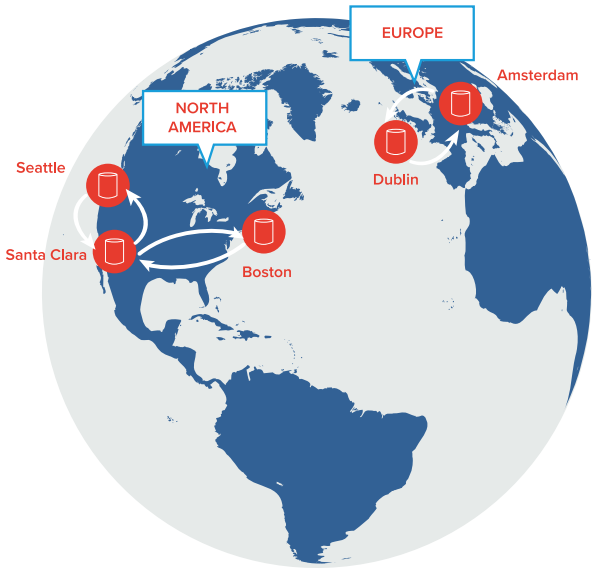
Oracle NETSUITE 数据中心简要介绍

企业级数据管理、安全性、性能和可用性

Oracle NetSuite 是全球较大的云 ERP 供应商，为 4 万多个组织提供支持，每天处理超过 5 亿个应用请求，每天新增 9 TB 数据。自 1998 年以来，Oracle NetSuite 在保持客户记录安全性方面一直成效卓著。

Oracle NetSuite 数据中心架构

Oracle NetSuite 在美国和欧洲地区的不同地理位置运行着 5 个数据中心。数据中心采用星型架构。美国和欧洲地区分别拥有一个专有数据中心，当本地区的任何其他数据中心发生故障时，该专有数据中心将为这些数据中心提供数据镜像、灾难恢复和故障切换功能。两个地区之间的数据不共享。所有数据中心设施由一家先进的托管服务提供商运营并提供抗震、防火保护以及供暖、制冷和备用电源。NetSuite 应用采用多租户模式，所有服务器、存储和硬盘驱动器均构建在多层冗余基础上。



Oracle NetSuite 数据中心基础设施概况

数据管理

- 冗余：Oracle NetSuite 系统中的很多层都实施了多层冗余。这一设计可使多个在线冗余系统自动承担故障组件的处理任务，这样当一个或多个要素发生故障时就不会中断服务。
- 灾难恢复：在同一地区内，数据通过内部专有复制机制在活动数据中心和专有 DR 数据中心之间执行复制和同步。当主数据中心发生故障时，所有运营都会切换至 DR 数据中心。这种故障切换过程每年都会在活动站点进行两次测试和验证。故障切换过程是自动化的，且能够通过按钮触发。Oracle NetSuite 的运营工程师身处不同地理位置，且工程师与数据中心分布在不同的地理位置，这样在发生任何灾难时就可以执行故障切换。Oracle NetSuite 每半年执行一次 DR 演习，确保系统和流程就位，并评估和增强关键 DR 人员的能力，确保成功实施 DR 活动。Oracle NetSuite 数据中心通过磁带备份支持客户发起的数据恢复。
- 可扩展性：Oracle NetSuite 为 4 万多个组织提供支持，每天处理超过 5 亿个应用请求，每天新增 9 TB 数据。Oracle NetSuite 系统可适应用量高峰，并通过向上扩展来应对更高的处理量和事务量。

应用安全

- 加密：用户唯一 ID 和密码的传输以及由此连接的所有数据，均按行业标准协议和密码套件进行加密。Oracle NetSuite 支持自定义属性加密并提供了加密 API。应用采用基于令牌的身份验证，而用户身份验证支持使用移动设备或身份验证 FOB 的现代双因素认证。
- 仅限于访问应用：系统划分为多层，这些层会将数据与 Oracle NetSuite 应用相分离。应用用户只能访问应用特性，而不能访问底层数据库或其他基础设施组件。
- 基于角色的访问和闲置时断开：客户可以为每个用户分配特定角色，这种角色具有特定权限，只能查看和使用与其工作相关的功能。系统实施完整的审计跟踪，将根据用户登录详细信息来跟踪每个事务的更改，并提供每个更改的时间戳。系统还会检测闲置连接并自动锁定浏览器屏幕以防止未经授权的人员通过无人看管的计算机屏幕进行访问。
- IP 地址限制：可以限制从特定计算机和/或位置访问 Oracle NetSuite 帐户。对于那些担心谁会访问以及从哪里可以访问其 Oracle NetSuite 帐户的客户，这些特性非常有用。此特性可大幅降低未经授权的第三方访问用户帐户的风险。

- 强健的密码策略：Oracle NetSuite 提供细粒度的密码配置选项—从用户密码的长度到用户密码按需到期设置。客户可以设置严格的密码策略来确保新密码与之前的密码不同，并且密码是由数字、字母和特殊字符构成的复杂组合。如果多次尝试失败，则帐户会被锁定。对于要求更高级别访问控制的客户来说，Oracle NetSuite 提供了使用简单物理令牌的多因素身份验证。除了输入自己的密码之外，用户还必须拥有可生成随机一次性密码的物理令牌。这些强健的密码可以防止密钥记录器、偷看者、钓鱼程序和密码破解程序访问用户的帐户。

运营安全性

- 持续监视：Oracle NetSuite 使用多个入侵检测系统 (IDS) 来识别尝试访问其网络的恶意流量。这些系统可阻止对数据中心的未授权访问，并记录和调查任何未经授权的连接。Oracle NetSuite 还通过企业级病毒防护软件来防止木马、蠕虫、病毒和其他恶意软件威胁企业软件和应用。
- 职责分离：Oracle NetSuite 除了在所有运营级别执行强制性员工背景调查之外，还提供了职责分离。它遵循最低权限原则 (POLA)，只向员工分配履行自身职责所需的权限。
- 物理访问：所有数据中心的运营商均实施严格的物理安全策略和控制措施，允许预先授权的 Oracle NetSuite 运营人员进行访问：
  - 第一层安全措施包括照片 ID 门禁卡和生物识别系统。这个多因素身份验证系统可提供额外的保证，可防止徽章丢失的风险或其他假冒合法用户的企图。门禁卡设备位于主要入口点，用于保护数据中心的关键区域。
  - 单人门和 T-DAR 人员控制系统可确保一次只对一个人进行身份验证，从而防止尾随。通过可靠地检测并防止尾随和捎带进入安全门，大幅提高了门禁系统的有效性。
  - 此外，周边所有的门都在警报和监控的范围之内，所有外墙、门窗和主要内部入口均采用保险商实验室 (UL) 评定的弹道保护材料建造。数据中心周围的植被和其他物体均依照使入侵者无法隐藏的原则设计。

- 安排警卫：警卫负责监控所有警报、人员活动、入口点以及运输和接收过程，并确保 24x7 全天候严格遵守进出程序。持续对警卫进行意识培训和技能培养。入口点和其他受保护区域安装了大量具有平移/俯仰/变焦功能的 CCTV 视频监控摄像机。视频将受到监控和检查，以备不可抵赖审核。
- 专业安保团队：Oracle NetSuite 通过一个全球安保团队来实施安全策略、监视警报以及调查系统中的任何异常行为。该团队在全球多个位置提供 24x7 全天候安保。所有生产访问都将经过安全团队的审查和批准。
- 数据中心性能审计：Oracle NetSuite 运营管理负责按照 SSAE 16 II 型、ISAE 3402 II 型和 PCI 标准实施审计控制。NetSuite 根据美国国家标准与技术研究院 (NIST) 特刊 800-30 以及 ISO 27000 系列标准进行全面的风险管理流程建模。通过定期审计确保人员绩效、程序合规性、设备可维护性、授权记录更新和关键盘存周期均高于标准。
- 安全性认证：Oracle NetSuite 已通过 SSAE 16 II 型和 ISAE 3402 II 型审计，并且经过 PCI-DSS 认证，符合欧盟-美国隐私保护标准。NetSuite 根据 NIST 标准（包括 800-53 和 ISO27000 系列标准）定义了其信息安全管理系统。
  - Oracle NetSuite 的 SSAE 16 II 型和 ISAE 3402 II 型审计由四大审计公司编制和执行。SSAE 16 II 型和 ISAE 3402 II 型报告表明，我们的控制环境 (包括对数据和网络安全性、备份和恢复过程、系统可用性和应用开发的控制）已通过深度审计。根据萨班斯 - 奥克斯利法案第 404 条的规定，对于公司财务报告内部控制有效性的报告流程而言，SAS 70 II 型审计报告至关重要。
  - 在符合 PCI-DSS 要求的情况下，Oracle NetSuite提供可选 3D 安全信用卡身份验证 — 也称作 VISA 验证服务和 MasterCard SecureCode。3D Secure 提高了信用卡欺诈保护的级别。它要求购物者为其信用卡创建身份验证密码，或者要求他们输入密码 (如果已经指定了密码）。

- Oracle NetSuite 已经通过了国际标准化组织 (ISO) 27001 认证，后者是衡量信息安全管理系统 (ISMS) 的主要国际标准。该标准要求对安全风险、威胁、漏洞及其影响进行系统性检查。为了通过认证，组织必须设计和实施全面的信息安全控制套件，并采用全面的管理流程来确保信息安全控制可持续满足组织的需求。这一重要的行业认证证明 Oracle NetSuite 将致力于持续维护和完善其信息安全管理和数据保管计划。

性能

- 可扩展的应用架构：Oracle NetSuite 应用运行在一个三层架构上。所有三层（网络、应用和数据库）都是可水平扩展的，并且支持多数据中心部署。Oracle NetSuite 目前运行于 4000 多台生产主机上。
- 性能团队：Oracle NetSuite 在每一层上都投入了大量资源来确保性能。包括由开发人员和 DBA 组成的专属性能团队，专门负责主动验证应用性能基准并通过调优来充分发挥应用的性能。
- 高性能数据库：Oracle NetSuite 在具有多个内核和高配置 RAM 的高性能数据库服务器硬件上运行。Oracle NetSuite 生产数据库服务器仅在闪存 SSD 存储器上运行，可确保实现行业领先的数据库 IO性能。
- 性能监视工具：Oracle NetSuite 的应用性能监视工具提供了一个全面的性能信息仪表盘，让您可以轻松快捷地深入了解站点性能问题的根本原因。通过捕获关键性能数据并快速识别、分析和修复问题区域，您可以优化性能、改善客户体验并维护关键事务。

可用性

- 服务级别承诺：Oracle NetSuite 的 SLC 保证所有客户能够在 99.5% 的时间里享受正常运行的 NetSuite 生产应用（预定的服务窗口除外）。如果 NetSuite 未能在 99.5% 的时间内提供应用服务，则可向客户退款。一直以来，我们的实际正常运行时间可达 99.98%。登录公开的网页 http://status.netsuite.com 可随时查询系统状态。
- 世界一流的托管运营团队：Oracle NetSuite 拥有一个由专业托管运营人员组成的全球团队，在运行需要高性能和高可用性的大型云和 SaaS 业务应用方面积累了数十年的相关经验。该团队会主动监视整个系统的运行状况，并运用行业先进、基于警报和趋势的工具来及时识别和解决问题，防患于未然。团队借助自动恢复程序提供 24x7 的突发事件相应。

- 冗余互联网连接：网络在可用性、完整性和机密性方面达到或超过了全球商业电信标准。所有 Oracle NetSuite 数据中心都有三个 10 Gbps 多路径管道，可确保当任意两个连接同时发生故障时都不会影响用户体验。这种冗余可实现可靠的连接和超长的正常运行时间，而不会在数据中心中产生单点数据传输瓶颈。此外，每个数据中心都会使用 2 个专有 10 Gbps 电路来进行数据复制。
- 备用电源系统：Oracle NetSuite 设计了一个清洁能源持续电源方案。通过冗余配置的不间断电源系统 (UPS) 来支持配置空间环境控制。每一个 UPS 电池系统都可以在没有发电机的情况下满负荷工作 15 分钟。紧急发电机通常可在 10 秒钟之内提供备用电源，且足以支持整 个设施在大型负载下运行。除了 UPS 系统，NetSuite 还利用数据中心内的电源管理模块和配电单元打造了一个物理集成和电气冗余的系统，专用于提供计算机设备负载的电源选择、隔离、分配以及监测和控制。
- HVAC 系统：所有数据中心都配备了空调，可提供适当的散热，确保站点在可接受的温度范围内运行。为了保持空调的气流，每个地区采用一个 N+1 冗余 HVAC 单元系统。HVAC 单元由常规和应急电力系统供电，共同确保其可用性。此外，当发生紧急情况，需要从直流电转换为发电机电源时，冷水箱可以保持空调机组的正常运行。
- 消防：Oracle NetSuite 数据中心采用先进的消防方案。数据中心采用先进的“嗅探”系统，并“配有感温探测和干式喷水灭火系统。
- 地震工程：除了在所有设备机架上安装地震支架之外，Oracle NetSuite 运营的数据中心还提供隔震设备来为设备提供缓冲。机架固定在站点高架地板下面的混凝土板上。

要了解更多信息，请联系我们

免费咨询热线：400-610-6668

咨询邮箱地址：SALESINQUIRY_CN@ORACLE.COM