **物理访问：**两个数据中心的运营商实施严格的物理安全策略和控制措施，可实现NetSuite业务部预授权人员的无人陪同访问。
  - 安全的第一层包括照片ID感应卡以及生物识别系统。多因素身份验证系统提供额外保障，防止丢失徽章风险或者其他假冒企图。感应卡读卡器安在主要入口处，用以保护数据中心内部的关键区域。
  - 单人门以及T-DAR捕人陷阱确保每次只有一个人进行身份验证，防止捎带（即，紧随前人、逃避身份验证）情况发生。采用可靠的检测技术并通过安全门防止捎带，能够在很大程度上提升访问控制系统的效力。

- 此外，数据中心周边所有的门均安装有报警和监控设施，所有外墙、门、窗户以及主要室内入口均采用具有保险商实验室（UL）额定弹道保护作用的材料建造。对数据中心周围的植被和其他物体进行美化，使得闯入者无法藏匿。

- **为数据中心安排警卫：**数据中心的警卫负责监控所有报警设施、人员活动、访问点以及运输和接收情况，全天候确保出入程序正确无误。不断对警卫进行意识训练和技能建设。在数据中心配置和其他安全区域入口处安装有多台具有泛倾斜变焦功能的CCTV视频监控摄像机。监控并存储视频，以备不可抵赖审核。

- **特别安全小组：**NetSuite设立了全球安全小组（共有九名成员），专门负责实施安全策略、监控警报设施并调查系统范围内的任何异常行为。该小组分布于全球多个地区，全天候工作。安全小组负责审查并批准对生产区域的所有访问。

- **数据中心性能审计：**NetSuite业务部主管负责按照SSAE 16 II型、ISAE 3402 II型以及PCI实施审计控制。NetSuite效仿国家标准与技术研究院（NIST）的特种出版物800-30以及ISO 27000系列标准制定综合风险管理程序。定期实施审计，以便确保员工绩效、程序合规性、设备可用性、更新的授权记录以及关键的盘点循环在标准以上。

- **安全认证：**NetSuite已通过SSAE 16 II型和ISAE 3402 II型审计，获得PCI-DSS认证并经“《欧盟-美国安全港协议（EU-US Safe Harbor）》”认可。NetSuite按照NIST标准，包括800-53和ISO27000系列标准定义信息安全管理系统。

  - NetSuite的SSAE 16 II型和ISAE 3402 II型审计由四大会计师事务所（Big Four audit firm）筹备和实施。SSAE 16 II型和ISAE 3402 II型审计报告表明，我们的控制环境（包括对数据、网络安全、备份和恢复程序、系统可用性以及应用程序开发的控制）已通过深入审计。根据《萨班斯-奥克斯利法案（Sarbanes-Oxley Act）》第404条的相关规定，对于报告公司财务报告之内部控制的有效性而言，SAS 70 II型审计报告是必不可少的。

- NetSuite按照PCI-DSS的要求开发出可选的3D安全信用卡身份验证功能（也就是所谓的“签证和万事达信用卡安全码验证”）。3D安全验证功能提升了信用卡的防欺诈水平。它要求购物者为自己的信用卡创建身份验证密码，或者要求他们输入密码（前提是已经分配到这种密码）。

- 《欧盟-美国安全港协议》是将个人信息从欧盟国家传输至美国的关键。欧盟组织都知道，在《欧盟-美国安全港协议》框架中进行自我认证的组织提供“充分的”隐私保护（定义见欧洲委员会的数据保护指令）。NetSuite拥护美国商务部（US Department of Commerce）所发布的“安全港隐私保护原则”（针对欧洲经济区（EEA）范围内个人的资料，来源于子公司、客户和其他商业伙伴）。核实NetSuite加入《欧盟-美国安全港协议》的情况，请登陆 http://safeharbor.export.gov/list.aspx.，查阅其上发布的安全港组织公示名单。

- NetSuite已通过国际标准化组织（ISO）27001标准（即，用于测量信息安全管理系统（ISMS）的领先国际标准）认证。该标准要求对安全风险、威胁、漏洞及其影响进行系统检查。想要通过该标准认证的组织必须设计并实施一套综合信息安全控制措施并采用全面的管理程序，以确保信息安全控制措施能够不断满足组织需求。NetSuite已通过这项重要的行业认证，这足以说明公司一直不断致力于维护并改善自身的信息安全管理及数据保管程序。

性能

- **可扩缩的应用程序体系结构：**NetSuite应用程序在三层体系结构上运行。这三层体系结构（分别是网络、应用程序和数据库）可横向扩展并为多数据中心部署提供支持。目前，NetSuite在生产区域运行超过1000台主机。
- **性能团队：**NetSuite为各层次性能投放大量资源。其中包括专门设立由开发人员和数据库管理员（DBA）组成的性能团队。该团队旨在主动验证应用程序性能基准并在最大程度上提升应用程序的性能。
- **高性能数据库：**NetSuite在多核且具有最大内存配置的高性能数据库服务器硬件上运行。NetSuite生产数据库服务器仅在闪存固态硬盘上运行，以此确保业内在最短的时间内能够使用数据库IO性能。

可用性

- **服务级承诺：**NetSuite的服务级承诺（SLC）保证所有客户能够在99.5%的时间内享用正常运行的生产应用程序（预定的服务窗口除外）。倘若NetSuite未能在99.5%的时间内向客户提供应用程序服务，则可向客户退款。按照惯例，我们的实际正常运行时间可达99.98%。登陆公开网页http://status.netsuite.com.，可随时查询系统状态。
- **世界一流的主机操作团队：**NetSuite专门设立有全球性主机操作团队，团队成员累积有几十年的关于大型云计算和软件即服务（SaaS）业务应用程序（要求高性能和高可用性）的运行经验。该团队主动监控整个系统的健康状况，具体采用行业领先的基于警报和趋势工具（旨在实际场地受到影响之前发现并解决相关事件）。该团队全天候工作，采用自动化恢复程序积极应对任何事件。
- **冗余的互联网连接：**为达到或超越关于可用性、完整性和机密性的全球商业电信标准，我们设立了相关网络。NetSuite的两个数据中心均配备有三根1 Gbp多路径管线。这种设计的优势在于，任何两处连接发生故障，都不会对用户体验产生影响。这种冗余能够确保连接可靠并实现正常运行时间的最大化，避免单点与数据中心之间的数据传输瓶颈。此外，每个数据中心还专门设有用于复制数据的两个10 Gbp电路。

- **备用电源系统：**NetSuite已制定出清洁能源和持续电力的解决方案。在配置空间的冗余配置支持环境控制中配备有不间断供电系统（UPS）。每个不间断供电系统的电池系统可在不使用发电机的情况下满负荷工作15分钟。通常情况下，紧急发电机在10秒以内提供备用电力，然后调整规模，以最大负荷为整个设施提供支持。除了不间断供电系统之外，NetSuite还在数据中心地板上安装电源管理模块和配电装置，形成物理集成和电力冗余系统，以便为计算机设备负荷选择资源，进行电力隔离、分配、监测和控制。
- **暖通空调（HVAC）系统：**两个数据中心均配备有空调，有助于适当散热，为现场营造适当的操作环境（即，室温处于可接受范围）。为保持空调流，在各地安装有暖通空调装置的N+1冗余系统。为了维持可用性，暖通空调装置由正常和紧急的电气系统驱动。此外还配备有冷水罐，以便在紧急情况下实现从直接功率到发电机功率的过渡。
- **火灾扑救：**NetSuite的数据中心采用最先进的火灾扑救方法。各系统配备有最高水准的“嗅探器”（附有感温探测以及干式喷水灭火系统）。
- **地震工程：**除在所有设备机架上安装防震拉撑设施之外，NetSuite的数据中心还配备有地震隔离设备，以便利用缓冲作用防止设施移动。设备机架全部锚定至站点活地板下的混凝土板。