Oracle® Solaris 11 安全准则

文件号码 E25819
2012 年 3 月

ORACLE

120413@25097

目录

前言

本指南提供了 Oracle Solaris 操作系统 (Oracle Solaris OS) 安全准则。首先，本指南介绍了企业 OS 必须解决的安全问题。然后，它还介绍了 Oracle Solaris OS 的缺省安全功能。最后，本指南提供了强化系统和使用 Oracle Solaris 安全功能来保护数据和应用程序需要执行的具体步骤。您可以根据站点的安全策略调整本指南中提供的建议。

目标读者

《Oracle Solaris 11 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
- 在软件中实现站点安全策略
- 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。

获取 Oracle 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 ls -a 列出所有文件。 machine_name% you have mail.

表 P–1 印刷约定 （续）

字体或符号	含义	示例
AaBbCc123	用户键入的内容，与计算机屏幕输出的显示不同	`machine_name% su` `Password:`
aabbcc123	要使用实名或值替换的命令行占位符	删除文件的命令为 `rm` *filename*。
AaBbCc123	保留未译的新词或术语以及要强调的词	这些称为 *Class* 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	`#`
C shell	`machine_name%`
C shell 超级用户	`machine_name#`

◆ ◆ ◆ 第 1 章

1 Oracle Solaris 11 安全概述

Oracle Solaris 11 是一款强大的高级企业操作系统，提供已被证实有效的安全功能。Oracle Solaris 11 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要求。传统的操作系统会存在固有的安全漏洞，而 Oracle Solaris 11 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。在 Oracle 多种基于 SPARC 和 x86 的系统上以及其他第三方供应商硬件平台上对 Oracle Solaris 11 进行了充分测试并提供支持。

Oracle Solaris 11 安全保护

Oracle Solaris 通过保护磁盘上的数据以及传输中的数据为公司数据和应用程序提供了坚实的基础。Oracle Solaris 资源管理器（称为**资源管理**）和 Oracle Solaris Zones 提供隔离应用程序并防止应用程序被误用的功能。这些功能与通过 Oracle Solaris 的特权和基于角色的访问控制 (role-based access control, RBAC) 功能实现的最小特权一起，可减少入侵者或一般用户操作的安全风险。已验证的加密协议（如 IP 安全 (IP security, IPsec)）通过 Internet 提供虚拟专用网络 (virtual private network, VPN)，并在 LAN 或 WAN 内提供通道，以便安全传送数据。此外，Oracle Solaris 的审计功能可确保记录关注的任何活动。

Oracle Solaris 11 安全服务通过为系统和网络提供保护层来提供深层防御。Oracle Solaris 通过在内核实用程序内限制实用程序可执行的特权操作来保护内核。缺省网络配置在系统上以及网络中提供数据保护。IPsec（Oracle Solaris 的 IP 过滤器功能）和 Kerberos 可提供附加保护。

Oracle Solaris 安全服务包括：

- 保护内核－内核守护进程和设备受文件权限和特权保护。
- 保护登录－登录需要口令。口令是强加密的。远程登录最初通过 Oracle Solaris 的安全 Shell 功能限定为已验证的加密通道。`root` 帐户无法直接登录。
- 保护数据－磁盘上的数据受文件权限保护。可以配置其他保护层。例如，可以使用访问控制列表 (access control list, ACL)、将数据放置在区域中、加密文件、加密 Oracle Solaris ZFS 数据集、创建只读 ZFS 数据集以及挂载文件系统，以便无法运行 `setuid` 程序且无法执行可执行文件。

Oracle Solaris 11 安全技术

可配置 Oracle Solaris 的安全功能以实施站点的安全策略。

以下各节对 Oracle Solaris 安全功能进行了简短介绍。这些说明包括对本指南以及介绍这些功能的其他 Oracle Solaris 系统管理指南中更详细的解释和过程的引用。

审计服务

审计是指收集有关系统资源使用情况的数据。审计数据提供安全相关的系统事件的记录。以后便可以使用此数据来指定系统上执行的操作的职责。

审计是安全评估、验证和认证机构的基本要求。审计还可阻止潜在的入侵者。

有关更多信息，请参见以下内容：

- 有关与审计相关的手册页列表，请参见《Oracle Solaris 管理：安全服务》中的第 29 章 “审计（参考）”。
- 有关指南，请参见第 30 页中的 “审计除登录/注销之外的重要事件”以及手册页。
- 有关审计的概述，请参见《Oracle Solaris 管理：安全服务》中的第 26 章 “审计（概述）”。
- 有关审计任务，请参见《Oracle Solaris 管理：安全服务》中的第 28 章 “管理审计（任务）”。

基本审计报告工具

使用 Oracle Solaris 的基本审计报告工具 (Basic Audit Reporting Tool, BART) 功能，可以通过在一段时间内对系统执行文件级别的检查来全面地验证系统。通过创建 BART 清单，可轻松可靠地收集已部署系统上所安装软件栈的组件的相关信息。

BART 是一个非常有用的工具，可在一个系统或一个系统网络上进行完整性管理。

有关更多信息，请参见以下内容：

- 所选手册页包括 `bart(1M)`、`bart_rules(4)` 和 `bart_manifest(4)`。
- 有关指南，请参见第 42 页中的 “创建系统的 BART 快照”、第 45 页中的 “使用基本审计报告工具”以及手册页。
- 有关 BART 的概述，请参见《Oracle Solaris 管理：安全服务》中的第 6 章 “使用基本审计报告工具（任务）”。
- 有关使用 BART 的示例，请参见《Oracle Solaris 管理：安全服务》中的“使用 BART（任务）”以及手册页。

加密服务

Oracle Solaris 的加密框架功能和密钥管理框架 (Key Management Framework, KMF) 功能为加密服务和密钥管理提供中央系统信息库。硬件、软件和最终用户可无缝访问经过优化的算法。各种公钥基础结构 (public key infrastructure, PKI) 的不同存储机制、管理实用程序和编程接口可在采用 KMF 接口时使用统一接口。

加密框架通过各个命令、用户级别编程接口、内核编程接口、用户级别框架以及内核级别框架向用户和应用程序提供加密服务。加密框架以对最终用户无缝的方式向应用程序和内核模块提供这些加密服务。它还向最终用户提供直接的加密服务，例如对文件进行加密和解密。

KMF 提供用于集中管理公钥对象（例如 X.509 证书和公钥/私钥对）的工具和编程接口。存储这些对象所用的格式可能有所不同。KMF 还提供了一种工具，用于管理定义应用程序如何使用 X.509 证书的策略。KMF 支持第三方插件。

有关更多信息，请参见以下内容：

- 所选手册页包括 `cryptoadm(1M)`、`encrypt(1)`、`mac(1)`、`pktool(1)` 和 `kmfcfg(1)`。
- 有关加密服务的概述，请参见《Oracle Solaris 管理：安全服务》中的第 11 章 “加密框架（概述）”和《Oracle Solaris 管理：安全服务》中的第 13 章 “密钥管理框架”。
- 有关使用加密框架的示例，请参见《Oracle Solaris 管理：安全服务》中的第 12 章 “加密框架（任务）”以及手册页。

文件权限和访问控制条目

用于保护文件系统中对象的第一道防线是为每个文件系统对象指定的缺省 UNIX 权限。UNIX 权限支持为对象的所有者、指定给对象的组以及其他所有人指定唯一访问权限。此外，ZFS 还支持访问控制列表 (access control list, ACL)（也称为访问控制条目 (access control entry, ACE)），从而更好地控制个人或组对文件系统对象的访问权限。

有关更多信息，请参见以下内容：

- 有关对 ZFS 文件设置 ACL 的说明，请参见 chmod(1) 手册页。
- 有关文件权限的概述，请参见《Oracle Solaris 管理：安全服务》中的“使用 UNIX 权限保护文件”。
- 有关保护 ZFS 文件的概述和示例，请参见《Oracle Solaris 管理：ZFS 文件系统》中的第 8 章 “使用 ACL 和属性保护 Oracle Solaris ZFS 文件”以及手册页。

包过滤

包过滤可提供基本的保护以防止基于网络的攻击。Oracle Solaris 包括 IP 过滤器功能和 TCP 包装。

IP 过滤器

Oracle Solaris 的 IP 过滤器功能可创建一个防火墙以抵御基于网络的攻击。

具体来说，IP 过滤器提供有状态包过滤功能，可按照 IP 地址或网络、端口、协议、网络接口以及通信方向对包进行过滤。它还包括无状态包过滤以及创建和管理地址池的功能。此外，IP 过滤器还具有执行网络地址转换 (network address translation, NAT) 和端口地址转换 (port address translation, PAT) 的功能。

有关更多信息，请参见以下内容：

- 所选手册页包括 ipfilter(5)、ipf(1M)、ipnat(1M)、svc.ipfd(1M) 和 ipf(4)。
- 有关 IP 过滤器的概述，请参见《Oracle Solaris 管理：IP 服务》中的第 20 章 “Oracle Solaris 中的 IP 过滤器（概述）”。
- 有关使用 IP 过滤器的示例，请参见《Oracle Solaris 管理：IP 服务》中的第 21 章 “IP 过滤器（任务）”以及手册页。
- 有关 IP 过滤器策略语言的语法的信息和示例，请参见 ipnat(4) 手册页。

TCP 包装

TCP 包装提供了一种实现访问权控制的方法，即根据 ACL 检查请求特定网络服务的主机的地址。请求将相应地被授权或拒绝。TCP 包装还会记录网络服务的主机请求，这是一种非常有用的监视功能。可配置 Oracle Solaris 的安全 Shell 和 sendmail 功能以使用 TCP 包装。可能受到访问控制的网络服务包括 ftpd 和 rpcbind。

TCP 包装支持一种丰富的配置策略语言，从而使组织不仅可以全局指定安全策略，还可以基于每个服务指定安全策略。可根据主机名、IPv4 或 IPv6 地址、网络组名称、网络甚至 DNS 域允许或限制对服务的进一步访问。

有关更多信息，请参见以下内容：

- 有关 TCP 包装的信息，请参见《Oracle Solaris 管理：IP 服务》中的“如何使用 TCP 包装控制对 TCP 服务的访问”。
- 有关 TCP 包装的访问控制语言的语法的信息和示例，请参见 `hosts_access`(4) 手册页。

口令和口令约束

强用户口令有助于抵御涉及暴力破解猜测的攻击。

Oracle Solaris 具有许多可用于提升强用户口令的功能。可设置口令长度、内容、更改频率以及修改要求，并可保留口令历史记录。提供了要避免使用的口令的口令字典。还提供了多个可能的口令算法。

有关更多信息，请参见以下内容：

- 《Oracle Solaris 管理：安全服务》中的“维护登录控制”
- 《Oracle Solaris 管理：安全服务》中的“保证登录和口令的安全（任务）”
- 所选手册页包括 `passwd`(1) 和 `crypt.conf`(4)。

可插拔验证模块

使用可插拔验证模块 (Pluggable Authentication Module, PAM) 框架，可以协调和配置帐户、凭证、会话和口令的用户验证要求。

通过 PAM 框架，组织可定制用户验证体验以及帐户、会话和口令管理功能。系统登录服务（例如 `login` 和 `ftp`）使用 PAM 框架确保系统的所有入口点均已受到安全保护。通过该体系结构，在字段中替换或修改验证模块可防止系统受到任何新发现的漏洞的威胁，而无需更改使用 PAM 框架的任何系统服务。

有关更多信息，请参见以下内容：

- 《Oracle Solaris 管理：安全服务》中的第 15 章 “使用 PAM”
- `pam.conf`(4) 手册页

Oracle Solaris 中的特权

特权是针对内核中强制执行的进程的细粒度单项权利。Oracle Solaris 定义了 80 多项特权，从基本特权（例如 `file_read`）到更为专业的特权（例如 `proc_clock_highres`）。可将特权授予命令、用户、角色或系统。许多 Oracle Solaris 命令和守护进程仅使用执行其任务所需的特权运行。使用特权又称为**进程权限管理**。

能够识别特权的程序可防止入侵者获取超过程序本身使用的更多特权。此外，利用特权，组织可以限制要授予其系统上运行的服务和进程的特权。

有关更多信息，请参见以下内容：

- 《Oracle Solaris 管理：安全服务》中的“特权（概述）”
- 《Oracle Solaris 管理：安全服务》中的“使用特权（任务）”
- 《Oracle Solaris 11 开发者安全性指南》中的第 2 章 “开发特权应用程序”
- 所选手册页包括 `ppriv(1)` 和 `privileges(5)`。

远程访问

远程访问攻击可能会损坏系统和网络。在当今的 Internet 环境中，确保网络访问安全是必不可少的，甚至在 WAN 和 LAN 环境中也非常有用。

IPsec 和 IKE

IP 安全 (IP security, IPsec) 通过对包进行验证和/或加密来保护 IP 包。Oracle Solaris 对 IPv4 和 IPv6 均支持 IPsec。由于 IPsec 在应用层下得到了很好的实现，因此 Internet 应用程序可充分利用 IPsec，而无需修改其代码。

IPsec 及其密钥交换协议 IKE 使用加密框架中的算法。此外，加密框架还为使用 metaslot 的应用程序提供了一个 softtoken 密钥库。将 IKE 配置为使用 metaslot 时，组织可选择在磁盘上、已连接的硬件密钥库上或在 softtoken 密钥库中存储密钥。

若管理得当，IPsec 是保证网络通信安全的有效工具。

有关更多信息，请参见以下内容：

- 《Oracle Solaris 管理：IP 服务》中的第 14 章 “IP 安全体系结构（概述）”
- 《Oracle Solaris 管理：IP 服务》中的第 15 章 “配置 IPsec（任务）”
- 《Oracle Solaris 管理：IP 服务》中的第 17 章 “Internet 密钥交换（概述）”
- 《Oracle Solaris 管理：IP 服务》中的第 18 章 “配置 IKE（任务）”
- 所选手册页包括 `ipsecconf(1M)` 和 `in.iked(1M)`。

安全 Shell

通过 Oracle Solaris 的安全 Shell 功能，用户或服务可通过加密信道在远程系统之间访问或传输文件。在安全 Shell 中，所有网络通信都已加密。安全 Shell 还可用作即时请求的虚拟专用网络 (virtual private network, VPN)，从而可通过已验证的加密网络链路在本地系统和远程系统之间转发 X 窗口系统通信或者连接各个端口号。

因此，安全 Shell 可防止潜在入侵者读取拦截的通信，并防止有敌意的人欺骗系统。缺省情况下，安全 Shell 是新安装系统上唯一活动的远程访问机制。

有关更多信息，请参见以下内容：

- 《Oracle Solaris 管理：安全服务》中的第 17 章 “使用 安全 Shell（任务）”
- 所选手册页包括 `ssh(1)`、`sshd(1M)`、`sshd_config(4)` 和 `ssh_config(4)`。

Kerberos 服务

Oracle Solaris 的 Kerberos 功能甚至支持通过运行 Kerberos 服务的异构网络执行单点登录和安全事务。

Kerberos 基于麻省理工学院 (Massachusetts Institute of Technology, MIT) 开发的 Kerberos V5 网络验证协议。Kerberos 服务是一种客户机/服务器的体系结构，用于通过网络提供安全事务。该服务可提供功能强大的用户验证以及完整性和保密性。使用 Kerberos 服务，只需一次登录即可安全访问其他系统、执行命令、交换数据以及传输文件。此外，通过该服务，管理员还可以限制对服务和系统的访问。

有关更多信息，请参见以下内容：

- 《Oracle Solaris 管理：安全服务》中的第 VI 部分, “Kerberos 服务”
- 所选手册页包括 `kerberos(5)` 和 `kinit(1)`。

基于角色的访问控制

RBAC 允许组织根据用户或角色的独特需要和要求选择性地向其授予管理权限，从而应用最小特权安全原则。

Oracle Solaris 的基于角色的访问控制 (role-based access control, RBAC) 功能控制用户对通常限于 `root` 角色的任务的访问。通过对进程和用户应用安全属性，RBAC 可以在多个管理员之间分布管理权限。RBAC 又称为**用户权限管理**。

有关更多信息，请参见以下内容：

- 《Oracle Solaris 管理：安全服务》中的第 III 部分, “角色、权限配置文件和特权”
- 所选手册页包括 `rbac(5)`、`roleadd(1M)`、`profiles(1)` 和 `user_attr(4)`。

服务管理工具

使用 Oracle Solaris 的服务管理工具 (Service Management Facility, SMF) 功能可添加、删除、配置和管理服务。SMF 使用 RBAC 控制对系统上的服务管理功能的访问。具体来说，SMF 使用授权确定可管理服务的用户以及该用户可执行的功能。

通过 SMF，组织可以控制对服务的访问，以及控制启动、停止和刷新这些服务的方式。

有关更多信息，请参见以下内容：

- 《Oracle Solaris 管理：常见任务》中的第 6 章 “管理服务（概述）”
- 《Oracle Solaris 管理：常见任务》中的第 7 章 “管理服务（任务）”
- 所选手册页包括 `svcadm(1M)`、`svcs(1)` 和 `smf(5)`。

Oracle Solaris ZFS 文件系统

ZFS 是 Oracle Solaris 11 的缺省文件系统。ZFS 文件系统从根本上更改了 Oracle Solaris 文件系统的管理方式。ZFS 强健、可伸缩，且易于管理。由于 ZFS 中的文件系统创建是轻量级的，因此可轻松建立配额和保留空间。UNIX 权限、ACE 保护文件以及 RBAC 支持 ZFS 数据集的委托管理。

有关更多信息，请参见以下内容：

- 《Oracle Solaris 管理：ZFS 文件系统》中的第 1 章 “Oracle Solaris ZFS 文件系统（介绍）”
- 《Oracle Solaris 管理：ZFS 文件系统》中的第 3 章 “Oracle Solaris ZFS 与传统文件系统之间的差别”
- 《Oracle Solaris 管理：ZFS 文件系统》中的第 6 章 “管理 Oracle Solaris ZFS 文件系统”
- 所选手册页包括 `zfs(1M)` 和 `zfs(7FS)`。

Oracle Solaris Zones

使用 Oracle Solaris Zones 软件分区技术，可以在共享硬件资源的同时维护每个服务器一个应用程序的部署模型。

区域是虚拟化操作环境，通过这些环境，多个应用程序可在同一物理硬件上彼此隔离运行。这种隔离可防止某个区域内运行的进程监视或影响其他区域内运行的进程、查看彼此的数据或处理底层硬件。区域还提供了一个抽象层，将应用程序与系统上部署的物理属性（例如物理设备路径和网络接口名称）隔离开来。

有关更多信息，请参见以下内容：

- 《Oracle Solaris 管理：Oracle Solaris Zones、Oracle Solaris 10 Zones 和资源管理》中的第 II 部分, “Oracle Solaris Zones”
- 所选手册页包括 `brands(5)`、`zoneadm(1M)` 和 `zonecfg(1M)`。

Trusted Extensions

Oracle Solaris 的 Trusted Extensions 功能是安全标记技术的可选启用层，该技术支持将数据安全策略与数据所有权分离。Trusted Extensions 支持基于所有权的传统自主访问控制 (discretionary access control, DAC) 策略以及基于标签的强制访问控制 (mandatory access control, MAC) 策略。如果不启用 Trusted Extensions 层，则所有标签均相等，因此不会将内核配置为强制执行 MAC 策略。启用基于标签的 MAC 策略时，将通过比较与请求访问权限的进程（主体）和包含数据的对象关联的标签来限制所有数据流。与其他大多数多级别操作系统不同，Trusted Extensions 包括一个多级别桌面。

Trusted Extensions 符合通用准则有标签的安全保护配置文件 (Labeled Security Protection Profile, LSPP)、基于角色的访问保护配置文件 (Role-Based Access Protection Profile, RBACPP) 以及受控访问保护配置文件 (Controlled Access Protection Profile, CAPP) 的要求。但 Trusted Extensions 实现的独特之处在于，能够在最大限度地提高兼容性和最大限度地减少开销的同时提供高级别的保证。

有关更多信息，请参见以下内容：

- 有关配置和维护 Trusted Extensions 的信息，请参见《Trusted Extensions 配置和管理》。
- 有关使用多级别桌面的信息，请参见《Trusted Extensions 用户指南》。
- 所选手册页包括 `trusted_extensions(5)` 和 `labeld(1M)`。

Oracle Solaris 11 安全缺省设置

安装后，Oracle Solaris 可防止系统被入侵并可监视登录尝试，同时还提供其他安全功能。

系统访问受限制和监视

初始用户帐户和 root 角色帐户 – 初始用户帐户可以从控制台登录。为该帐户指定了 root 角色。这两个帐户的口令最初是相同的。

- 登录后，初始用户可承担 root 角色对系统进行进一步配置。承担角色后，系统将提示用户更改 root 口令。请注意，没有角色可以直接登录，包括 root 角色。
- 在 /etc/security/policy.conf 文件中为初始用户指定了缺省设置。缺省设置包括 "Basic Solaris User"（基本 Solaris 用户）权限配置文件和 "Console User"（控制台用户）权限配置文件。通过这些权限配置文件，用户可以读取和写入 CD 或 DVD，在没有特权的系统上运行任何命令，并在控制台中停止和重新启动系统。
- 还为初始用户帐户指定了 "System Administrator"（系统管理员）权限配置文件。因此，在不承担 root 角色的情况下，初始用户具有一些管理权限，如安装软件和管理命名服务的权限。

口令要求 – 用户口令长度必须至少为六个字符，且至少包含一个字母字符和一个数字字符。口令通过 SHA256 算法进行散列处理。更改口令时，所有用户（包括 root 角色）必须遵守这些口令要求。

受限网络访问 – 安装后，可保护系统免受网络入侵。允许初始用户通过使用 ssh 协议的已验证加密连接进行远程登录。这是唯一一个接受传入包的网络协议。ssh 密钥通过 AES128 算法进行包装。进行加密和验证后，用户访问系统时不会遭到拦截、修改或欺骗。

记录的登录尝试 – 为所有 login/logout 事件（登录、注销、切换用户、启动和停止 ssh 会话以及屏幕锁定）和所有无归属（失败）登录启用审计服务。由于 root 角色无法登

录，因此可在审计迹中跟踪充当 root 的用户的名称。初始用户可根据通过 "System Administrator"（系统管理员）权限配置文件授予的权限查看审计日志。

内核、文件和桌面保护已就位

初始用户登录后，内核、文件系统和桌面应用程序受最小特权、权限和基于角色的访问控制 (role-based access control, RBAC) 保护。

内核保护 – 对于许多守护进程和管理命令，只为它们指定了使它们能够成功执行所必需的特权。许多守护进程通过没有 root (UID=0) 特权的特殊管理帐户运行，因此它们不会被劫持转而执行其他任务。这些特殊管理帐户无法登录。设备受特权保护。

文件系统 – 缺省情况下，所有文件系统均为 ZFS 文件系统。用户的 umask 是 022，因此当某个用户创建新文件或目录时，仅允许该用户对其进行修改。允许用户组的成员读取和搜索目录以及读取文件。用户组之外的登录可列出目录并读取文件。目录权限为 drwxr-xr-x (755)。文件权限为 -rw-r--r-- (644)。

桌面 applet – 桌面 applet 受 RBAC 保护。例如，只有初始用户或 root 角色可以使用软件包管理器 applet 安装新软件包。对于没有为其指定使用软件包管理器权限的一般用户，不显示软件包管理器。

其他安全功能已工作

Oracle Solaris 11 提供了可用于配置系统和用户以满足站点安全要求的安全功能。

- **基于角色的访问控制 (role-based access control, RBAC)** – Oracle Solaris 提供了大量授权、特权和权限配置文件。root 是唯一定义的角色。权限配置文件为您创建的角色提供了良好的基础。此外，一些管理命令需要 RBAC 授权才能成功执行。没有授权的用户无法运行命令，即使这些用户具有所需的特权。
- **用户权限** – 在 /etc/security/policy.conf 文件中为用户指定了基本特权集、权限配置文件和授权，就如同第 17 页中的 “系统访问受限制和监视”中介绍的初始用户一样。用户登录尝试不受限制，但审计服务会记录所有失败的登录。
- **系统文件保护** – 系统文件受文件权限保护。只有 root 角色可以修改系统配置文件。

站点安全策略和做法

对于安全系统或系统网络，站点必须具有适当的安全策略以及支持该策略的安全做法。

有关更多信息，请查看以下内容：

- 《Trusted Extensions 配置和管理》中的附录 A “站点安全策略”
- 《Trusted Extensions 配置和管理》中的“安全要求实施”
- Keeping Your Code Secure (`http://blogs.oracle.com/maryanndavidson/entry/those_who_can_t_do`)

◆ ◆ ◆ 第 2 章

2 配置 Oracle Solaris 11 安全

本章介绍了配置系统安全时所需执行的操作。其内容涵盖了如何安装软件包、配置系统自身、配置各种子系统以及您可能需要的其他应用程序（例如 IPsec）。

安装 Oracle Solaris OS

安装 Oracle Solaris OS 时，请选择安装相应**组**软件包的介质。

- **Oracle Solaris Large Server** – 自动化安装程序 (Automated Installer, AI) 安装中的缺省清单和文本安装程序将安装 `group/system/solaris-large-server` 组，该组提供 Oracle Solaris 大型服务器环境。
- **Oracle Solaris Desktop** – Live Media 将安装 `group/system/solaris-desktop` 组，该组提供 Oracle Solaris 11 桌面环境。

  要创建供集中使用的桌面系统，请将 `group/feature/multi-user-desktop` 组添加到 Oracle Solaris 服务器。有关更多信息，请参见Optimizing the Oracle Solaris 11 Desktop for a Multiuser Environment一文。

有关使用自动化安装程序 (Automated Installer, AI) 的自动化安装，请参见《安装 Oracle Solaris 11 系统》中的第 III 部分, “使用安装服务器安装”。

请参见如下安装指南选择介质：

- 《安装 Oracle Solaris 11 系统》
- 《创建定制 Oracle Solaris 11 安装映像》
- 《添加和更新 Oracle Solaris 11 软件包》

确保系统安全

最好按顺序执行以下任务。此时，Oracle Solaris 11 OS 已安装，只有可承担 root 角色的初始用户才有权访问系统。

任务	说明	参考
1. 检验系统上的软件包。	检查安装介质中的软件包是否与已安装软件包相同。	第 22 页中的 “检验软件包”
2. 保护系统上的硬件设置。	要求输入口令才能更改硬件设置，以保护硬件。	《Oracle Solaris 管理：安全服务》中的“控制对系统硬件的访问（任务）”
3. 禁用不需要的服务。	阻止运行不属于系统必需功能的进程。	第 23 页中的 “禁用不需要的服务”
4. 要求进行设备分配。	阻止使用没有明确授权的可移除介质。设备包括麦克风、USB 驱动器和 CD。	《Oracle Solaris 管理：安全服务》中的“如何启用设备分配”
5. 阻止工作站所有者关闭系统电源。	阻止控制台用户关闭或暂停系统。	第 23 页中的 “为用户删除电源管理功能”
6. 创建用于反映站点安全策略的登录警告消息。	通知用户和潜在攻击者：系统处于受监视状态。	第 24 页中的 “在标题文件中放置安全消息” 第 24 页中的 “在桌面登录屏幕中放置安全消息”

▼ 检验软件包

安装后立即通过检验软件包来验证安装。

开始之前 您必须是 root 角色。

1. **运行 pkg verify 命令。**

   要保留记录，请将命令输出发送到某个文件。

   ```
   # pkg verify > /var/pkgverifylog
   ```

2. **查看日志中是否存在错误。**

3. **如果发现错误，则通过介质重新进行安装或修复错误。**

另请参见 有关更多信息，请参见 pkg(1) 和 pkg(5) 手册页。这些手册页中包含使用 pkg verify 命令的示例。

▼ 禁用不需要的服务

使用此过程可禁用系统不需要的服务。

开始之前 您必须是 root 角色。

1. **列出联机服务。**

```
# svcs | grep network
online         Sep_07   svc:/network/loopback:default
...
online         Sep_07   svc:/network/ssh:default
```

2. **禁用此系统不需要的服务。**

   例如，如果系统不是 NFS 服务器或 Web 服务器，而服务处于联机状态，则禁用这些服务。

```
# svcadm disable svc:/network/nfs/server:default
# svcadm disable svc:/network/http:apache22
```

另请参见 有关更多信息，请参见《Oracle Solaris 管理：常见任务》中的第 6 章“管理服务（概述）”和 svcs(1) 手册页。

▼ 为用户删除电源管理功能

使用此过程可阻止此系统的用户暂停系统或关闭系统电源。

开始之前 您必须是 root 角色。

1. **查看 "Console User"（控制台用户）权限配置文件的内容。**

```
% getent prof_attr | grep Console
Console User:RO::Manage System as the Console User:
profiles=Desktop Removable Media User,Suspend To RAM,Suspend To Disk,
Brightness,CPU Power Management,Network Autoconf User;
auths=solaris.system.shutdown;help=RtConsUser.html
```

2. **创建一个权限配置文件，该权限配置文件包括 "Console User"（控制台用户）配置文件中您希望用户保留的任何权限。**

   有关说明，请参见《Oracle Solaris 管理：安全服务》中的“如何创建或更改权限配置文件”。

3 **在 /etc/security/policy.conf 文件中注释掉 "Console User"（控制台用户）权限配置文件。**

```
#CONSOLE_USER=Console User
```

4 **将您在步骤 2 中创建的权限配置文件指定给用户。**

```
# usermod -P +new-profile username
```

另请参见 有关更多信息，请参见《Oracle Solaris 管理：安全服务》中的“policy.conf 文件”以及 policy.conf(4) 和 usermod(1M) 手册页。

▼ 在标题文件中放置安全消息

使用此过程可创建用于反映站点安全策略的警告消息。这些文件的内容将在本地和远程登录时显示。

注 – 此过程中的样例消息不满足美国政府要求，也可能不满足您的安全策略。

开始之前 您必须是 root 角色。最佳做法是就安全消息的内容向贵公司的法律顾问进行咨询。

1 **在 /etc/issue 文件中键入安全消息。**

```
# vi /etc/issue
      ALERT   ALERT   ALERT   ALERT   ALERT

This machine is available to authorized users only.

If you are an authorized user, continue.

Your actions are monitored, and can be recorded.
```

有关更多信息，请参见 issue(4) 手册页。

telnet 程序将 /etc/issue 文件的内容显示为登录消息。有关其他应用程序使用该文件的信息，请参见第 33 页中的 “向 ssh 和 ftp 用户显示安全消息”和第 24 页中的 “在桌面登录屏幕中放置安全消息”。

2 **在 /etc/motd 文件中添加安全消息。**

```
# vi /etc/motd
This system serves authorized users only. Activity is monitored and reported.
```

▼ 在桌面登录屏幕中放置安全消息

从多种方法中选择一种来创建供用户在登录时查看的安全消息。

有关更多信息，请在桌面上单击 "System"（系统）> "Help"（帮助）菜单以启动 GNOME 帮助浏览器。您也可以使用 `yelp` 命令。在 `gdm`(1M) 手册页的“`GDM Login Scripts and Session Files`”（GDM 登录脚本和会话文件）部分介绍了桌面登录脚本。

注 – 此过程中的样例消息不满足美国政府要求，也可能不满足您的安全策略。

开始之前 您必须是 `root` 角色。最佳做法是就安全消息的内容向贵公司的法律顾问进行咨询。

- **在桌面登录屏幕中放置安全消息。**

  您有几种选择。创建对话框的这几种方式都可以使用第 24 页中的 “在标题文件中放置安全消息”的步骤 1 中的 `/etc/issue` 文件。

  - **选项 1：创建用户登录时在对话框中显示安全消息的桌面文件。**

    ```
    # vi /usr/share/gdm/autostart/LoginWindow/banner.desktop
    [Desktop Entry]
    Type=Application
    Name=Banner Dialog
    Exec=/usr/bin/zenity --text-info --width=800 --height=300 \
    --title="Security Message" \
    --filename=/etc/issue
    OnlyShowIn=GNOME;
    X-GNOME-Autostart-Phase=Application
    ```

    在登录窗口中进行验证后，用户必须关闭该对话框才能访问工作区。有关 `zenity` 命令的选项，请参见 `zenity`(1) 手册页。

  - **选项 2：修改 GDM 初始化脚本以在对话框中显示安全消息。**

    `/etc/gdm` 目录包含三个初始化脚本，它们分别在桌面登录之前、登录期间以及登录后显示安全消息。Oracle Solaris 10 版本中也提供了这些脚本。

    - **在出现登录屏幕之前显示安全消息。**

      ```
      # vi /etc/gdm/Init/Default
      /usr/bin/zenity --text-info --width=800 --height=300 \
      --title="Security Message" \
      --filename=/etc/issue
      ```

    - **验证后在登录屏幕上显示安全消息。**

      此脚本在显示用户工作区之前运行。可修改 `Default.sample` 脚本来创建此脚本。

      ```
      # vi /etc/gdm/PostLogin/Default
      /usr/bin/zenity --text-info --width=800 --height=300 \
      --title="Security Message" \
      --filename=/etc/issue
      ```

    - **验证后在用户的初始工作区中显示安全消息。**

      ```
      # vi /etc/gdm/PreSession/Default
      /usr/bin/zenity --text-info --width=800 --height=300 \
      ```

```
--title="Security Message" \
--filename=/etc/issue
```

注 – 可将该对话框包含在用户工作区的窗口中。

- **选项 3：修改登录窗口以在输入字段上方显示安全消息。**
  登录窗口将扩大以容纳您的消息。此方法不指向 `/etc/issue` 文件。必须将文本键入 GUI。

  注 – 登录窗口 `gdm-greeter-login-window.ui` 将被 `pkg fix` 和 `pkg update` 命令覆盖。要保存更改，请将文件复制到配置文件目录，并在升级系统后将更改与新文件合并。有关更多信息，请参见 `pkg(5)` 手册页。

  a. **将目录转到登录窗口用户界面。**

     ```
     # cd /usr/share/gdm
     ```

  b. **可选保存原始登录窗口 UI 的副本。**

     ```
     # cp gdm-greeter-login-window.ui /etc/gdm/gdm-greeter-login-window.ui.orig
     ```

  c. **使用 GNOME 工具包接口设计程序向登录窗口添加标签。**
     `glade-3` 程序将打开 GTK+ 接口设计程序。将安全消息键入在用户输入字段上方显示的标签。

     ```
     # /usr/bin/glade-3 /usr/share/gdm/gdm-greeter-login-window.ui
     ```

     要查看接口设计程序的指南，请在 GNOME 帮助浏览器中单击 "Development"（开发）。`glade-3(1)` 手册页列在 "Manual Pages"（手册页）的 "Applications"（应用程序）下。

  d. **可选修改登录窗口 GUI 后，保存副本。**

     ```
     # cp gdm-greeter-login-window.ui /etc/gdm/gdm-greeter-login-window.ui.site
     ```

示例 2–1 创建桌面登录时显示的简短警告消息

在本示例中，管理员键入一条简短消息作为桌面文件中 `zenity` 命令的参数。管理员还使用 `--warning` 选项在消息中显示警告图标。

```
# vi /usr/share/gdm/autostart/LoginWindow/bannershort.desktop
[Desktop Entry]
Type=Application
Name=Banner Dialog
Exec=/usr/bin/zenity --warning --width=800  --height=150 --title="Security Message" \
--text="This system serves authorized users only. Activity is monitored and reported."
OnlyShowIn=GNOME;
X-GNOME-Autostart-Phase=Application
```

确保用户安全

此时，只有可承担 root 角色的初始用户才有权访问系统。最好按顺序执行以下任务，然后一般用户才可以登录。

任务	说明	参考
要求使用强口令并频繁更改口令。	增强每个系统上的缺省口令约束。	第 27 页中的 “设置更强的口令约束”
为一般用户配置有限制性的文件权限。	为一般用户的文件权限设置比 022 限制性更为严格的值。	第 29 页中的 “为一般用户设置限制性更为严格的 umask 值”。
为一般用户设置帐户锁定。	在不用于管理的系统上，设置系统范围的帐户锁定并减少激活锁定的登录次数。	第 28 页中的 “为一般用户设置帐户锁定”
预先选择其他审计类。	更好地监视和记录系统面临的潜在威胁。	第 30 页中的 “审计除登录/注销之外的重要事件”
向 syslog 实用程序发送审计事件的文本摘要。	提供对重要审计事件（例如，登录和尝试登录）的实时监视。	第 30 页中的 “实时监视 lo 事件”
创建角色。	向多个可信用户分发独立的管理任务，这样任一用户都不会损坏系统。	《Oracle Solaris 管理：常见任务》中的“设置用户帐户” 《Oracle Solaris 管理：安全服务》中的“如何创建角色” 《Oracle Solaris 管理：安全服务》中的“如何指定角色”。
仅在用户的桌面上显示允许的应用程序。	阻止用户查看或使用其无权使用的应用程序。	请参见《Trusted Extensions 配置和管理》中的“如何限定用户仅使用桌面应用程序”。
限制用户的特权。	删除用户不需要的基本特权。	第 31 页中的 “为用户删除不需要的基本特权”

▼ 设置更强的口令约束

如果缺省设置不满足您的站点安全要求，请使用此过程。相关步骤遵循 /etc/default/passwd 文件中的条目列表顺序执行。

开始之前 更改缺省设置之前，请确保更改后允许所有用户向其应用程序和网络上的其他系统进行验证。

您必须是 root 角色。

- 编辑 **/etc/default/passwd** 文件。

  a. 要求用户每个月都更改口令，但频率不能超过每三周更改一次。

  ```
  ## /etc/default/passwd
  ##
  MAXWEEKS=
  MINWEEKS=
  MAXWEEKS=4
  MINWEEKS=3
  ```

  b. 要求口令长度至少为八个字符。

  ```
  #PASSLENGTH=6
  PASSLENGTH=8
  ```

  c. 保留口令历史记录。

  ```
  #HISTORY=0
  HISTORY=10
  ```

  d. 要求与上一口令具有最小差异。

  ```
  #MINDIFF=3
  MINDIFF=4
  ```

  e. 要求至少有一个大写字母。

  ```
  #MINUPPER=0
  MINUPPER=1
  ```

  f. 要求至少有一个数字。

  ```
  #MINDIGIT=0
  MINDIGIT=1
  ```

另请参见

- 有关用于限制口令创建的变量列表，请参见 /etc/default/passwd 文件。该文件中指出了缺省设置。
- 有关在安装后生效的口令约束，请参见第 17 页中的“系统访问受限制和监视”。
- passwd(1) 手册页

▼ 为一般用户设置帐户锁定

使用此过程可在登录尝试失败特定次数后锁定一般用户帐户。

注 – 请勿对可以承担角色的用户设置帐户锁定，因为您可以锁定相应角色。

开始之前 您必须是 root 角色。请勿在用于管理活动的系统上在系统范围内设置此保护。

1. **将 LOCK_AFTER_RETRIES 安全属性设置为 YES。**

   - **在系统范围内设置。**

     ```
     # vi /etc/security/policy.conf
     ...
     #LOCK_AFTER_RETRIES=NO
     LOCK_AFTER_RETRIES=YES
     ...
     ```

   - **对每个用户设置。**

     ```
     # usermod -K lock_after_retries=yes username
     ```

2. **将 RETRIES 安全属性设置为 3。**

   ```
   # vi /etc/default/login
   ...
   #RETRIES=5
   RETRIES=3
   ...
   ```

另请参见

- 有关用户和角色安全属性的讨论，请参见《Oracle Solaris 管理：安全服务》中的第 10 章 “Oracle Solaris 中的安全属性（参考）”。
- 所选手册页包括 `policy.conf(4)` 和 `user_attr(4)`。

▼ 为一般用户设置限制性更为严格的 umask 值

如果缺省 `umask` 值 `022` 的限制性不够严格，请使用此过程设置限制性更为严格的掩码。

开始之前 您必须是 `root` 角色。

- **在各种 shell 的框架目录中修改登录配置文件中的 umask 值。**

  Oracle Solaris 为管理员提供了用于定制用户 shell 缺省值的目录。这些框架目录包括诸如 `.profile`、`.bashrc` 和 `.kshrc` 等文件。

  选择以下值之一：

  - `umask 027`－提供中等文件保护

    (`740`)－`w`（组），`rwx`（其他用户）
  - `umask 026`－提供稍严格的文件保护

    (`741`)－`w`（组），`rw`（其他用户）
  - `umask 077`－提供完整的文件保护

    (`700`)－组或其他用户无权访问

另请参见 有关更多信息，请参见以下内容：

- 《Oracle Solaris 管理：常见任务》中的“设置用户帐户”
- 《Oracle Solaris 管理：安全服务》中的“缺省 umask 值”
- 所选手册页包括 usermod(1M) 和 umask(1)。

▼ 审计除登录/注销之外的重要事件

使用此过程可以审计管理命令、侵入系统的尝试以及站点安全策略所指定的其他重要事件。

注 – 本过程中的示例可能不足以满足您的安全策略。

开始之前 您必须是 root 角色。您要实现与审计有关的站点安全策略。

1. **审计用户和角色对特权命令的所有使用情况。**

   对于所有用户和角色，将 AUE_PFEXEC 审计事件添加到其预选掩码中。

   ```
   # usermod -K audit_flags=lo,ps:no username

   # rolemod -K audit_flags=lo,ps:no rolename
   ```

2. **记录审计命令的参数。**

   ```
   # auditconfig -setpolicy +argv
   ```

3. **记录审计命令的执行环境。**

   ```
   # auditconfig -setpolicy +arge
   ```

另请参见

- 有关审计策略的信息，请参见《Oracle Solaris 管理：安全服务》中的“审计策略”。
- 有关设置审计标志的示例，请参见《Oracle Solaris 管理：安全服务》中的“配置审计服务（任务）”和《Oracle Solaris 管理：安全服务》中的“审计服务的故障排除（任务）”。
- 要配置审计，请参见 auditconfig(1M) 手册页。

▼ 实时监视 lo 事件

使用此过程可在您要监视的事件发生时为其激活 audit_syslog 插件。

开始之前 您必须承担 root 角色才能修改 syslog.conf 文件。其他步骤要求您分配有 "Audit Configuration"（审计配置）权限配置文件。

1. **将 lo 类发送到 audit_syslog 插件，并激活该插件。**

   ```
   # auditconfig -setplugin audit_syslog active p_flags=lo
   ```

2. **将 audit.notice 项添加到 syslog.conf 文件。**

   此缺省项包括日志文件的位置。

   ```
   # cat /etc/syslog.conf
   ...
   audit.notice       /var/adm/auditlog
   ```

3. **创建日志文件。**

   ```
   # touch /var/adm/auditlog
   ```

4. **刷新 syslog 服务的配置信息。**

   ```
   # svcadm refresh system/system-log
   ```

5. **刷新审计服务。**

   审计服务在刷新时将读取审计插件的更改。

   ```
   # audit -s
   ```

另请参见

- 要将审计摘要发送到其他系统，请参见《Oracle Solaris 管理：安全服务》中的“如何配置 syslog 审计日志”后的示例。
- 审计服务可生成大量输出。要管理日志，请参见 logadm(1M) 手册页。
- 要监视输出，请参见第 46 页中的 “监视 audit_syslog 审计摘要”。

▼ 为用户删除不需要的基本特权

在特殊情况下，可从一般用户的基本特权集中删除三种基本特权中的一个或多个特权。

- file_link_any－允许进程创建指向某个 UID 所拥有的文件的硬链接，但是该 UID 不能与该进程的有效 UID 相同。
- proc_info－允许进程检查它可以向其发送信号的进程以外的进程的状态。不能被检查的进程在 /proc 中不可见，并且似乎并不存在。
- proc_session－允许进程在其会话之外发送信号或跟踪进程。

开始之前 您必须是 root 角色。

1. **阻止用户链接到不归其所有的文件。**

   ```
   # usermod -K defaultpriv=basic,!file_link_any user
   ```

2. **阻止用户检查不归其所有的进程。**

   ```
   # usermod -K defaultpriv=basic,!proc_info user
   ```

3. **阻止用户从其当前会话启动第二个会话，例如启动 ssh 会话。**

   ```
   # usermod -K defaultpriv=basic,!proc_session user
   ```

4 **将所有三种特权从用户的基本特权集中删除。**

```
# usermod -K defaultpriv=basic,!file_link_any,!proc_info,!proc_session user
```

另请参见 有关更多信息，请参见《Oracle Solaris 管理：安全服务》中的第 8 章 “使用角色和特权（概述）”和 `privileges(5)` 手册页。

确保内核安全

此时，您可能已经创建了可承担角色的用户，且创建了角色。只有 `root` 角色可以修改系统文件。

任务	说明	参考
防止程序利用可执行栈。	设置用于防止利用缓冲区溢出（缓冲区溢出会利用可执行栈）的系统变量。	《Oracle Solaris 管理：安全服务》中的“防止可执行文件危及安全”
保护可能包含敏感信息的核心文件。	创建针对核心文件限定访问的目录。	《Oracle Solaris 管理：常见任务》中的“如何启用全局核心文件路径” 《Oracle Solaris 管理：常见任务》中的“管理核心文件（任务列表）”

配置网络

此时，您可能已经创建了可承担角色的用户，且创建了角色。只有 `root` 角色可以修改系统文件。

从以下网络任务中，根据您的站点要求执行可提供附加安全性的任务。这些网络任务可通知远程登录的用户：系统受到保护，这些网络任务还可增强 IP、ARP 和 TCP 协议。

任务	说明	参考
显示用于反映站点安全策略的警告消息。	通知用户和潜在攻击者：系统处于受监视状态。	第 33 页中的 “向 `ssh` 和 `ftp` 用户显示安全消息”
禁用网络路由选择守护进程。	限制可能存在的网络探查器访问系统。	第 34 页中的 “禁用网络路由选择守护进程”
防止散播有关网络拓扑的信息。	防止广播包。	第 35 页中的 “禁用广播包转发”
	阻止对广播回显请求和多播回显请求的响应。	第 35 页中的 “禁止响应回显请求”

任务	说明	参考
对于充当其他域的网关的系统（例如防火墙或 VPN 节点），打开严格的源和目标多宿主。	阻止其标头中没有网关地址的包在网关外移动。	第 36 页中的 “设置严格多宿主”
通过控制不完整系统连接的数量阻止 DOS 攻击。	限制 TCP 侦听器所允许的不完整 TCP 连接数。	第 36 页中的 “设置最大不完整 TCP 连接数”
通过控制允许的传入连接数阻止 DOS 攻击。	指定 TCP 侦听器的缺省最大暂挂 TCP 连接数。	第 37 页中的 “设置最大暂挂 TCP 连接数”
为初始 TCP 连接生成强随机数。	符合 RFC 1948 指定的序列号生成值。	第 37 页中的 “为初始 TCP 连接指定强随机数”
将网络参数恢复为安全的缺省值。	提高因管理操作而降低的安全性。	第 37 页中的 “将网络参数重置为安全值”
向网络服务添加 TCP 包装，以将应用程序限定为仅供合法用户使用。	指定允许访问网络服务（例如 FTP）的系统。 缺省情况下，`sendmail` 应用程序由 TCP 包装进行保护，如《Oracle Solaris 管理：网络服务》中的“sendmail 版本 8.12 支持 TCP 包装”中所述。	要为所有 `inetd` 服务启用 TCP 包装，请参见《Oracle Solaris 管理：IP 服务》中的“如何使用 TCP 包装控制对 TCP 服务的访问”。 有关保护 FTP 网络服务的 TCP 包装的示例，请参见《Oracle Solaris 管理：网络服务》中的“如何使用 SMF 启动 FTP 服务器”。

▼ 向 ssh 和 ftp 用户显示安全消息

使用以下过程在远程登录和文件传输时显示警告。

开始之前 您必须是 `root` 角色。在第 24 页中的 “在标题文件中放置安全消息”的步骤 1 中创建了 `/etc/issue` 文件。

1 要向使用 `ssh` 登录的用户显示安全消息，请执行以下操作：

a. 在 `/etc/sshd_config` 文件中取消对 Banner 指令的注释。

```
# vi /etc/ssh/sshd_config
# Banner to be printed before authentication starts.
Banner /etc/issue
```

b. 刷新 `ssh` 服务。

```
# svcadm refresh ssh
```

有关更多信息，请参见 `issue(4)` 和 `sshd_config(4)` 手册页。

2 **要向使用 ftp 登录的用户显示安全消息，请执行以下操作：**

a. **将 DisplayConnect 指令添加到 proftpd.conf 文件中。**

```
# vi /etc/proftpd.conf
# Banner to be printed before authentication starts.
DisplayConnect /etc/issue
```

b. **重新启动 ftp 服务。**

```
# svcadm restart ftp
```

有关更多信息，请参见 ProFTPD (http://www.proftpd.org/) Web 站点。

▼ 禁用网络路由选择守护进程

使用此过程可在安装后阻止网络路由，方法是指定缺省路由器。否则，请在手动配置路由后执行此过程。

注 – 许多网络配置过程都要求禁用路由选择守护进程。因此，您可能已在某个大型配置过程中禁用此守护进程。

开始之前 您必须分配有 "Network Management"（网络管理）权限配置文件。

1 **检验路由选择守护进程是否正在运行。**

```
# svcs -x svc:/network/routing/route:default
svc:/network/routing/route:default (in.routed network routing daemon)
 State: online since April 10, 2011 05:15:35 AM PDT
   See: in.routed(1M)
   See: /var/svc/log/network-routing-route:default.log
Impact: None.
```

如果服务未运行，则可在此处停止。

2 **禁用路由选择守护进程。**

```
# routeadm -d ipv4-forwarding -d ipv6-forwarding
# routeadm -d ipv4-routing -d ipv6-routing
# routeadm -u
```

3 **检验路由选择守护进程是否已被禁用。**

```
# svcs -x routing/route:default
svc:/network/routing/route:default (in.routed network routing daemon)
 State: disabled since April 11, 2011 10:10:10 AM PDT
Reason: Disabled by an administrator.
   See: http://sun.com/msg/SMF-8000-05
   See: in.routed(1M)
Impact: This service is not running.
```

另请参见 routeadm(1M) 手册页

▼ 禁用广播包转发

缺省情况下，Oracle Solaris 将转发广播包。如果您的站点安全策略要求您降低广播泛洪的可能性，请使用此过程更改缺省设置。

注 – 在禁用 `_forward_directed_broadcasts` 网络属性时，将禁用广播 ping。

开始之前 您必须分配有 "Network Management"（网络管理）权限配置文件。

1. **将 IP 包的广播包转发属性设置为 0。**

```
# ipadm set-prop -p _forward_directed_broadcasts=0 ip
```

2. **检验当前值。**

```
# ipadm show-prop -p _forward_directed_broadcasts ip
PROTO  PROPERTY                       PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip     _forward_directed_broadcasts   rw   0         --           0         0,1
```

另请参见 `ipadm(1M)` 手册页

▼ 禁止响应回显请求

使用此过程可防止散播有关网络拓扑的信息。

开始之前 您必须分配有 "Network Management"（网络管理）权限配置文件。

1. **将 IP 包对广播回显请求的响应属性设置为 0，然后检验当前值。**

```
# ipadm set-prop -p _respond_to_echo_broadcast=0 ip

# ipadm show-prop -p _respond_to_echo_broadcast ip
PROTO  PROPERTY                  PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip     _respond_to_echo_broadcast rw   0         --           1         0,1
```

2. **将 IP 包对多播回显请求的响应属性设置为 0，然后检验当前值。**

```
# ipadm set-prop -p _respond_to_echo_multicast=0 ipv4
# ipadm set-prop -p _respond_to_echo_multicast=0 ipv6

# ipadm show-prop -p _respond_to_echo_multicast ipv4
PROTO  PROPERTY                  PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv4   _respond_to_echo_multicast rw   0         --           1         0,1
# ipadm show-prop -p _respond_to_echo_multicast ipv6
PROTO  PROPERTY                  PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   _respond_to_echo_multicast rw   0         --           1         0,1
```

另请参见 有关更多信息，请参见《Oracle Solaris 可调参数参考手册》中的“_respond_to_echo_broadcast 和 _respond_to_echo_multicast（ipv4 或 ipv6）”和 `ipadm`(1M) 手册页。

▼ 设置严格多宿主

对于充当其他域的网关的系统（例如防火墙或 VPN 节点），使用此过程可打开严格多宿主。

Oracle Solaris 11 发行版为 IPv4 和 IPv6 引入了新的属性 `hostmodel`。此属性可控制 IP 包在多宿主系统上的发送和接收行为。

开始之前 您必须分配有 "Network Management"（网络管理）权限配置文件。

1. **将 IP 包的 `hostmodel` 属性设置为 `strong`。**

```
# ipadm set-prop -p hostmodel=strong ipv4
# ipadm set-prop -p hostmodel=strong ipv6
```

2. **检验当前值并注意可能的值。**

```
# ipadm show-prop -p hostmodel ip
PROTO  PROPERTY    PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   hostmodel   rw   strong    strong       weak      strong,src-priority,weak
ipv4   hostmodel   rw   strong    strong       weak      strong,src-priority,weak
```

另请参见 有关更多信息，请参见《Oracle Solaris 可调参数参考手册》中的“hostmodel（ipv4 或 ipv6）”和 `ipadm`(1M) 手册页。

有关严格多宿主使用情况的更多信息，请参见《Oracle Solaris 管理：IP 服务》中的“如何在隧道模式下使用 IPsec 保护 VPN”。

▼ 设置最大不完整 TCP 连接数

使用此过程可通过控制不完整的暂挂连接数阻止拒绝服务 (denial of service, DOS) 攻击。

开始之前 您必须分配有 "Network Management"（网络管理）权限配置文件。

1. **设置最大传入连接数。**

```
# ipadm set-prop -p _conn_req_max_q0=4096 tcp
```

2. **检验当前值。**

```
# ipadm show-prop -p _conn_req_max_q0 tcp
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
tcp    _conn_req_max_q0 rw   4096      --           128       1-4294967295
```

另请参见 有关更多信息，请参见《Oracle Solaris 可调参数参考手册》中的“_conn_req_max_q0”和 ipadm(1M) 手册页。

▼ 设置最大暂挂 TCP 连接数

使用此过程可通过控制允许的传入连接数阻止 DOS 攻击。

开始之前 您必须分配有 "Network Management"（网络管理）权限配置文件。

1. **设置最大传入连接数。**

```
# ipadm set-prop -p _conn_req_max_q=1024 tcp
```

2. **检验当前值。**

```
# ipadm show-prop -p _conn_req_max_q tcp
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
tcp    _conn_req_max_q  rw   1024      --           128       1-4294967295
```

另请参见 有关更多信息，请参见《Oracle Solaris 可调参数参考手册》中的“_conn_req_max_q”和 ipadm(1M) 手册页。

▼ 为初始 TCP 连接指定强随机数

以下过程设置 TCP 初始序列号生成参数以遵守 RFC 1948 (http://www.ietf.org/rfc/rfc1948.txt)。

开始之前 您必须承担 root 角色才能修改系统文件。

- **更改 TCP_STRONG_ISS 变量的缺省值。**

```
# vi /etc/default/inetinit
# TCP_STRONG_ISS=1
TCP_STRONG_ISS=2
```

▼ 将网络参数重置为安全值

许多缺省情况下安全的网络参数是可调的，因此可进行更改。如果站点条件允许，可将以下可调参数恢复为缺省值。

开始之前 您必须分配有 "Network Management"（网络管理）权限配置文件。参数的当前值不如缺省值安全。

1. **将 IP 包的源包转发属性设置为 0，然后检验当前值。**

   缺省值可阻止来自欺骗性包的 DOS 攻击。

```
# ipadm set-prop -p _forward_src_routed=0 ipv4
# ipadm set-prop -p _forward_src_routed=0 ipv6
# ipadm show-prop -p _forward_src_routed ipv4
PROTO  PROPERTY             PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv4   _forward_src_routed   rw   0         --           0         0,1
# ipadm show-prop -p _forward_src_routed ipv6
PROTO  PROPERTY             PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   _forward_src_routed   rw   0         --           0         0,1
```

   有关更多信息，请参见《Oracle Solaris 可调参数参考手册》中的“forwarding（ipv4 或 ipv6）”。

2. **将 IP 包的网络掩码响应属性设置为 0，然后检验当前值。**

   缺省值可防止散播有关网络拓扑的信息。

```
# ipadm set-prop -p _respond_to_address_mask_broadcast=0 ip
# ipadm show-prop -p _respond_to_address_mask_broadcast ip
PROTO PROPERTY                          PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip    _respond_to_address_mask_broadcast rw   0         --           0         0,1
```

3. **将 IP 包的时间戳响应属性设置为 0，然后检验当前值。**

   缺省值可删除系统上的其他 CPU 需求，并防止散播有关网络的信息。

```
# ipadm set-prop -p _respond_to_timestamp=0 ip
# ipadm show-prop -p _respond_to_timestamp ip
PROTO  PROPERTY                 PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip     _respond_to_timestamp    rw   0         --           0         0,1
```

4. **将 IP 包的广播时间戳响应属性设置为 0，然后检验当前值。**

   缺省值可删除系统上的其他 CPU 需求，并防止散播有关网络的信息。

```
# ipadm set-prop -p _respond_to_timestamp_broadcast=0 ip
# ipadm show-prop -p _respond_to_timestamp_broadcast ip
PROTO  PROPERTY                 PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip     _respond_to_timestamp_broadcast  rw   0         --           0         0,1
```

5. **将 IP 包的忽略重定向属性设置为 0，然后检验当前值。**

   缺省值可阻止系统上的其他 CPU 需求。

```
# ipadm set-prop -p _ignore_redirect=0 ipv4
# ipadm set-prop -p _ignore_redirect=0 ipv6
# ipadm show-prop -p _ignore_redirect ipv4
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv4   _ignore_redirect  rw   0         --           0         0,1
# ipadm show-prop -p _ignore_redirect ipv6
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   _ignore_redirect  rw   0         --           0         0,1
```

6. **阻止 IP 源路由。**

   如果需要 IP 源路由以进行诊断，则不要禁用此网络参数。

```
# ipadm set-prop -p _rev_src_routes=0 tcp
# ipadm show-prop -p _rev_src_routes tcp
```

```
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
tcp    _rev_src_routes  rw   0         --           0         0,1
```

有关更多信息，请参见《Oracle Solaris 可调参数参考手册》中的“_rev_src_routes”。

7 **将 IP 包的忽略重定向属性设置为 0，然后检验当前值。**

缺省值可阻止系统上的其他 CPU 需求。通常，在设计完善的网络上不需要重定向。

```
# ipadm set-prop -p _ignore_redirect=0 ipv4
# ipadm set-prop -p _ignore_redirect=0 ipv6
# ipadm show-prop -p _ignore_redirect ipv4
PROTO  PROPERTY          PERM  CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv4   _ignore_redirect  rw    0         --           0         0,1
# ipadm show-prop -p _ignore_redirect ipv6
PROTO  PROPERTY          PERM  CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   _ignore_redirect  rw    0         --           0         0,1
```

另请参见 `ipadm(1M)` 手册页

保护文件系统和文件

ZFS 文件系统是轻量级系统，可进行加密、压缩，并可为其配置保留空间和磁盘空间限制。

以下任务概述了 Oracle Solaris 的缺省文件系统 ZFS 中的可用保护。有关其他信息，请参见《Oracle Solaris 管理：ZFS 文件系统》中的“设置 ZFS 配额和预留空间”和 `zfs(1M)` 手册页。

任务	说明	参考
通过管理和保留磁盘空间阻止 DOS 攻击。	按文件系统、用户或组或者按项目指定对磁盘空间的使用。	《Oracle Solaris 管理：ZFS 文件系统》中的“设置 ZFS 配额和预留空间”
保证数据集及其后代所需的最小磁盘空间量。	按文件系统、用户或组或者按项目保证所需磁盘空间。	《Oracle Solaris 管理：ZFS 文件系统》中的“设置 ZFS 文件系统的预留空间”
加密文件系统上的数据。	使用加密以及创建数据集时设定用于访问数据集的口令短语来保护数据集。	《Oracle Solaris 管理：ZFS 文件系统》中的“加密 ZFS 文件系统” 《Oracle Solaris 管理：ZFS 文件系统》中的“加密 ZFS 文件系统的示例”
指定 ACL 以比一般 UNIX 文件权限更精确的粒度保护文件。	扩展安全属性可能对保护文件非常有用。 有关使用 ACL 的注意事项，请参见《Hiding Within the Trees》 (`http://www.usenix.org/publications/login/2004-02/pdfs/brunette.pdf`)（《在树内隐藏》）。	ZFS 端到端数据完整性 (`http://blogs.oracle.com/bonwick/entry/zfs_end_to_end_data`)

保护和修改文件

只有 root 角色可以修改系统文件。

任务	说明	参考
为一般用户配置有限制性的文件权限。	为一般用户的文件权限设置比 022 限制性更为严格的值。	第 29 页中的 “为一般用户设置限制性更为严格的 umask 值”
阻止使用未授权文件替换系统文件。	通过脚本或使用 BART 查找未授权文件。	《Oracle Solaris 管理：安全服务》中的“如何查找具有特殊文件权限的文件”

确保应用程序和服务安全

可以配置 Oracle Solaris 安全功能来保护应用程序。

创建区域以包含关键应用程序

区域是隔离进程的容器。它们是应用程序及其各部分的有用容器。例如，区域可用于将 Web 站点的数据库与站点的 Web 服务器隔离。

有关信息和过程，请参见以下内容：

- 《Oracle Solaris 管理：Oracle Solaris Zones、Oracle Solaris 10 Zones 和资源管理》中的第 15 章 “Oracle Solaris Zones 介绍”
- 《Oracle Solaris 管理：Oracle Solaris Zones、Oracle Solaris 10 Zones 和资源管理》中的“区域摘要（按功能）”
- 《Oracle Solaris 管理：Oracle Solaris Zones、Oracle Solaris 10 Zones 和资源管理》中的“非全局区域提供的功能”
- 《Oracle Solaris 管理：Oracle Solaris Zones、Oracle Solaris 10 Zones 和资源管理》中的“在系统上设置区域（任务列表）”
- 《Oracle Solaris 管理：Oracle Solaris Zones、Oracle Solaris 10 Zones 和资源管理》中的第 16 章 “非全局区域配置（概述）”
- 《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 数据库》）

管理区域中的资源

区域提供了许多用来管理区域资源的工具。

有关信息和过程，请参见以下内容：

- 《Oracle Solaris 管理：Oracle Solaris Zones、Oracle Solaris 10 Zones 和资源管理》中的第 14 章 “资源管理配置示例”
- 《Oracle Solaris 管理：Oracle Solaris Zones、Oracle Solaris 10 Zones 和资源管理》中的第 I 部分, “Oracle Solaris 资源管理”

配置 IPsec 和 IKE

IPsec 和 IKE 可保护节点与网络（使用 IPsec 和 IKE 联合配置）之间的网络传输。

有关信息和过程，请参见以下内容：

- 《Oracle Solaris 管理：IP 服务》中的第 14 章 “IP 安全体系结构（概述）”
- 《Oracle Solaris 管理：IP 服务》中的第 17 章 “Internet 密钥交换（概述）”
- 《Oracle Solaris 管理：IP 服务》中的第 15 章 “配置 IPsec（任务）”
- 《Oracle Solaris 管理：IP 服务》中的第 18 章 “配置 IKE（任务）”

配置 IP 过滤器

IP 过滤器功能可提供防火墙。

有关信息和过程，请参见以下内容：

- 《Oracle Solaris 管理：IP 服务》中的第 20 章 “Oracle Solaris 中的 IP 过滤器（概述）”
- 《Oracle Solaris 管理：IP 服务》中的第 21 章 “IP 过滤器（任务）”

配置 Kerberos

可以使用 Kerberos 服务保护您的网络。此客户机/服务器体系结构可通过网络提供安全事务。该服务可提供功能强大的用户验证以及完整性和保密性。使用 Kerberos 服务，可以安全登录到其他系统、执行命令、交换数据以及传输文件。此外，通过该服务，管理员还可以限制对服务和系统的访问。作为 Kerberos 用户，您可以控制其他用户对您帐户的访问。

有关信息和过程，请参见以下内容：

- 《Oracle Solaris 管理：安全服务》中的第 20 章 “规划 Kerberos 服务”
- 《Oracle Solaris 管理：安全服务》中的第 21 章 “配置 Kerberos 服务（任务）”

- 所选手册页包括 kadmin(1M)、pam_krb5(5) 和 kclient(1M)。

向传统服务添加 SMF

通过将应用程序添加到 Oracle Solaris 的服务管理工具 (Service Management Facility, SMF) 功能，可将应用程序限定为仅由可信用户或角色来配置。

有关信息和过程，请参见以下内容：

- 《Oracle Solaris 管理：安全服务》中的“如何为传统应用程序添加 RBAC 属性”
- Securing MySQL using SMF - the Ultimate Manifest (http://blogs.oracle.com/bobn/entry/securing_mysql_using_smf_the)（使用 SMF 保护 MySQL－最终清单）。
- 所选手册页包括 smf(5)、smf_security(5)、svcadm(1M) 和 svccfg(1M)。

创建系统的 BART 快照

配置系统后，可以创建一个或多个 BART 清单。这些清单可提供系统的快照。这样，您便可调度一般快照并进行比较。有关更多信息，请参见第 45 页中的“使用基本审计报告工具”。

添加多级别（有标签）安全

Trusted Extensions 通过执行强制访问控制 (mandatory access control, MAC) 策略扩展了 Oracle Solaris 安全。敏感标签将自动应用到所有数据源（网络、文件系统和窗口）和数据使用者（用户和进程）。基于数据（对象）标签和使用者（主体）之间的关系对所有数据的访问权进行限制。分层功能包括一组可识别标签的服务。

Trusted Extensions 服务的部分列表包括：

- 有标签联网
- 可识别标签的文件系统挂载和共享
- 有标签桌面
- 标签配置和转换
- 可识别标签的系统管理工具
- 可识别标签的设备分配

group/feature/trusted-desktop 软件包提供 Oracle Solaris 多级别的可信桌面环境。

配置 Trusted Extensions

必须先安装 Trusted Extensions 软件包，然后配置系统。软件包安装完成后，系统便可通过直接连接的位映射显示屏（如手提电脑或工作站）运行桌面。需要进行网络配置才能与其他系统进行通信。

有关信息和过程，请参见以下内容：

- 《Trusted Extensions 配置和管理》中的第 I 部分, “Trusted Extensions 的初始配置”
- 《Trusted Extensions 配置和管理》中的第 II 部分, “管理 Trusted Extensions”

配置有标签的 IPsec

可以使用 IPsec 保护您的有标签包。

有关信息和过程，请参见以下内容：

- 《Oracle Solaris 管理：IP 服务》中的第 14 章 “IP 安全体系结构（概述）”
- 《Trusted Extensions 配置和管理》中的“有标签 IPsec 的管理”
- 《Trusted Extensions 配置和管理》中的“配置有标签 IPsec（任务列表）”

◆ ◆ ◆ 第 3 章

3 监视和维护 Oracle Solaris 11 安全

Oracle Solaris 提供了两种系统工具来监视安全性，即基本审计报告工具 (Basic Audit Reporting Tool, BART) 功能和审计服务。各个程序和应用程序也可以创建访问日志和使用日志。

使用基本审计报告工具

BART 清单提供系统上已安装内容的静态记录。可以随着时间的推移在不同系统之间对 BART 清单进行比较，从而跟踪对已安装系统所做的更改和系统之间的差异。

有关信息和过程，请参见以下内容：

- 《Oracle Solaris 管理：安全服务》中的“基本审计报告工具（概述）”
- 《Oracle Solaris 管理：安全服务》中的“使用 BART（任务）”
- 《Oracle Solaris 管理：安全服务》中的“BART 清单、Rules 文件和报告（参考）”

有关跟踪对已安装系统所做更改的特定说明，请参见《Oracle Solaris 管理：安全服务》中的“如何比较同一个系统在一段时间内的清单”。

使用审计服务

审计保留系统使用情况的记录。审计服务包括帮助分析审计数据的工具。

《Oracle Solaris 管理：安全服务》中的第 VII 部分, “在 Oracle Solaris 中审计” 中对审计服务进行了介绍。

- 《Oracle Solaris 管理：安全服务》中的第 26 章 “审计（概述）”
- 《Oracle Solaris 管理：安全服务》中的第 27 章 “规划审计”

- 《Oracle Solaris 管理：安全服务》中的第 28 章“管理审计（任务）”
- 《Oracle Solaris 管理：安全服务》中的第 29 章“审计（参考）”

  有关手册页及其链接的列表，请参见《Oracle Solaris 管理：安全服务》中的“审计服务手册页”。

以下审计服务过程可能对满足站点要求有所帮助：

- 创建单独的角色以配置审计、检查审计以及启动和停止审计服务。

  将 "Audit Configuration"（审计配置）、"Audit Review"（审计检查）和 "Audit Control"（审计控制）权限配置文件用作角色的基础。

  要创建角色，请参见《Oracle Solaris 管理：安全服务》中的“如何创建角色”。
- 在 `syslog` 实用程序中监视已审计事件的文本摘要。

  激活 `audit_syslog` 插件，然后监视报告的事件。

  请参见《Oracle Solaris 管理：安全服务》中的“如何配置 syslog 审计日志”。
- 限定审计文件的大小。

  将 `audit_binfile` 插件的 `p_fsize` 属性设置为有用的大小。考虑您的检查调度、磁盘空间、`cron` 作业频率以及其他因素。

  例如，请参见《Oracle Solaris 管理：安全服务》中的“如何为审计迹指定审计空间”。
- 在单独的 ZFS 池上调度完整审计文件到审计检查文件系统的安全传输。
- 查看审计检查文件系统上的完整审计文件。

监视 audit_syslog 审计摘要

通过 `audit_syslog` 插件，可以记录预选审计事件的摘要。

可以在终端窗口中显示审计摘要，因为它们是通过运行类似如下的命令生成的：

```
# tail -0f /var/adm/auditlog
```

查看并归档审计日志

可以采用文本格式或在浏览器中采用 XML 格式查看审计记录。

有关信息和过程，请参见以下内容：

- 《Oracle Solaris 管理：安全服务》中的“审计日志”
- 《Oracle Solaris 管理：安全服务》中的“如何防止审计迹溢出”
- 《Oracle Solaris 管理：安全服务》中的“在本地系统上管理审计记录（任务）”

查找未授权文件

可以查找程序上 `setuid` 和 `setgid` 权限的潜在未授权使用情况。可疑可执行文件为用户而不是系统帐户（例如 `root` 或 `bin`）授予所有权。

有关过程和示例，请参见《Oracle Solaris 管理：安全服务》中的“如何查找具有特殊文件权限的文件”。

◆ ◆ ◆ 附 录 A

Oracle Solaris 安全的参考书目

以下参考文档包含有用的 Oracle Solaris 系统安全信息。早期发行版的 Oracle Solaris OS 中的安全信息中，部分信息仍然有用，还有部分信息已经过时。

Oracle Solaris 11 参考文档

以下书籍和文章包含有关 Oracle Solaris 11 系统的安全介绍：

- 《Oracle Solaris 管理：安全服务》

  此安全指南由 Oracle 出版，面向 Oracle Solaris 11 管理员。此指南描述了 Oracle Solaris 的安全功能以及在配置系统时如何使用这些功能。前言部分包含指向其他可能包含安全信息的 Oracle Solaris 系统管理指南的链接。

- 《Oracle Solaris Security: Oracle Solaris Express》(`http://www.oracle.com/technetwork/articles/servers-storage-admin/os11esecurity-186797.pdf`)（《Oracle Solaris 安全：Oracle Solaris Express》）

  本文提供了此发行版 2010 年 11 月版的 Oracle Solaris 安全功能的快照。

- 《ORACLE SOLARIS 11 EXPRESS 2010.11 WHAT'S NEW》(`http://www.oracle.com/technetwork/server-storage/solaris11/documentation/solaris-express-whatsnew-201011-175308.pdf`)（《ORACLE SOLARIS 11 EXPRESS 2010.11 新增功能》）

  本文提供了此发行版 2010 年 11 月版的 Oracle Solaris 功能的快照。

有关可能有用的 Oracle Solaris 10 参考文档，请参见《Oracle Solaris 10 Security Guidelines》。