ORACLE NETSUITE OPENAIR 数据中心

企业级数据管理、安全性和可用性

OpenAir 数据中心架构

OpenAir 运行在两个不同地理位置的数据中心内，分别是马萨诸塞州的主数据中心和位于加州的辅助数据中心。当主数据中心无法正常运行时，辅助数据中心将提供数据镜像、灾难恢复和故障切换功能。两个数据中心设施均由先进的托管服务提供商运营，并提供抗震、防火以及供暖、制冷和备用电源。OpenAir 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之上。

OpenAir 数据中心基础设施概况：

数据管理

冗余： OpenAir 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： 马萨诸塞州主数据中心的数据会定期复制和同步到加州的辅助数据中心。当主数据中心发生故障时，将从辅助数据中心为客户提供服务。

可扩展性：截至 2014 年 9 月，12 个月以来，OpenAir 每月支持超过 12.5 万用户，每月处理超过 4.55 亿次客户请求。OpenAir 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，都将使用 AES 128 位 TLS 进行加密。

仅限于访问应用：系统分为多个层次，这些层次会将数据与 OpenAir 应用相分离。应用用户只能使用应用特性来访问数据，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，只能查看并使用与其工作相关的功能。基于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，从而进行完整的审计跟踪。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 OpenAir 帐户。对于那些担心谁会访问以及从哪里可以访问其 OpenAir 帐户的客户，这些特性非常有用。

强健的密码策略：OpenAir 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。

OpenAir 在主数据中心和辅助数据中心中运行。

版权所有 © 2017，Oracle 和/或其关联公司。保留所有权利。

运营安全性

持续监视：OpenAir 使用入侵检测系统 (IDS) 来识别尝试访问其网络的恶意流量。针对数据中心的未经授权的访问尝试会被阻止，并且会记录并调查任何未经授权的连接尝试。此外还会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影响企业软件和应用。

职责分离：除了在 OpenAir 的所有运营级别执行强制性员工背景调查之外，还会执行职责分离。OpenAir 遵守最低权限原则 (POLA)，只向员工分配履行自身职责所需的权限。

物理访问：两个数据中心的运营商都将实施严格的物理安全策略和控制措施：

- 第一层安全措施包括在所有入口设置照片 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以及其他假冒企图。
- 单人门和 T-DAR 捕人陷阱可确保一次只对一个人进行身份验证，从而防止尾随或借道。
- 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。

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 全天候正确遵守进出程序。持续对警卫进行意识培训和技能培养。警卫会随机进行巡视。入口点和其他受保护区域安装 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。

数据中心性能审计：OpenAir 运营管理负责按照 SSAE 16/ ISAE 3402 II 型标准实施审计控制。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达到或超过行业标准。

安全性认证：OpenAir 经过 SSAE 16/ISAE 3402 II 型审计并且通过了欧盟-美国安全港协议认证。OpenAir 根据行业标准定义了其信息安全管理系统。

OpenAir 的 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，对于公司财务报告之内部控制有效性的报告流程而言，SSAE 16/ISAE 3402 II 型审计报告至关重要。

版权所有 © 2017，Oracle 和/或其关联公司。保留所有权利。

欧盟-美国安全港协议是将个人数据从欧盟 (EU) 国家传输至美国的重要准则。欧盟组织都知道，根据欧盟委员会数据保护指令的规定，通过欧盟-美国安全港协议自我认证的组织都将提供“充分”的隐私保护。OpenAir 遵守美国商务部公布的安全港隐私保护原则（针对 EEA 的个人数据，来自于子公司、客户和其他业务合作伙伴）。

可用性

服务级别承诺： OpenAir 的 SLC 保证所有客户能够在 99.5% 的时间里享受正常运行的 OpenAir 生产应用（预定的服务窗口除外）。如果 OpenAir 未能在 99.5% 的时间内提供应用服务，则可向客户退款。

冗余互联网连接： 网络在可用性、完整性和机密性方面可达到或超过全球商业电信标准。两个数据中心均配备两条管道，可突破 100Mbps。这种冗余可实现可靠的连接和超长正常运行时间，而不会在数据中心中产生单点数据传输瓶颈。

备用电源系统： 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高负载下运行。

HVAC 系统： 数据中心配备有空调，有助于适当散热，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，每个地区采用了一个 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。

消防： 数据中心采用新的消防方式，利用先进的“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，辅助数据中心还提供隔震设备来为设备提供缓冲。

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

版权所有 © 2017，Oracle 和/或其关联公司。保留所有权利。