白皮书

自治修补的安全性优势：Oracle 自治数据库

由 Oracle 赞助

Carl W. Olofson
2018 年 10 月

内容提要

在本白皮书中，我们将介绍及时修补数据库管理系统 (DBMS) 软件的重要性，尤其是及时应用安全补丁的重要性。通常，大多数数据中心不会经常修补系统，从而会让数据库暴露在风险之下。本白皮书将讨论这类风险以及引发数据库不可用的相关因素。

有人也许认为，迁移到云端托管数据库服务便能解决可用性问题，然而此类服务仍然需要客户与服务提供商进行交互，因此修补过程中仍然存在数据库不可用问题。相比之下，Oracle 自治数据库云服务能够在不停机的情况下及时修补系统，保证持续可用性和最高安全性，从而彻底解决这个问题。

方案概要

修补问题

计算机软件并不是一成不变的，它们需要不断地改进和更新。有时这是为了改变使用模式或纠正之前未检测到的问题，但大多数时候这是为了修补可能会被恶意攻击者发现和利用的各种漏洞。鉴于数据泄露会给企业带来大麻烦，因此更新工作对于数据库来说尤其重要，而这些更新是通过修补完成的。

什么是修补？

补丁是为改变软件行为而插入到现有软件中的一小段代码。它们可能为了修复某个已知问题、实施某种大家期待的功能改进，或者堵上某个安全性漏洞。在为数据库服务器应用补丁时，我们通常需要让服务器下线以便修改代码，然后再让其重新上线。

修补为什么会成为一个大问题？

既然延迟修补可能会让企业遭受潜在的黑客攻击，那么企业为什么不立即执行修补呢？这是因为修补工作涉及系统停机和员工工作，因此必须安排在非工作时间进行。然而，即便是在夜间，让数据库离线还是会带来不便，特别是在需要保证 7x24 可用性的环境中，离线方案是不可行的。作为替代方案，我们可以配置第二个数据库服务器，在其中加载软件、应用补丁、测试经修补的系统，然后进行服务器切换。

在这种方案下，当我们让其中一台服务器停止服务，将最后的事务传递至另一台服务器，并让另一台服务器上线时，系统通常会发生短暂的服务中断。因此，修补会产生额外的人工工作，中断其他任务并干扰运营安排。而这些活动的成本可能相当高。具体来说，大多数用户拥有多个数据库实例，修补工作的总工时成本大致可以按每个实例一小时来计算。因为即便修补本身只需 15 分钟，但整个过程，包括让系统离线、应用补丁、验证补丁以及让系统重新上线，总共可能需要一小时之久，这甚至还没有算上由于系统管理员和其他运营人员围绕此活动开展工作而导致的运营中断时间。因此，企业通常不会在发布补丁的第一时间应用它们，而是安排某个时间批量打补丁。

延迟修补可能导致哪些风险？

不及时打补丁会产生的后果是，已在当前代码库中修复的问题将得不到解决，功能增强将不可用，更重要的是，已知漏洞将仍然存在，让数据库面临遭到黑客攻击的风险。延迟修补还可能导致其他一些问题。许多 DBA 在电话求助时都会感到心情沮丧，支持工程师反问的第一句往往是“你们的补丁版本是多少？”如果不是最新版本，支持工程师会建议他们先更新至当前补丁版本，如果问题仍然没有得到解决再打电话求助。此外，安全风险尤其巨大。当数据库厂商发布补丁来解决某个漏洞时，通常意味着那个漏洞已广为人知，而黑客们也已开始伺机向尚未修补该漏洞的数据库发动攻击。因此，延迟修补具备相当大的危险性。

云服务修补

迁移至云端可以解决及时修补的问题，但这并不一定是完美的解决方案。在很多使用公有云服务的案例中，用户通常采用“责任共担模式”，即，对系统物理层面的责任（包括安全性）由托管云提供商承担，而对软件状态的责任（包括修补）由用户承担。在这种模式下，软件修补工作还是需要由员工来执行，并且会导致停机。

即便某些托管云数据库提供商可为数据库服务器提供全部软件支持，他们还是需要与用户一起安排修补工作，因为修补会导致服务中断。单单这一个问题就足以让有些用户放弃在第一时间修补软件，选择累积多个补丁进行批量修补。

如何才能解决修补问题？

要确保及时应用补丁，唯一办法是使用提供不间断修补流程的服务。这种服务能够杜绝延迟修补或累积多个补丁进行批量修补的现象，确保数据库服务器始终运行修复了所有已知安全性漏洞的新版本。这种能力的重要性不言而喻。

Oracle 自治数据库

Oracle 自治数据库是 Oracle 云中提供的一款托管云数据库服务。对于出于法律要求或运营需要而将数据保留在数据中心的客户，Oracle 还提供 Oracle 公有云本地化解决方案，这是一款由 Oracle 云团队远程管理、但架设在客户数据中心内部的物理系统。

完整的云数据库服务

Oracle 自治数据库是一款完整的云服务，所有运营方面的繁琐工作均由 Oracle 云团队打理，包括数据库的升级和修补工作。该系统还能自治调优，利用机器学习算法持续改进性能。它采用透明的滚动升级方式，可确保在发布补丁的第一时间应用补丁，并且不会产生任何服务中断。因此，用户无需费神安排修补工作，也不必担心系统停机。

Oracle 的修补方法

Oracle 即时应用所有安全补丁，其他补丁则是根据预定计划来应用补丁。我们采用滚动修补方式，消除了停机时间，确保数据库持续可用。Oracle 能这样做是因为我们的硬件配置支持不间断运行，我们的软件支持在服务器之间平滑切换。而这一切要归功于 Oracle 长期以来在不间断运行服务器集群方面积累的丰富经验，其中特别值得一提的是我们在 2001 年推出的 Real Application Clusters (RAC)。Oracle 自治数据库软件的自治调优功能提供卓越的灵活性，可确保系统性能平稳。该技术是 Oracle 数十年研发投入的成果，最初在 Oracle9*i* 和自管理功能一起推出时即获得广泛赞誉。修补和补丁测试流程在后台运行，用户几乎查觉不到这些流程的运行。与需要手动操作且易于出错的其他修补方法相比，这种方法显然非常优越。

Oracle 自治数据库的其他安全性功能

除了补丁管理，Oracle 自治数据库还提供三大重要功能来确保数据库的安全性。它们是：

- **加密。**Oracle 对静态数据和传输中数据均进行加密。不仅在存储节点和处理节点之间传输的数据经过加密，甚至缓存中的数据也会保持加密。系统会自动启用该功能。
- **对数据管理和数据库管理实行职责分离。**Oracle 通过 Database Vault 和可插拔数据库锁定配置文件等特性实现数据库管理（由 Oracle 负责）和数据管理（由自治数据库客户负责）的职责分离。
- **审计。**Oracle 自治数据库自动配置、启用并持续运行数据审计。该数据库系统会记录可疑的访问模式，并能灵活地将对收集数据的分析扩展到其他服务甚至本地部署的安全信息和事件监视系统上。

未来展望

IDC 认为，大多数企业数据将在未来五到七年迁移至云端，在此过程中，数据安全性要求将逐步增强。企业在决定采用哪种 RDBMS 来托管其宝贵而敏感的数据时，Oracle 自治数据库系统提供的这些功能仍然是关键考虑因素。放眼未来，数据量将继续快速增长，数据形式也存在更多变数，在识别待保护数据和制定不影响数据库性能的保护措施方面，我们面临的挑战也将越来越大。

挑战/机遇

将数据迁移至云端可应对常见的大多数非法数据访问问题，包括企业数据中心通常存在的服务器配置不当现象以及“后门”密码。Oracle 自治数据库更是提供大量功能来保障数据安全。然而恶意攻击者的手段愈来愈狡猾，新型攻击方法层出不穷。即便这里所述的 Oracle 安全性方法大幅领先于同类产品，但数据库安全方面的新威胁仍在不断袭来，需要我们保持警惕、锐意创新、深谋远虑才能战胜它们。

总结

数据库安全性受到多种多样的威胁，有些涉及应用设计和开发，另外一些则涉及数据库管理系统。当 DBMS 开发人员发现漏洞时，通常会发布补丁来解决它们。延迟应用此类补丁会导致数据库暴露在攻击之中。但企业往往会因为手动应用补丁所涉及的成本、风险和运营中断而延迟打补丁。

针对这一问题，Oracle 在 Oracle 自治数据库中提供了应对方法，让企业能够及时地自动应用安全补丁，不仅避免了手动修补流程伴随的风险，而且不会产生任何运营中断。采用该解决方案，企业可以选择将数据迁移至 Oracle 云，也可以通过 Oracle 公有云本地化解决方案将数据保留在本地数据中心。

该服务在数据库安全性方面可为客户带来下列优势：

- 消除手动应用安全补丁的成本和风险
- 及时、自动地应用安全补丁，确保针对所有已知漏洞应用最新更新
- 提供可增强数据库安全性的其他功能，包括对静态数据和传输中数据进行加密；自动、持续进行活动审计；以及通过 Database Vault 确保只有实际操作数据的人员才能看到相关数据。

考虑到这些优势，IDC 建议用户：

- 弄清楚几个问题：我们多久应用一次安全补丁？有多少已知漏洞正在威胁我们的数据？
- 计算应用安全补丁的劳动力和运营成本（包括运营中断和人为错误风险），以便确定当前做法给企业带来的成本。
- 考虑部署能够自动应用安全补丁并且由专业的专家团队管理的系统，替代当前的安全策略。
- 评估 Oracle 自治数据库在最大化保障数据库安全性方面的潜在优势。

关于 IDC

International Data Corporation (IDC) 是一家面向信息技术、通讯和消费技术市场提供市场情报、咨询服务以及各种活动的卓越全球提供商。IDC 帮助 IT 专业人士、业务高管和投资团体就技术采购和商业战略制定基于事实的决策。IDC 拥有 1100 多名分析师，就全球 110 多个国家/地区的技术和行业机遇及发展趋势提供全球性、地区性和当地的专业建议。50 年来，IDC 一直为客户提供战略洞察，帮助他们实现关键业务目标。IDC 是全球领先的技术媒体、研究和会展公司 IDG 旗下的一家子公司。

全球总部

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter：@IDC
idc-community.com
www.idc.com