**概览**

在 Coupa，我们致力于为客户提供一个可靠、安全的应用程序，让您可以随时随地管理您的支出。 我们已经合作了[亚马逊网络服务](https://aws.amazon.com/)它提供了硬件和基础设施来支持 Coupa 的电子采购平台。

AWS 于 2002 年 7 月推出，是全球最受欢迎的商品计算和虚拟安全存储随需应变的基础设施。

**物理安全**

有了通过 EC2 服务提供物理托管基础设施的 Amazon.com，Amazon 通过各种方法（如[安全白皮书](http://aws.amazon.com/security).亚马逊 EC2 服务的建筑、服务器和基础设施与他们数十亿美元的 Amazon.com 是一样的，所以你可以保证你的应用程序和数据是安全的。

**运输安全**

我们使用高级加密（AES-256 256 位）加密客户和数据中心之间的所有通信。只有通过安全会话（https）才能访问 Coupa 的随需应变应用程序和服务，并且只能使用经过身份验证的登录和密码。密码不会以原始形式传输或存储，因此不会被第三方泄露。

**周界与服务器安全**

我们通过在 hypervisor、内核和应用程序级别上使用最先进的防火墙，以及在所有服务器上使用入侵检测系统来保护我们的应用程序基础设施。 如果发现任何异常情况，我们的异常检测系统会立即 24/7 地通知操作人员。此外，我们还与第三方安全公司和顾问合作，对漏洞威胁进行评估，包括渗透测试。

我们所有的前端服务器都在防火墙后面，只能通过 https 协议访问。周边防火墙内的数据库服务器受专有的不可路由 IP 寻址方案、网络地址转换等保护。这些特性的细节是专有的。

通过维护所有生产服务器的最少访问点，我们加强了操作系统级的严格安全性。操作系统帐户受到保护使用安全的公钥认证只有操作人员有权访问服务器.为了安全起见，所有操作系统都在每个供应商推荐的补丁级别上维护，并且通过禁用或删除任何不必要的用户、开放端口和进程来加强。对数据库的访问是通过有限的和单独的访问控制密码来控制的。

我们的员工不能直接访问生产设备、数据库或客户数据，除非需要进行系统管理、维护和备份。在需要了解的基础上，对客户数据的访问进一步限于技术和客户支持人员。除非法律要求，Coupa以外的任何一方不得接触客户数据。如需更多资料，请参阅[Coupa 隐私政策](http://www.coupa.com/privacy-policy/).

**应用安全**

没有客户可以看到其他客户的数据。这是在体系结构的几个层次上强制实施的，包括任何页面访问都需要的经过身份验证的会话。会话存储在 cookies 中，不对任何客户可识别信息进行编码。也没有任何客户 ID 在页面访问期间传输或存储，从而防止 ID 欺骗。

**可靠性与备份**

除了 Amazon.com 提供的物理冗余（网络、电源）之外，我们对其基础架构的每个组件都有冗余配置。所有客户数据都存储在带有实时故障转移的冗余数据库服务器上。所有客户数据都放在 RAID 类硬件上，实时复制到不同数据中心的次要环境，然后每隔 60 分钟备份到 Amazon.com S3 服务上。然后，Amazon.com S3 服务在全球的 Amazon.com 数据中心中被复制。

**灾难恢复程序**

我们能够利用 Amazon AWS 云提供最好的类灾难恢复程序。如上所述，使用 Amazon AWS 服务进行数据存储，我们消除了客户数据丢失的风险。如果客户的主要硬件发生故障，我们可以立即切换到与主硬件同时运行的次要硬件。如果主服务器和辅助服务器都发生了故障，我们有能力在几分钟内故障转移到美国和欧洲的任何数量的 Amazon.com 数据中心。

**数据库安全性**

为每个客户对数据库进行分区，这样不同客户的数据就不会混合在一起。数据库基础设施通过防火墙与应用服务器和 Internet 完全隔离。只有应用服务器可以使用强身份验证查询数据库。敏感数据（如密码）在存储到数据库之前用加密的强密码进行加密。数据库服务器具有保护所有 Coupa 服务器的相同的基于主机的安全性。