

Oracle® Solaris 10 安全准则

版权所有 © 2011, Oracle 和/或其附属公司。保留所有权利。

本软件和相关文档是根据许可证协议提供的，该许可证协议中规定了关于使用和公开本软件和相关文档的各种限制，并受知识产权法的保护。除非在许可证协议中明确许可或适用法律明确授权，否则不得以任何形式、任何方式使用、拷贝、复制、翻译、广播、修改、授权、传播、分发、展示、执行、发布或显示本软件和相关文档的任何部分。除非法律要求实现互操作，否则严禁对本软件进行逆向工程设计、反汇编或反编译。

此文档所含信息可能随时被修改，恕不另行通知，我们不保证该信息没有错误。如果贵方发现任何问题，请书面通知我们。

如果将本软件或相关文档交付给美国政府，或者交付给以美国政府名义获得许可证的任何机构，必须符合以下规定：

U.S. GOVERNMENT RIGHTS

Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

本软件或硬件是为了在各种信息管理应用领域内的一般使用而开发的。它不应被应用于任何存在危险或潜在危险的应用领域，也不是为此而开发的，其中包括可能会产生人身伤害的应用领域。如果在危险应用领域内使用本软件或硬件，贵方应负责采取所有适当的防范措施，包括备份、冗余和其它确保安全使用本软件或硬件的措施。对于因在危险应用领域内使用本软件或硬件所造成的一切损失或损害，Oracle Corporation 及其附属公司概不负责。

Oracle 和 Java 是 Oracle 和/或其附属公司的注册商标。其他名称可能是各自所有者的商标。

Intel 和 Intel Xeon 是 Intel Corporation 的商标或注册商标。所有 SPARC 商标均是 SPARC International, Inc 的商标或注册商标，并应按照许可证的规定使用。AMD、Opteron、AMD 徽标以及 AMD Opteron 徽标是 Advanced Micro Devices 的商标或注册商标。UNIX 是 The Open Group 的注册商标。

本软件或硬件以及文档可能提供了访问第三方内容、产品和服务的方式或有关这些内容、产品和服务的信息。对于第三方内容、产品和服务，Oracle Corporation 及其附属公司明确表示不承担任何种类的担保，亦不对其承担任何责任。对于因访问或使用第三方内容、产品或服务所造成的任何损失、成本或损害，Oracle Corporation 及其附属公司概不负责。

目录

| | |
|---------------------------------------|----------|
| 前言 | 5 |
| 1 Oracle Solaris 10 安全准则 | 9 |
| Oracle Solaris 10 系统强化参考文档 | 9 |
| Oracle Solaris 10 的其他安全参考文档 | 10 |

前言

本指南提供了有关 Oracle Solaris 操作系统 (Oracle Solaris OS) 安全准则的链接和描述。系统强化参考文档描述了如何强化 Oracle Solaris 10 系统以及如何使用 Oracle Solaris 安全功能保护数据和应用程序。您可以根据站点的安全策略调整这些参考文档中提供的建议。

此外，本指南还提供了关于 Oracle Solaris 安全性的背景信息链接以及指导您完成常见实施的白皮书。

目标读者

《Oracle Solaris 10 安全准则》适用于安全管理员和执行以下任务的其他管理员：

- 分析安全要求
- 在软件中实现安全策略
- 安装和配置 Oracle Solaris OS
- 维护系统和网络安全

要使用本指南，必须具备常规的 UNIX 管理知识和扎实的软件安全性基础知识，并了解站点安全策略。

相关的第三方 Web 站点引用

本文档引用了第三方 URL 以提供其他相关信息。

Oracle 对本文档中提到的第三方 Web 站点的可用性不承担任何责任。对于此类站点或资源中的（或通过它们获得的）任何内容、广告、产品或其他资料，Oracle 并不表示认可，也不承担任何责任。对于因使用或依靠此类站点或资源中的（或通过它们获得的）任何内容、产品或服务而造成的或连带产生的实际或名义损坏或损失，Oracle 概不负责，也不承担任何责任。

获取 Oracle 技术支持

Oracle 客户可以通过 My Oracle Support 获取电子支持。有关信息，请访问 <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info>，或访问 <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs>（如果您听力受损）。

印刷约定

下表介绍了本书中的印刷约定。

表 P-1 印刷约定

| 字体或符号 | 含义 | 示例 |
|------------------|-----------------------|---|
| AaBbCc123 | 命令、文件和目录的名称；计算机屏幕输出 | 编辑 .login 文件。 使用 <code>ls -a</code> 列出所有文件。 <code>machine_name% you have mail.</code> |
| AaBbCc123 | 用户键入的内容，与计算机屏幕输出的显示不同 | <code>machine_name%su</code> Password: |
| <i>aabbcc123</i> | 要使用实名或值替换的命令行占位符 | 删除文件的命令为 <code>rm filename</code> 。 |
| <i>AaBbCc123</i> | 保留未译的新词或术语以及要强调的词 | 这些称为 <i>Class</i> 选项。 注意： 有些强调的项目在联机时以粗体显示。 |
| 新词术语强调 | 新词或术语以及要强调的词 | 高速缓存 是存储在本地的副本。 请勿保存文件。 |
| 《书名》 | 书名 | 阅读《用户指南》的第 6 章。 |

命令中的 shell 提示符示例

下表显示了 Oracle Solaris OS 中包含的缺省 UNIX shell 系统提示符和超级用户提示符。请注意，在命令示例中显示的缺省系统提示符可能会有所不同，具体取决于 Oracle Solaris 发行版。

表 P-2 shell 提示符

| shell | 提示符 |
|---|-----|
| Bash shell、Korn shell 和 Bourne shell | \$ |
| Bash shell、Korn shell 和 Bourne shell 超级用户 | # |

表 P-2 shell 提示符 (续)

| shell | 提示符 |
|--------------|---------------|
| C shell | machine_name% |
| C shell 超级用户 | machine_name# |

Oracle Solaris 10 安全准则

Oracle Solaris 10 是一款强大的高级企业操作系统，其提供已被证实有效的安全功能。Oracle Solaris 10 通过一个复杂的网络范围的安全系统控制用户访问文件、保护系统数据库和使用系统资源的方式，可以满足各层的安全需求。传统的操作系统会存在固有的安全漏洞，而 Oracle Solaris 10 的灵活性使其可以满足从企业服务器到桌面客户端的各种安全目标。

Oracle Solaris 10 系统强化参考文档

以下两篇文档描述了如何强化 Oracle Solaris，如何使用其安全功能配置系统，以便在向系统中添加应用程序和用户时实现安全操作，以及如何使用特定安全功能保护基于网络的应用程序。每一文档标题后都有简短说明。

- 《CIS Solaris 10 Benchmark v5.0.0》(<http://benchmarks.cisecurity.org/en-us/?route=downloads.show.single.solaris10.500>) (《CIS Solaris 10 基准 v5.0.0》)，2010 年 7 月 9 日。

此文档的另一名称是《Security Configuration Benchmark for Solaris 10 11/06 through 10/09》。此基准是多方耗费七年多时间取得的工作成果，对其做出贡献的包括 Oracle Corporation、美国国防信息系统局 (Defense Information Systems Agency, DISA)、因特网安全中心 (Center for Internet Security, CIS)、美国国家标准技术研究所 (National Institute of Standards and Technology, NIST)、美国国家安全局 (National Security Agency, NSA) 以及众多企业、学术机构和个人。此基准确立了 Oracle、CIS、NSA 和 DISA 认可的一套基本强化准则。

- 《An Overview of Solaris 10 Operating System Security Controls》(http://www.nsa.gov/ia/_files/os/sunsol_10/s10-cis-appendix-v1.1.pdf) (《Solaris 10 操作系统安全控制概述》)，Glenn Brunette 编著，2007 年 9 月，v1.0

《Security Configuration Benchmark for Solaris 10 11/06 through 10/09》的此附录重点讨论 Oracle Solaris 10 中的安全控制，这一部分不在系统强化和安全配置验证的范围内。此附录完整概述了 Oracle Solaris 10 的安全特性和功能，并提供了一些具体建议（如有可能）。

Oracle Solaris 10 的其他安全参考文档

以下指南和文章补充说明了上一节中的系统强化准则：

- 《系统管理指南：安全性服务》

此安全指南由 Oracle 出版，面向 Oracle Solaris 10 管理员。此指南描述了 Oracle Solaris 10 OS 的安全功能以及在配置系统时如何使用这些功能。与《Security Configuration Benchmark for Solaris 10 11/06 through 10/09》不同，此指南不是一篇关于系统强化或最佳做法的文档。

- 《Solaris 10 Security Essentials》，Oracle 工程师，2009。ISBN 978-0137012336

Solaris 工程师和技术文档编写者在此普及版书中描述了 Solaris 的 12 项安全技术，并提供了相应示例。与《Security Configuration Benchmark for Solaris 10 11/06 through 10/09》不同，此指南不是一篇关于系统强化或最佳做法的文档。

- 《Using Oracle® Solaris 10 to Overcome Security Challenges》(<http://www.oracle.com/technetwork/server-storage/solaris/solaris-10-security-167783.pdf>) (《使用 Oracle® Solaris 10 应对安全挑战》)，2010 年 8 月。

此 Oracle 白皮书针对需要全面的系统安全功能的组织。需要高效的计算机安全解决方案的 IT 部门可以使用 Oracle Solaris 10 独特而强大的安全功能来帮助企业抵御潜在威胁，遵循公司和监管机构的要求，并预防安全问题。此白皮书概述了 Oracle Solaris 安全功能。此白皮书不是一篇关于强化或最佳做法的文档。

- 《Hardening Oracle Database with Oracle Solaris Security Technologies》(<http://www.oracle.com/technetwork/server-storage/solaris/solaris-security-hardening-db-167784.pdf>) (《使用 Oracle Solaris 安全技术强化 Oracle Database》)，Glenn Faden 和 Christoph Schuba 合著，2010 年 8 月。

此 Oracle 白皮书描述和演示了 Oracle Solaris OS 商品化的安全功能可以如何用于锁定面向网络的服务，以便保护其免受内部和外部威胁。技术概念及其实现以实际操作形式提供，即采用 Oracle Database Server 11g 发行版 2 运行示例（该示例在 Solaris 10 10/09 发行版上执行）进行说明。