Oracle® Solaris 11 安全准则

文件号码 E53931-02
2014 年 9 月

ORACLE

目录

表

使用本文档

- **概述** – 概述 Oracle Solaris 安全功能和使用这些功能来强化和保护已安装系统及其应用程序的准则。
- **目标读者** – 系统管理员、安全管理员、应用程序开发者以及在 Oracle Solaris 11 系统上开发、部署或评估安全的审计人员。
- **必备知识** – 站点安全要求。

产品文档库

位于 http://www.oracle.com/pls/topic/lookup?ctx=E56344 的文档库中包含此产品的最新信息和已知问题。

获得 Oracle 支持

Oracle 客户可通过 My Oracle Support 获得电子支持。有关信息，请访问 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info；如果您听力受损，请访问 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs。

反馈

可以在 http://www.oracle.com/goto/docfeedback 上提供有关本文档的反馈。

♦ ♦ ♦ 第 1 章

1 关于 Oracle Solaris 安全

Oracle Solaris 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 进行了充分测试并提供支持。

Oracle Solaris 11.2 的新增安全功能

本节重点向现有客户介绍有关此发行版新增重要安全功能的信息。

- 借助新的 `compliance` 命令，您可以评估系统是否符合安全标准。您可以使用该命令评估并报告系统是否符合行业标准安全基准（包括 PCI-DSS）。有关详细信息，请参见《Oracle Solaris 11.2 安全遵从性指南 》和 `compliance(1M)` 手册页。
- Oracle Solaris 的加密框架功能通过了有关 Oracle Solaris 11.1 SRU 5.5 和 Oracle Solaris 11.1 SRU 3 发行版中用户级函数和内核函数的 FIPS 140-2 第 1 级验证。
  - 有关通过 Oracle FIPS 140 验证的产品的列表，请参见 Oracle FIPS 140 Software Validations (http://www.oracle.com/technetwork/topics/security/fips140-software-validations-1703049.html)（Oracle FIPS 140 软件验证）。
  - 有关在系统上启用 FIPS 140 模式 的信息，请参见《Using a FIPS 140 Enabled System in Oracle Solaris 11.2 》。

- Oracle Solaris 11.1 通过了加拿大通用评估准则体系认证。请参见“Oracle Solaris 11 通用评估准则 EAL4+ 认证” [25]。
- 审计服务可以使用 Oracle Audit Vault 来存储、查看和分析审计记录。请参见《在 Oracle Solaris 11.2 中管理审计 》中的“将 Oracle Audit Vault and Database Firewall 用于存储和分析审计记录”。
- 经验证的引导可保护 Oracle SPARC T5 系列服务器和 Oracle SPARC T7 系列服务器上的引导过程免受威胁。有关更多信息，请参见《在 Oracle Solaris 11.2 中确保系统和连接设备的安全 》中的“使用验证的引导”。
- 可以使用证书和密钥来保护以下对象的自动安装 (Automatic Installation, AI)：安装服务器、指定客户机系统、指定安装服务的所有客户机以及任何其他 AI 客户机。安全 AI 可保护 Oracle Solaris 软件包安全传输到系统。请参见《安装 Oracle Solaris 11.2 系统 》中的“提高自动化安装的安全性”。
- 提供了新的组安装软件包 `pkg:/group/system/solaris-minimal-server`。有关组软件包内容的说明和比较，请参见《Oracle Solaris 11.2 Package Group Lists 》。
- 可以使用 AI 安装 Kerberos 客户机，以便客户机在首次引导时就是基于 Kerberos 的系统。请参见《安装 Oracle Solaris 11.2 系统 》中的“如何使用 AI 配置 Kerberos 客户机”。
- 在此发行版中，物理全局区域（称为不可变全局区域）和虚拟全局区域（称为 Oracle Solaris 内核区域）可以为只读区域。不可变全局区域的功能比内核区域稍为强大，但这两种区域均无法永久更改系统的硬件或配置。与允许写入的区域相比，只读区域引导速度更快且安全性更高。

  出于维护目的，不可变全局区域定义了一组称为可信计算基 (Trusted Computing Base, TCB) 的特殊进程，您可以通过称为可信路径的受保护登录配置此类进程。有关更多信息，请参见《创建和使用 Oracle Solaris 区域 》中的第 12 章 “配置和管理不可编辑的区域”。有关区域配置资源的信息，请参见《Oracle Solaris Zones 介绍 》。另请参见 `mwac(5)` 和 `tpd(5)` 手册页。

  Oracle Solaris 内核区域对部署合规系统很有用。例如，可以配置合规系统，创建统一归档，然后将映像部署为内核区域。有关更多信息，请参见 `solaris-kz(5)` 手册页、《创建和使用 Oracle Solaris 内核区域 》、《Oracle Solaris 11.2 虚拟环境介绍 》中的“Oracle Solaris Zones 概述”和《在 Oracle Solaris 11.2 中使用统一归档文件进行系统恢复和克隆 》。
- 用户权限和进程权限的新增功能包括：
  - 对 PAM 服务基于时间以及基于位置的访问控制
  - 在 RBAC 上管理的授权角色 (Authorization Roles Managed on RBAC, ARMOR)，为预定义角色
  - 强制用户先提供口令再运行特权操作的权限配置文件
  - 网络监测和系统监测权限配置文件，用于在具有特权但不是 `root` 的情况下运行诊断命令 `ipstat`、`tcpstat`、`snoop` 和 `intrstat`

  有关详细信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“Oracle Solaris 11.2 中新增的权限功能”。

- IKE 版本 2 (IKE Version 2, IKEv2) 提供了最新 IKE 协议，用于对受 IPsec 保护的网络数据包进行自动密钥管理。有关详细信息，请参见《在 Oracle Solaris 11.2 中确保网络安全 》中的“Oracle Solaris 11.2 中新增的网络安全功能”。
- Oracle Hardware Management Pack (HMP) 提供了用于配置和更新固件的命令行工具。有关如何安全地配合其他 Oracle 硬件产品（如网络交换机和网络接口卡）使用 HMP 的信息，请参见《Oracle Hardware Management Pack for Oracle Solaris 安全指南 》。

Oracle Solaris 11 安装后安全性

Oracle Solaris 安装时使用“缺省安全”(Secure by Default, SBD)。此安全状况可保护系统免受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。安装时，初始用户与 root 帐户的口令完全相同。

- 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，且至少包含两个字母字符和一个非字母字符。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，用户访问远程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，因此在审计迹中记录充当 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、系统文件和桌面应用程序均受文件权限、特权以及用户权限保护。用户权限也称为基于角色的访问控制 (Role-based Access Control, RBAC)。

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。缺省目录权限为 `drwxr-xr-x` (`755`)。文件权限为 `-rw-r--r--` (`644`)。

系统文件 – 受文件权限保护的系统配置文件。只有 `root` 角色或分配有对特定系统文件的编辑权限的用户可以修改系统文件。

桌面 Applet – 桌面 Applet 受权限管理所保护。因此，管理操作（例如，在打印管理器中添加远程打印机）仅限于拥有对打印操作的管理权限的用户和角色。

Oracle Hardware Management Package

Oracle Hardware Management Package 提供了一组用于配置、管理和监视 Oracle 服务器的实用程序。这组适用于 Oracle 硬件的增值工具始终可用。这组工具可以自动向 ILOM 提供与硬件相关的信息，使其能够充分了解系统硬件。有关实用程序和安全性的信息，请参见 Systems Management and Diagnostics Documentation (http://www.oracle.com/goto/ohmp/docs)（系统管理与诊断文档）。

Oracle Solaris 可配置的安全性

除 Oracle Solaris 缺省安全设置所提供的坚实基础之外，Oracle Solaris 系统的安全设置还具有极高的可配置性，从而能够满足多种多样的安全要求。

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。

保护数据

Oracle Solaris 可在整个安装、使用和归档期间防止数据遭到引导。

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，缺省文件系统（即 ZFS）还支持访问控制列表 (Access Control List, ACL)，这些访问控制列表能够更加精确地控制对单个或多组文件系统对象的访问。

有关更多信息，请参见以下内容：

- 有关文件权限的概述，请参见《在 Oracle Solaris 11.2 中确保文件的安全和确认文件完整性 》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《在 Oracle Solaris 11.2 中管理 ZFS 文件系统 》中的第 7 章 “使用 ACL 和属性保护 Oracle Solaris ZFS 文件” 和手册页。
- 有关对 ZFS 文件设置 ACL 的说明，请参见 `chmod(1)` 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。KMF 为各种公钥基础结构 (Public Key Infrastructure, PKI) 的不同存储机制、管理实用程序和编程接口提供了统一接口。

加密框架提供了一个包含算法和 PKCS #11 库的公共存储区来处理加密要求。PKCS #11 库依据 RSA Security Inc. 的 PKCS #11 加密令牌接口 (Cryptographic Token Interface, Cryptoki) 标准实现。加密服务（例如对文件进行加密和解密）可供一般用户使用。

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《在 Oracle Solaris 11.2 中管理加密和证书 》中的第 1 章 “加密框架” 和《在 Oracle Solaris 11.2 中管理加密和证书 》中的第 4 章 “密钥管理框架”。
- 有关使用加密框架的示例，请参见《在 Oracle Solaris 11.2 中管理加密和证书 》中的第 3 章 “加密框架” 和手册页。
- 要启用加密框架 FIPS 140 提供者，请参见《在 Oracle Solaris 11.2 中管理加密和证书 》中的“如何创建启用了 FIPS 140 的引导环境”。

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 权限和 ACL 可保护文件，您可以在创建时对整个数据集进行加密。Oracle Solaris 权限管理支持对 ZFS 数据集的委托管理，也就是说，分配了有限的特权集的用户可以管理 ZFS 数据集。

有关更多信息，请参见以下内容：

- 《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“用户权限管理”
- 《在 Oracle Solaris 11.2 中管理 ZFS 文件系统 》中的第 1 章 “Oracle Solaris ZFS 文件系统（介绍）”
- 《在 Oracle Solaris 11.2 中管理 ZFS 文件系统 》中的“Oracle Solaris ZFS 与传统文件系统的区别”
- 《在 Oracle Solaris 11.2 中管理 ZFS 文件系统 》中的第 5 章 “管理 Oracle Solaris ZFS 文件系统”
- 《在 Oracle Solaris 11.2 中管理安全 Shell 访问 》中的“如何使用安全 Shell 远程管理 ZFS”
- 所选手册页包括 `zfs(1M)` 和 `zfs(7FS)`。

Java 加密扩展

Java 为 Java 应用程序开发者提供了 Java 加密扩展 (Java Cryptography Extension, JCE)。有关更多信息，请参见 Java SE Security (http://www.oracle.com/technetwork/java/javase/tech/index-jsp-136007.html)（Java SE 安全性）。

保护和隔离应用程序

应用程序可能是恶意软件和恶意用户的入口点。在 Oracle Solaris 中，只有使用特权并将应用程序包含在区域内才能减少这些威胁。应用程序可以仅使用该应用程序所需的特权运行，以便恶意用户不拥有访问系统其余部分的 root 特权。区域可以限制攻击的范围。对非全局区域中应用程序的攻击只会影响该区域中的进程，而不会影响该区域的主机系统。

地址空间布局随机化 (Address Space Layout Randomization, ASLR) 和服务管理工具 (Service Management Facility, SMF) 是能够保护应用程序的附加功能。ASLR 使得入侵者难以劫持可执行文件，而 SMF 功能使管理员能够限制对应用程序的启动、停止和使用。

Oracle Solaris 中的特权

特权是在内核中强制执行的针对进程的细粒度独立权限。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`）。可以向进程、用户或角色授予特权。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。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。

使用特权又称为进程权限管理。利用特权，组织可以指定并进而限制要向其系统上运行的服务和进程授予的特权。

有关更多信息，请参见以下内容：

- 《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“进程权限管理”
- 《面向开发者的 Oracle Solaris 11 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)`。

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。

在 Oracle Solaris 11.2 中，可以配置不可变的根文件系统。

有关更多信息，请参见以下内容：

- 《创建和使用 Oracle Solaris 区域 》中的“配置只读区域”
- 《Oracle Solaris Zones 介绍 》
- 所选手册页包括 `brands(5)`、`zoneadm(1M)` 和 `zonecfg(1M)`。

地址空间布局随机化

地址空间布局随机化 (Address Space Layout Randomization, ASLR) 功能会随机分配地址以供某个给定程序使用。ASLR 可以阻止特定类型的攻击（即那些基于掌握特定内存范围的确切位置而发起的攻击），并且可以在有人尝试停止程序时检测到这种意图。有关更多信息，请参见《在 Oracle Solaris 11.2 中确保系统和连接设备的安全 》中的“地址空间布局随机化”和如何验证 ASLR 是否已启用 [29]。

服务管理工具

服务是持久运行的应用程序。服务可以表示运行的应用程序、设备软件状态或一组其他服务。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 使用权限管理来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：

- 《在 Oracle Solaris 11.2 中管理系统服务 》
- 《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“如何将特定特权指定给 Apache Web 服务器”
- 所选手册页包括 `svcadm`(1M)、`svcs`(1) 和 `smf`(5)。

保护用户和分配额外权限

在 `/etc/security/policy.conf` 文件中为用户分配了基本特权集、权限配置文件和授权，就如同“系统访问受限制和监视” [13]中介绍的初始用户一样。这些权限均可配置。您可以拒绝用户的基本权限以及增加用户权限。

Oracle Solaris 可通过灵活的口令复杂度要求、可针对不同站点要求进行配置的验证以及用户权限管理（使用权限配置文件、授权和特权来限制和分配可信用户的管理权限）为用户提供保护。此外，称为角色的特殊共享帐户可以只为用户分配这些管理权限（如果用户承担该角色）。在 RBAC 上管理的授权角色 (ARMOR) 软件包提供了预定义角色。

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 具有许多功能，您可以使用这些功能根据站点要求配置用户口令。可以指定口令长度、内容、更改频率以及修改要求，还可以保留口令历史记录。它提供了应避免使用的口令的字典。还提供了多个可能的口令散列算法。缺省算法为 SHA256。

有关更多信息，请参见以下内容：

- 《在 Oracle Solaris 11.2 中确保系统和连接设备的安全 》中的“维护登录控制”
- 《在 Oracle Solaris 11.2 中确保系统和连接设备的安全 》中的“保证登录和口令的安全”
- 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，管理员可以协调和配置帐户、凭证、会话和口令的用户验证要求，而不必修改要求验证的服务。

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 `ssh`）使用 PAM 框架保护刚安装的系统的所有入口点。通过 PAM，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。

Oracle Solaris 提供了一组广泛的 PAM 模块和配置，可满足大多数站点策略的要求。有关更多信息，请参见以下内容：

- 《在 Oracle Solaris 11.2 中管理 Kerberos 和其他验证服务 》中的第 1 章 “使用可插拔验证模块”
- 《面向开发者的 Oracle Solaris 11 安全性指南 》中的“编写使用 PAM 服务的应用程序”
- `pam.conf(4)` 手册页

用户权限管理

Oracle Solaris 中的用户权限是根据最小特权安全原则进行控制的。组织不但可以根据自身的独特需要和要求选择性地向用户或角色授予管理权限，还可以根据需要拒绝用户的权限。权限的实现方式包括为进程提供特权以及为用户或 SMF 方法提供授权。权限配置文件提供了一种十分方便的方法，可将特权和授权收集到相关权限包中。

有关更多信息，请参见以下内容：

- 《在 Oracle Solaris 11.2 中确保用户和进程的安全 》
- 所选手册页包括 `auths(1)`、`privileges(5)`、`profiles(1)`、`rbac(5)`、`roleadd(1M)`、`roles(1)` 和 `user_attr(4)`。

保护网络通信

可以通过如下功能保护网络通信：防火墙、联网应用程序上的 TCP 包装和已验证的加密远程连接。

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。

防火墙

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：

- 有关 IP 过滤器的概述，请参见《在 Oracle Solaris 11.2 中确保网络安全 》中的第 4 章 “关于 Oracle Solaris 中的 IP 过滤器”。
- 有关使用 IP 过滤器的示例，请参见《在 Oracle Solaris 11.2 中确保网络安全 》中的第 5 章 “配置 IP 过滤器” 和手册页。
- 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。
- 所选手册页包括 `ipfilter(5)`、`ipf(1M)`、`ipnat(1M)`、`svc.ipfd(1M)` 和 `ipf(4)`。

TCP 包装

TCP 包装可为 Internet 服务提供访问控制。启用了多个 Internet (`inetd`) 服务时，`tcpd` 守护进程会根据 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 包装还会在 `syslog` 中记录主机对网络服务的请求，这是一项非常有用的监视功能。

可配置 Oracle Solaris 的 安全 Shell (`ssh`) 和 `sendmail` 功能以使用 TCP 包装。以一对一方式映射到可执行文件的网络服务（例如，`proftpd` 和 `rpcbind`）是 TCP 包装的候选对象。

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 TCP 包装的信息，请参见以下内容：

- 如何使用 TCP 包装 [42]
- 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。
- 所选手册页包括 `tcpd`(1M) 和 `inetd(1M)`。

远程访问

远程访问攻击会损坏系统和网络。Oracle Solaris 可为网络传输提供深度防御。防御功能包括数据传输的加密和验证检查、登录验证以及禁用不需要的远程服务。

IPsec 和 IKE

IP 安全 (IP Security, IPsec) 通过对 IP 包进行验证和/或加密来保护网络传输。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 及其自动密钥交换 (automatic key exchange, IKE) 协议使用由加密框架提供的算法。此外，加密框架还提供一个中央密钥库。将 IKE 配置为使用 metaslot 时，组织可选择在磁盘上、在已连接的硬件密钥库上或在称为 *softtoken* 的软件密钥库中存储密钥。

IPsec 和 IKE 需要进行配置，因此应对其进行安装，但缺省情况下处于未启用状态。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：

- 《在 Oracle Solaris 11.2 中确保网络安全 》中的第 6 章 “关于 IP 安全体系结构”
- 《在 Oracle Solaris 11.2 中确保网络安全 》中的第 7 章 “配置 IPsec”
- 《在 Oracle Solaris 11.2 中确保网络安全 》中的“IPsec 和 FIPS 140”
- 《在 Oracle Solaris 11.2 中确保网络安全 》中的第 8 章 “关于 Internet 密钥交换”
- 《在 Oracle Solaris 11.2 中确保网络安全 》中的第 9 章 “配置 IKEv2”
- 所选手册页包括 `ipsecconf(1M)` 和 `in.iked(1M)`。

安全 Shell

缺省情况下，Oracle Solaris 的 安全 Shell 功能是新安装的系统上唯一活动的远程访问机制。其他所有网络服务均禁用，或处于“仅监听”模式。

安全 Shell 可在两个系统之间创建加密通信通道。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。

有关更多信息，请参见以下内容：

- 《在 Oracle Solaris 11.2 中管理安全 Shell 访问 》中的第 1 章 “使用安全 Shell（任务）”
- 《在 Oracle Solaris 11.2 中管理安全 Shell 访问 》中的“安全 Shell 和 FIPS 140”
- 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 功能甚至支持通过异构网络（这些网络上的系统运行不同的操作系统并且运行 Kerberos 服务）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：

- 《在 Oracle Solaris 11.2 中管理 Kerberos 和其他验证服务 》
- 《在 Oracle Solaris 11.2 中管理 Kerberos 和其他验证服务 》中的“FIPS 140 算法和 Kerberos 加密类型”
- 所选手册页包括 kadmin(1M)、kdcmgr(1M)、kerberos(5)、kinit(1) 和 krb5.conf(4)。

维护系统安全

Oracle Solaris 提供了以下功能用于维护系统安全：

- 验证的引导 – 可保护引导过程。缺省情况下，验证的引导已禁用。
- 软件包验证 – 验证已安装的软件包是否与源系统信息库中的软件包完全相同。
- 审计服务 – 可审计系统的访问和使用。缺省情况下启用审计。
- 文件完整性验证 – BART 清单可以列出系统上的每个文件，而比较这些清单可以验证文件完整性是否得到保持。
- 日志文件 – SMF 会为每个服务提供日志文件。`syslog` 实用程序不但提供了一个中央文件用于命名和配置系统服务的日志，而且可以向管理员通知关键事件（可选）。其他功能（如审计）也会创建各自的日志。
- 遵从性报告 – Oracle Solaris 提供了多项安全基准，用作对系统进行评估的依据。这些评估所生成的报告有助于评估系统的安全状况。

验证的引导

验证的引导是 Oracle Solaris 的一项功能，可保护系统的引导过程。此功能可保护系统免受威胁，如安装未经授权的内核模块和特洛伊木马应用程序。缺省情况下，验证的引导已禁用。

有关更多信息，请参见《在 Oracle Solaris 11.2 中确保系统和连接设备的安全 》中的第 2 章 “保护 Oracle Solaris 系统完整性”。

软件包完整性验证

安装或更新软件包后，可以运行 `pkg verify` 命令以确保系统上的软件包与源系统信息库中的软件包完全相同。

有关更多信息，请参见 pkg(1) 手册页和如何检验软件包 [28]。

审计服务

Oracle Solaris 提供了审计服务，用于收集有关系统访问和使用的数据。审计数据提供了带有可靠时间戳的日志，其中记录与安全相关的系统事件。以后便可以使用此数据来指定系统上执行的操作的职责。

审计是安全评估机构、验证机构、合规机构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《在 Oracle Solaris 11.2 中管理审计 》中的第 7 章 “审计参考”。
- 有关准则，请参见如何审计除登录/注销以外的重要事件 [38]和手册页。
- 有关审计的概述，请参见《在 Oracle Solaris 11.2 中管理审计 》中的第 1 章 “关于 Oracle Solaris 中的审计”。
- 有关审计任务，请参见《在 Oracle Solaris 11.2 中管理审计 》中的第 3 章 “管理审计服务”。

文件完整性验证

使用 Oracle Solaris 的 BART 功能，可以通过在系统运行一段时间后对系统执行文件级别的检查来全面验证系统。安装后，可运行 `pkg verify` 命令以确认源软件包的内容是否与目标软件包的内容完全相同。执行软件包验证后，BART 清单可以轻松可靠地收集有关系统上的文件的信息。

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。可将某个系统的文件与其原始文件进行比较，也可以与其他系统的文件进行比较。报告可能指示以下信息：系统未修补、入侵者安装了未经批准的文件或者入侵者更改了敏感文件（例如 `root` 拥有的文件）的权限或内容。

有关更多信息，请参见以下内容：

- 有关准则，请参见“使用 BART 检验文件完整性” [49]、“使用 BART 检验文件完整性” [49] 和手册页。
- 有关 BART 的概述，请参见《在 Oracle Solaris 11.2 中确保文件的安全和确认文件完整性 》中的第 2 章 “使用 BART 检验文件完整性”。
- 有关使用 BART 的示例，请参见《在 Oracle Solaris 11.2 中确保文件的安全和确认文件完整性 》中的“关于使用 BART” 和手册页。
- 所选手册页包括 `bart(1M)`、`bart_rules(4)` 和 `bart_manifest(4)`。

日志文件

Oracle Solaris 的服务管理工具 (Service Management Facility, SMF) 功能可逐个记录其服务的状态。许多服务（例如审计和 安全 Shell）会写入各自的日志。`syslog` 或 `rsyslog` 守护进程会写入一个集中式日志，该日志可通知和警告管理员许多服务出现了危险情况。例如，审计服务可以配置为将汇总的审计记录写入 `syslog`。请参见 `syslogd(1M)` 和 `syslog.conf(4)` 手册页。

符合安全标准

`compliance assess` 命令可提供系统的安全状况快照。评估所生成的报告会建议对系统进行特定更改以满足行业安全基准。有关更多信息，请参见《Oracle Solaris 11.2 安全遵从性指南 》和 `compliance(1M)` 手册页。

标签安全

Oracle Solaris 中的标签安全由 Trusted Extensions 功能提供。

Oracle Solaris 中的 Trusted Extensions 功能

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。

Trusted Extensions 实现的独特之处在于，它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。Trusted Extensions 是 “Oracle Solaris 11 通用评估准则 EAL4+ 认证” [25]的一部分。

Trusted Extensions 可满足通用评估准则标签安全软件包 (Labeled Security Package, LSP) 的要求。请参见“Oracle Solaris 11 通用评估准则 EAL4+ 认证” [25]。

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 》。
- 所选手册页包括 `trusted_extensions(5)`、`labeladm(1M)` 和 `labeld(1M)`。

有标签文件系统

缺省情况下，在具有相同标签的区域中为文件系统分配单个标签。可以创建多级别 ZFS 数据集，将其挂载到 Trusted Extensions 系统上，然后使用相应权限升级和降级该数据集中的文件。有关更多信息，请参见《Trusted Extensions 配置和管理 》中的“需要为文件重新设置标签的多级别数据集”。

有标签网络通信

Trusted Extensions 可为网络通信设置标签。系统将根据始发网络端点与接收网络端点各自关联的标签的比较结果来限制数据流。此外，还必须为网关和中间跃点设置标签，以允许传递通信的标签上的信息。NFS 和多级别 ZFS 数据集可在网络上提供其他功能。

有关更多信息，请参见以下内容：

- 《Trusted Extensions 配置和管理 》中的“在 Trusted Extensions 中配置网络接口”
- 《Trusted Extensions 配置和管理 》中的第 15 章 “可信网络”
- 《Trusted Extensions 配置和管理 》中的第 16 章 “在 Trusted Extensions 中管理网络”

Trusted Extensions 多级别桌面

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。可以对用户进行配置，以便只有允许的标签对其可见。可将每个标签配置为需要单独的口令。

有关更多信息，请参见《Trusted Extensions 用户指南 》。要配置用户，请参见《Trusted Extensions 配置和管理 》中的第 11 章 “在 Trusted Extensions 中管理用户、权限和角色”。

Oracle Solaris 11 通用评估准则 EAL4+ 认证

Oracle Solaris 11 通过了加拿大通用评估准则体系的评估保证级别 4 (Evaluation Assurance Level 4, EAL4) 认证，并通过缺陷修复来提高安全级别 (EAL4+)。根据通用评估准则互认协定 (Common Criteria Recognition Arrangement, CCRA)，EAL4 是 26 个国家/地区互相认可的最高评估级别。

该认证适用于操作系统保护框架 (Operating System Protection Profile, OSPP)，并且包括以下扩展包：

- 高级管理
- 扩展标识和验证

- 标签安全
- 虚拟化

有关认证的信息，请参见：

- Oracle Security Evaluations Matrix (http://www.oracle.com/technetwork/topics/security/security-evaluations-099357.html)
- The Common Criteria Recognition Arrangement (http://www.commoncriteriaportal.org/ccra/)（通用评估准则互认协定）
- Operating System Protection Profile (http://www.commoncriteriaportal.org/files/ppfiles/pp0067b_pdf.pdf)（操作系统保护框架）

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。如果您在开发程序或安装第三方程序，您必须安全地开发和安装这些程序。

有关更多信息，请查看以下内容：

- Importance of Software Security Assurance (http://www.oracle.com/us/support/assurance/overview/index.html)
- 《面向开发者的 Oracle Solaris 11 安全性指南 》中的附录 A “适用于开发者的安全编码准则”
- 《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“实现安全要求”
- 保证代码安全 (http://blogs.oracle.com/maryanndavidson/entry/those_who_can_t_do)

♦ ♦ ♦ 第 2 章

2 配置 Oracle Solaris 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，可选择软件包系统信息库中称为组的一组软件包。不同的组提供不同用途的软件包，如多用途服务器、最小安装版系统和桌面系统。软件包已签名，您可以验证其安全传输。

安装 Oracle Solaris OS 时，请选择安装相应的组软件包的介质，如下所示：

- 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都会安装 `group/system/solaris-large-server` 组，该组提供了 Oracle Solaris 大型服务器环境。
- Oracle Solaris Small Server – 自动化安装程序 (Automated Installer, AI) 安装和文本安装程序可选择安装 `group/system/solaris-small-server` 组，该组将提供可以向其添加软件包的有用命令行环境。
- Oracle Solaris Minimal Server – 自动化安装程序 (Automated Installer, AI) 安装和文本安装程序可选择安装 `group/system/solaris-minimal-server` 组，该组将提供可以仅向其添加所需软件包的最低限度命令行环境。
- 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` 组添加到桌面服务器。有关更多信息，请参见以下文章：《Optimizing the Oracle Solaris 11 Desktop for a Multiuser Environment》。

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 11.2 系统》中的第 III 部分, “使用安装服务器安装”。

选择介质时，请参见以下安装指南和软件包内容指南：

- 《安装 Oracle Solaris 11.2 系统》
- 《创建定制 Oracle Solaris 11.2 安装映像》
- 《在 Oracle Solaris 11.2 中添加和更新软件》
- 《Oracle Solaris 11.2 Package Group Lists》

在初始状态下保护系统

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

表 2-1 保护系统任务列表

任务	描述	有关说明
1. 检验系统上的软件包。	检查安装源中的软件包是否与已安装的软件包完全相同。	如何检验软件包 [28]
2. 确保可执行文件受到保护。	检查 ASLR 是否已启用。	如何验证 ASLR 是否已启用 [29]
3. 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。在 x86 系统上，对 GRUB 菜单的访问会受到控制。在 SPARC 系统上，`eeprom` 命令可保护硬件。	《在 Oracle Solaris 11.2 中确保系统和连接设备的安全》中的“控制对系统硬件的访问”
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。	如何禁用不需要的服务 [29]
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。	如何为用户删除电源管理功能 [30]
6. 创建用于反映站点安全策略的登录警告消息。	执行验证前后通知用户系统处于受监视状态。	如何在标题文件中放置安全消息 [31] 如何在桌面登录屏幕中放置安全消息 [32]

▼ 如何检验软件包

安装后立即通过检验软件包来验证安装。

开始之前 您必须承担 `root` 角色。有关更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全》中的“使用所指定的管理权限”。

1. 查看安装日志。

2. 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
   ```

3. 查看日志中是否存在错误。

4. 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。

▼ 如何验证 ASLR 是否已启用

缺省情况下，带有标记的可执行指令将写到未连接的地址空间，以降低入侵者在可执行栈上注入指令的能力。

开始之前 您必须承担 `root` 角色。有关更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“使用所指定的管理权限”。

1. 验证 ASLR 是否已启用。

   ```
   # sxadm info
   EXTENSION       STATUS                  CONFIGURATION
   aslr            enabled (all)           enabled (all)
   ```

   值 `all` 的功能比缺省值更加强大，并且可能会导致依赖内存中的连续栈的应用程序发生错误。例如，数据库可能依赖内存中的连续栈。

2. 如果 ASLR 已禁用，请启用缺省值并验证该值是否有效。

   ```
   # sxadm delcust aslr
   # sxadm info
   EXTENSION       STATUS                  CONFIGURATION
   aslr            enabled (tagged-files)  system default (default)
   ```

另请参见 要进行调试，可以通过对特定二进制文件调用 `sxadm` 命令来关闭 ASLR。有关示例，请参见 sxadm(1M) 手册页。

▼ 如何禁用不需要的服务

使用此过程可禁用此系统不需要的服务。

开始之前 您必须承担 `root` 角色。有关更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“使用所指定的管理权限”。

1. 列出联机网络服务。

```
# svcs | grep network
online         Sep_07   svc:/network/loopback:default
online         Sep_07   svc:/network/http:apache22
online         Sep_07   svc:/network/nfs/server: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，但这些服务器的服务处于联机状态，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《在 Oracle Solaris 11.2 中管理系统服务 》中的第 1 章 “服务管理工具简介”和 `svcs(1)` 手册页。

▼ 如何为用户删除电源管理功能

使用此过程可阻止系统控制台上的用户暂停系统或关闭系统电源。如果控制台用户能够拔下系统硬件，则此软件解决方案将不起作用。

开始之前 您必须承担 `root` 角色。有关更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“使用所指定的管理权限”。

1. 查看 "Console User"（控制台用户）权限配置文件的内容。

```
% profiles -p "Console User" info
 name=Console User
 desc=Manage System as the Console User
 auths=solaris.system.shutdown,solaris.device.cdrw,
             solaris.smf.manage.vbiosd,solaris.smf.value.vbiosd
 profiles=Suspend To RAM,Suspend To Disk,Brightness,CPU Power Management,
                Network Autoconf User
 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《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“如何创建权限配置文件”。

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. 分配在步骤 2 中创建的权限配置文件。

   - 如果许多用户共享同一个权限配置文件，则在权限配置文件中设置此值将是一个可伸缩的解决方案。

     ```
     # usermod -P shared-profile username
     ```

   - 此外，也可以在 `policy.conf` 文件中为每个系统分配一个配置文件。

     ```
     # pfedit /etc/security/policy.conf...
     #PROFS_GRANTED=Basic Solaris User
     PROFS_GRANTED=shared-profile,Basic Solaris User
     ```

另请参见 有关更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“policy.conf 文件”以及 `policy.conf`(4) 和 `usermod`(1M) 手册页。

▼ 如何在标题文件中放置安全消息

使用以下过程可在两个标题文件中创建反映站点安全策略的安全消息。`/etc/issue` 文件会在验证前显示，而 `/etc/motd` 文件会在验证后显示。

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。有关安全消息内容的信息，请向贵公司的法律顾问咨询。

开始之前 您必须成为具有 "Administrator Message Edit"（管理员消息编辑）权限配置文件的管理员。有关更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“使用所指定的管理权限”。

1. 创建 **`/etc/issue`** 文件并添加安全消息。

   ```
   # pfedit /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.
   ```

   `login` 命令在验证前显示 `/etc/issue` 的内容，就像 `ssh`、`telnet` 和 FTP 服务一样。要在桌面登录时显示 `/etc/issue` 的内容，请参见如何在桌面登录屏幕中放置安全消息 [32]。

   有关更多信息，请参见 `issue`(4) 和 `pfedit`(1M) 手册页。

2. 在 **`/etc/motd`** 文件中添加安全消息。

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

在 Oracle Solaris 中，用户的初始 shell 会显示 /etc/motd 文件的内容。

▼ 如何在桌面登录屏幕中放置安全消息

创建安全消息以供用户查看时，请从以下几种方法中选择一种：验证前查看、验证后查看或验证前后均可查看。/etc/issue 文件会在验证前显示，而 /etc/motd 文件会在验证后显示。

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。有关安全消息内容的信息，请向贵公司的法律顾问咨询。

开始之前 要创建文件，您必须承担 root 角色。要修改现有文件，您必须成为具有 solaris.admin.edit/*path-to-existing-file* 授权的管理员。

1. **可使用以下选项之一将安全消息放在验证前的桌面登录屏幕中。**

   创建验证前对话框的选项使用 /etc/issue 文件（来自如何在标题文件中放置安全消息 [31] 的步骤 1）中的安全消息。

   - **选项 1：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，它们分别在验证前、验证后以及验证前后显示安全消息。

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

     有关以非 root 用户身份编辑系统文件的信息，请参见 pfedit(1M) 手册页。

   - **选项 2：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） 保存修改后的登录窗口 UI 的副本。

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

2. 可使用以下选项之一将安全消息放在验证后的桌面登录屏幕中。

创建验证后对话框的选项使用 `/etc/motd` 文件（来自如何在标题文件中放置安全消息 [31] 的步骤 2）中的安全消息。

- 选项 1：在验证后的桌面中放置安全消息。

```
# pfedit /etc/gdm/PreSession/Default
/usr/bin/zenity --text-info --width=800 --height=300 \
--title="Security Message"  --filename=/etc/motd
```

注 - 可将该对话框包含在用户工作区的窗口中。

- 选项 2：创建验证后在附加窗口中显示安全消息的桌面文件。

```
# pfedit /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/motd
OnlyShowIn=GNOME;
X-GNOME-Autostart-Phase=Application
```

在登录窗口中进行验证后，用户必须关闭安全消息窗口才能访问工作区。有关 zenity 命令的选项，请参见 zenity(1) 手册页。

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。

```
# pfedit /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
```

保护用户

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。

表 2-2 保护用户任务列表

任务	描述	有关说明
要求使用强口令并定期更改口令。	增强每个系统上的缺省口令约束。	如何设置更强的口令约束 [35]
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。	如何为一般用户设置限制性更强的 umask 值 [37]。
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。	如何为一般用户设置账户锁定 [36]
为所有用户预选 cusa 审计类。	更好地监视和记录系统面临的潜在威胁。	如何审计除登录/注销以外的重要事件 [38]
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。 您可以使用预定义的 ARMOR 角色，创建自己的角色，或者也可以使用自己的角色来扩展 ARMOR。	《在 Oracle Solaris 11.2 中管理用户帐户和用户环境 》中的“使用 CLI 管理用户帐户” 《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“为用户指定权限”
减少可见的 GNOME 桌面应用程序的数量。	禁止用户使用会影响安全的桌面应用程序。	请参见《Oracle Solaris 11.2 Desktop 管理员指南 》中的第 11 章 “禁用 Oracle Solaris Desktop 系统中的功能”。
限制用户的特权。	删除用户不需要的基本特权。	如何为用户删除不需要的基本特权 [39]

▼ 如何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` 文件中变量条目的顺序。

开始之前 您必须是指定有 `solaris.admin.edit/etc/default/passwd` 授权的管理员。有关更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“使用所指定的管理权限”。

- 使用 **pfedit** 命令可在 **/etc/default/passwd** 文件中进行以下更改：

  a. 要求用户至少每四个月更改一次口令，但频率不能超过每三周更改一次。

  ```
  ## /etc/default/passwd
  ##
  #MAXWEEKS=
  #MINWEEKS=
  MAXWEEKS=13
  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
- 有关可限制口令创建的变量的列表，请参见 `passwd(1)` 手册页。
- 有关在安装后生效的口令约束，请参见“系统访问受限制和监视” [13]。

▼ 如何为一般用户设置账户锁定

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 - 角色是共享帐户。请勿对可承担角色的用户设置帐户锁定，也不要对角色设置帐户锁定，因为锁定用户会同时将角色锁定。

开始之前 请勿在用于管理活动的系统上在系统范围内设置此保护。相反，请监视管理系统的异常使用情况并保持其可供管理员使用。

您必须承担 `root` 角色。有关更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“使用所指定的管理权限”。

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

   选择属性值的范围。

   - **在系统范围内设置。**

     这种保护适用于尝试使用系统的任何用户。

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

   - **对每个用户设置。**

     这种保护仅适用于您对其运行此命令的用户。如果存在许多用户，这种保护将不是一个可伸缩的解决方案。

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

   - **创建并分配权限配置文件。**

     这种保护适用于您为其分配了此权限配置文件的任何用户或系统。

     a. **创建权限配置文件。**

        ```
        # profiles -p shared-profile -S ldap
        shared-profile: set lock_after_retries=yes
        ...
        ```

        有关创建权限配置文件的更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“创建权限配置文件和授权”。

     b. **将权限配置文件分配给用户或在系统范围内分配。**

如果许多用户共享同一个权限配置文件，则在权限配置文件中设置此值将是一个可伸缩的解决方案。

```
# usermod -P shared-profile username
```

此外，也可以在 policy.conf 文件中为每个系统分配一个配置文件。

```
# pfedit /etc/security/policy.conf
...
#PROFS_GRANTED=Basic Solaris User
PROFS_GRANTED=shared-profile,Basic Solaris User
```

2. **将 RETRIES 安全属性设置为 3。**
   选择属性值的范围。

   - 在系统范围内设置。

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

   - 对每个用户设置。

     ```
     # usermod -K lock_after_retries=3 username
     ```

   - 创建并分配权限配置文件。
     按照步骤 1.3 中的步骤创建包含 lock_after_retries=3 的权限配置文件。

另请参见

- 有关用户和角色安全属性的讨论，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的第 8 章 “Oracle Solaris 权限参考信息”。
- 所选手册页包括 policy.conf(4)、profiles(1)、user_attr(4) 和 usermod(1M)。

▼ 如何为一般用户设置限制性更强的 umask 值

umask 实用程序可设置用户创建的文件的文件权限位。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 您必须成为授权的管理员才能编辑框架文件。root 角色分配了这些授权。有关更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“使用所指定的管理权限”。

1. **查看 Oracle Solaris 为用户 shell 缺省值提供的示例文件。**

```
# ls -1a /etc/skel
.bashrc
.profile
local.cshrc
local.login
local.profile
```

2. **在 `/etc/skel` 文件中设置您要为用户分配的 `umask` 值。**

   选择以下值之一：

   - `umask 026` – 提供中等文件保护

     (`751`) – 为组提供 `r`，为其他用户提供 `x`
   - `umask 027` – 提供严格的文件保护

     (`750`) – 为组提供 `r`，其他用户无权访问。
   - `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：

- 《在 Oracle Solaris 11.2 中管理用户帐户和用户环境 》中的“使用 CLI 管理用户帐户”
- 《在 Oracle Solaris 11.2 中确保文件的安全和确认文件完整性 》中的“缺省 umask 值”
- 所选手册页包括 `useradd(1M)` 和 `umask(1)`。

▼ 如何审计除登录/注销以外的重要事件

使用此过程可审计管理命令、系统访问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 您必须承担 `root` 角色。有关更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“使用所指定的管理权限”。

1. **审计分配了管理权限配置文件的用户和角色对特权命令的所有使用情况。**

   将 `cusa` 审计类添加到其预选掩码中。

   ```
   # usermod -K audit_flags=cusa:no username
   ```

   ```
   # rolemod -K audit_flags=cusa:no rolename
   ```

   `cusa` 元类所包含的审计类在 `/etc/security/audit_class` 文件中列出。

2. 记录审计命令的参数。

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

3. （可选） 记录审计命令的执行环境。

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

注 - 此策略选项对故障排除很有用。

另请参见
- 有关审计策略的信息，请参见《在 Oracle Solaris 11.2 中管理审计 》中的“审计策略”。
- 有关设置审计标志的示例，请参见《在 Oracle Solaris 11.2 中管理审计 》中的“配置审计服务”和《在 Oracle Solaris 11.2 中管理审计 》中的“对审计服务进行故障排除”。
- auditconfig(1M) 手册页

▼ 如何为用户删除不需要的基本特权

在特殊情况下，可从一般用户或来宾用户的基本特权集中删除部分基本特权。例如，可以阻止 Sun Ray 用户检查不归其所有的进程的状态。

开始之前 您必须承担 root 角色。有关更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“使用所指定的管理权限”。

1. 列出基本特权集的完整定义。

   以下三种基本特权可能是候选的删除对象。

```
% ppriv -lv basic
file_link_any
 Allows a process to create hardlinks to files owned by a uid
 different from the process' effective uid.
...
proc_info
 Allows a process to examine the status of processes other
 than those it can send signals to.  Processes which cannot
 be examined cannot be seen in /proc and appear not to exist.
proc_session
 Allows a process to send signals or trace processes outside its
 session.
...
```

2. 选择特权删除操作的范围。

   - 在系统范围内设置。

拒绝向任何尝试使用系统的用户授予这些特权。这种特权删除方法可能适用于公用计算机。

```
# pfedit /etc/security/policy.conf
...
#PRIV_DEFAULT=basic
PRIV_DEFAULT=basic,!file_link_any,!proc_info,!proc_session
```

- 为各个用户删除特权。
  - 阻止用户链接到不归其所有的文件。

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

  - 阻止用户检查不归其所有的进程。

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

  - 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
    ```

  - 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
    ```

- 创建并分配权限配置文件。

  这种保护适用于您为其分配了此权限配置文件的任何用户或系统。

  a. 创建权限配置文件。

     ```
     # profiles -p shared-profile -S ldap
     shared-profile: set defaultpriv=basic,!file_link_any,!proc_info,!proc_session
     ...
     ```

     有关创建权限配置文件的更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“创建权限配置文件和授权”。

  b. 将权限配置文件分配给用户或在系统范围内分配。

     如果许多用户（例如 Sun Ray 用户或远程用户）共享同一个权限配置文件，则在权限配置文件中设置此值将是一个可伸缩的解决方案。

     ```
     # usermod -P shared-profile username
     ```

     此外，也可以在 `policy.conf` 文件中为每个系统分配一个配置文件。

     ```
     # pfedit /etc/security/policy.conf
     ...
     ```

```
#PROFS_GRANTED=Basic Solaris User
PROFS_GRANTED=shared-profile,Basic Solaris User
```

另请参见 有关更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的第 1 章 “使用权限控制用户和进程”和 `privileges(5)` 手册页。

保护网络

此时，您可能已经创建了可承担角色的用户，且创建了角色。

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。这些网络任务可增强 IP、ARP 和 TCP 协议的安全性。

表 2-3 配置网络任务列表

任务	描述	有关说明
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。	《在 Oracle Solaris 11.2 中确保网络安全 》中的“如何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。	《在 Oracle Solaris 11.2 中确保网络安全 》中的“如何禁用广播包转发”
	阻止对广播回显请求和多播回显请求的响应。	《在 Oracle Solaris 11.2 中确保网络安全 》中的“如何禁用回显请求的响应”
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。	《在 Oracle Solaris 11.2 中确保网络安全 》中的“如何设置严格多宿主”
通过控制不完整的系统连接的数量来阻止拒绝服务 (Denial of Service, DoS) 攻击。	限制 TCP 侦听器所允许的不完整 TCP 连接数。	《在 Oracle Solaris 11.2 中确保网络安全 》中的“如何设置不完整 TCP 连接的最大数目”
通过控制允许的传入连接数来阻止 DoS 攻击。	指定 TCP 侦听器的缺省最大暂挂 TCP 连接数。	《在 Oracle Solaris 11.2 中确保网络安全 》中的“如何设置暂挂 TCP 连接的最大数目”
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。	《在 Oracle Solaris 11.2 中确保网络安全 》中的“如何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。	如何使用 TCP 包装
配置防火墙。	使用 IP 过滤器功能可提供防火墙。	《在 Oracle Solaris 11.2 中确保网络安全 》中的第 4 章 “关于 Oracle Solaris 中的 IP 过滤器” 《在 Oracle Solaris 11.2 中确保网络安全 》中的第 5 章 “配置 IP 过滤器”
配置已验证的加密网络连接。	使用 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。	《在 Oracle Solaris 11.2 中确保网络安全 》中的第 7 章 “配置 IPsec” 《在 Oracle Solaris 11.2 中确保网络安全 》中的第 9 章 “配置 IKEv2”

▼ 如何使用 TCP 包装

以下步骤说明在 Oracle Solaris 中使用或者可以使用 TCP 包装的三种方式。

开始之前 必须承担 `root` 角色才能修改要使用 TCP 包装的程序。

1. 不需要保护具有 TCP 包装的 **`sendmail`** 应用程序。
   缺省情况下，该应用程序通过 TCP 包装进行保护，如《在 Oracle Solaris 11.2 中管理 sendmail 服务 》中的“sendmail 版本 8.12 支持 TCP 包装”中所述。

2. 要为所有 **`inetd`** 服务启用 TCP 包装，请参见《在 Oracle Solaris 11.2 中管理 TCP/IP 网络、IPMP 和 IP 隧道 》中的“如何使用 TCP 包装器控制对 TCP 服务的访问”。

3. 通过 TCP 包装保护 FTP 网络服务。

   a. 按照 **`/usr/share/doc/proftpd/modules/mod_wrap.html`** 模块中的说明操作。
      由于此模块是动态的，所以必须装入它才能与 FTP一起使用 TCP 包装。

   b. 通过将以下指令添加到 **`proftpd.conf`** 文件来装入该模块：

      ```
      # pfedit /etc/proftpd.conf
      <IfModule mod_dso.c>
          LoadModule mod_wrap.c
      </IfModule>
      ```

   c. 重新启动 FTP 服务。

      ```
      # svcadm restart svc:/network/ftp
      ```

保护文件系统

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配额。

`tmpfs` 文件系统可以无限制增长。要阻止拒绝服务 (Denial of Service, DoS) 攻击，请完成如何限制 `tmpfs` 文件系统的大小 [43]。

以下任务为 `tmpfs` 配置大小限制并概述了 ZFS（Oracle Solaris 中的缺省文件系统）中可用的保护。有关其他信息，请参见《在 Oracle Solaris 11.2 中管理 ZFS 文件系统 》中的“设置 ZFS 配额和预留空间”和 `zfs`(1M) 手册页。

表 2-4 保护文件系统任务列表

任务	描述	有关说明
通过管理和保留磁盘空间来阻止 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。	《在 Oracle Solaris 11.2 中管理 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。	《在 Oracle Solaris 11.2 中管理 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。	《在 Oracle Solaris 11.2 中管理 ZFS 文件系统 》中的“加密 ZFS 文件系统” 《在 Oracle Solaris 11.2 中管理 ZFS 文件系统 》中的“加密 ZFS 文件系统的示例”
限制 tmpfs 文件系统的大小。	阻止恶意用户通过在 /tmp 中创建大文件来降低系统速度。	如何限制 tmpfs 文件系统的大小 [43]

▼ 如何限制 tmpfs 文件系统的大小

缺省情况下，tmpfs 文件系统的大小不受限制。因此，tmpfs 可以不断增长，直至占满可用的系统内存和交换空间。因为 /tmp 目录供所有应用程序和用户使用，所以某个应用程序可能会占用所有可用系统内存。同样，恶意的非特权用户可能通过在 /tmp 目录中创建大文件来降低系统速度。为避免性能影响，您可以限制每个 tmpfs 挂载的大小。

您可以尝试多个值来获取最佳系统性能。

开始之前 要编辑 vfstab 文件，您必须成为分配有 solaris.admin.edit/etc/vfstab 授权的管理员。要重新引导系统，必须已为您指定了 "Maintenance and Repair"（维护和修复）权限配置文件。root 角色具有所有这些权限。有关更多信息，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“使用所指定的管理权限”。

1. **确定您系统的内存量。**

   注 - 以下示例所使用的 SPARC T3 系列系统配备具有更快 I/O 速率的固态驱动器 (Solid State Drive, SSD) 以及八个大小为 279.40 MB 的磁盘。系统大约有 500 GB 的内存。

```
% prtconf | head
System Configuration:  Oracle Corporation  sun4v
Memory size: 523776 Megabytes
System Peripherals (Software Nodes):

ORCL,SPARC-T3-4
scsi_vhci, instance #0
disk, instance #4
disk, instance #5
disk, instance #6
disk, instance #8
```

2. **计算 tmpfs 的内存限制。**

根据系统内存的大小，计算内存限制时您可能希望将大系统的阈值设为大约 20%，小系统的阈值设为大约 30%。

所以，对于较小的系统，请使用 .30 作为乘数。

```
10240M x .30 ≈ 340M
```

对于较大的系统，请使用 .20 作为乘数。

```
523776M x .20 ≈ 10475M
```

3. 使用该大小限制修改 **/etc/vfstab** 文件中的 **swap** 条目。

```
# pfedit /etc/vfstab
#device     device       mount       FS      fsck    mount mount
#to mount   to fsck      point       type    pass    at boot options
#
...
#swap       -            /tmp        tmpfs   -       yes     -
swap        -            /tmp        tmpfs   -       yes     size=10400m
/dev/zvol/dsk/rpool/swap   -      -  swap    -       no      -
```

4. 重新引导系统。

```
# reboot
```

5. 检验大小限制是否有效。

```
% mount -v
swap on /system/volatile type tmpfs
read/write/setuid/devices/rstchown/xattr/dev=89c0006 on Tues Feb 4 14:07:27 2014
swap on /tmp type tmpfs
read/write/setuid/devices/rstchown/xattr/size=10400m/dev=89c0006 on Tues ...
```

6. 监视内存使用情况并将大小限制调整至符合站点的要求。

df 命令颇为有用。swap 命令提供最有用的统计信息。

```
% df -h /tmp
Filesystem Size Used Available Capacity Mounted on
swap          7.  4G     44M    7.4G 1%       /tmp

% swap -s
total: 190248k bytes allocated + 30348k reserved = 220596k used,
7743780k available
```

有关更多信息，请参见 tmpfs(7FS)、mount_tmpfs(1M)、df(1M) 和 swap(1M) 手册页。

保护和修改文件

缺省情况下，只有 root 角色可以修改系统文件权限。分配有 solaris.admin.edit/*path-to-system-file* 授权的角色和用户可以修改 *system-file*。只有 root 角色可以搜索所有文件。

表 2-5 保护和修改文件任务列表

任务	描述	有关说明
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。	如何为一般用户设置限制性更强的 umask 值 [37]
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)
维护系统文件完整性。	通过脚本或使用 BART 查找未授权文件。	《在 Oracle Solaris 11.2 中确保文件的安全和确认文件完整性 》中的“如何查找具有特殊文件权限的文件”

保护系统访问和使用

可以配置 Oracle Solaris 安全功能，以保护对系统（包括系统和网络上的应用程序与服务）的使用。

表 2-6 保护系统访问和使用任务列表

任务	描述	有关说明
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。	《在 Oracle Solaris 11.2 中确保文件的安全和确认文件完整性 》中的“防止可执行文件危及安全”
确保标记用于地址空间布局随机化 (Address Space Layout Randomization, ASLR) 的二进制文件可以使用 ASLR。	为标记的二进制文件启用 ASLR。	如何验证 ASLR 是否已启用 [29]
配置审计。	定制审计配置以确保覆盖范围和文件完整性。	“使用审计服务” [50]
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。	《在 Oracle Solaris 11.2 中排除系统管理问题 》中的“启用文件路径” 《在 Oracle Solaris 11.2 中排除系统管理问题 》中的“管理核心文件规范”

任务	描述	有关说明
使用 SSL 内核代理保护 Web 服务器。	可以使用安全套接字层 (Secure Sockets Layer, SSL) 协议加密和加速 Web 服务器通信。	《在 Oracle Solaris 11.2 中确保网络安全 》中的第 3 章 “Web 服务器和安全套接字层协议”
创建区域以包含应用程序。	区域是隔离进程的容器。这些区域可以隔离应用程序以及应用程序的各个部分。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。	《Oracle Solaris Zones 介绍 》
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。	《在 Oracle Solaris 11.2 中进行资源管理 》

使用 SMF 保护传统服务

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，然后要求分配启动、刷新和停止服务的权限，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：

- 《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“使用扩展特权锁定资源”
- 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)`、`svcbundle(1M)` 和 `svccfg(1M)`。

配置 Kerberos 网络

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：

- 《在 Oracle Solaris 11.2 中管理 Kerberos 和其他验证服务 》中的第 3 章 “规划 Kerberos 服务”
- 《在 Oracle Solaris 11.2 中管理 Kerberos 和其他验证服务 》中的第 4 章 “配置 Kerberos 服务”
- 所选手册页包括 `kadmin(1M)`、`pam_krb5(5)` 和 `kclient(1M)`。

添加多级别标签安全

Trusted Extensions 通过执行基于标签的强制访问控制 (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

`system/trusted` 和 `system/trusted/trusted-global-zone` 软件包可满足无显示系统或不需要多级别桌面的服务器的需求。`system/trusted/trusted-extensions` 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。安装 `trusted-extensions` 软件包后，系统便可通过直接连接的位映射显示设备（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, “Trusted Extensions 的管理”

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：

- 《在 Oracle Solaris 11.2 中确保网络安全 》中的第 6 章 “关于 IP 安全体系结构”
- 《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“配置有标签的 IPsec”

♦ ♦ ♦ 第 3 章

3 维护和监视 Oracle Solaris 安全

执行初始安装和配置后，可以通过按照以下过程来维护和监视系统的安全状况：

- 定期检查审计记录
- 运行软件包和文件完整性检查
- 监视网络活动
- 运行遵从性检查

维护和监视系统安全

通过执行以下任务可维护并监视系统及数据的访问和使用情况以及系统是否符合站点的安全要求。

表 3-1 维护和监视系统任务列表

任务	描述	有关说明
验证系统上的软件包。	检查更新后的软件包是否与源软件包完全相同。	如何检验软件包 [28]
验证文件完整性。	配置之后，定期比较 BART 清单以确保只更改了应更改的文件。	“使用 BART 检验文件完整性” [49]
查找未授权文件。	查找可能未经授权在程序中使用 `setuid` 和 `setgid` 权限的情况。	《在 Oracle Solaris 11.2 中确保文件的安全和确认文件完整性 》中的“如何查找具有特殊文件权限的文件”
定期检查审计日志。	查找对系统的异常访问和使用。	“使用审计服务” [50]
实时检查审计日志中的登录和注销事件。	识别与尝试行为的发生时间接近的已尝试违规行为。	“实时监视审计记录” [51]
运行遵从性测试。	评估系统是否符合安全基准。	《Oracle Solaris 11.2 安全遵从性指南 》和 `compliance(1M)` 手册页

使用 BART 检验文件完整性

BART 是一个基于规则的文件完整性扫描和报告工具，它使用加密强度散列与文件系统元数据来报告更改。

有关信息和过程，请参见以下内容：

- 《在 Oracle Solaris 11.2 中确保文件的安全和确认文件完整性 》中的“关于 BART”
- 《在 Oracle Solaris 11.2 中确保文件的安全和确认文件完整性 》中的“关于使用 BART”
- 《在 Oracle Solaris 11.2 中确保文件的安全和确认文件完整性 》中的“BART 清单、规则文件和报告”

有关跟踪对已安装系统所做更改的具体说明，请参见《在 Oracle Solaris 11.2 中确保文件的安全和确认文件完整性 》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。

《在 Oracle Solaris 11.2 中管理审计 》中对审计服务进行了介绍。有关手册页及其链接的列表，请参见《在 Oracle Solaris 11.2 中管理审计 》中的“审计服务手册页”。

以下审计服务过程对许多安全环境都很有用：

- 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。将角色分配给可信用户。

  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。

  要创建角色或使用预定义的 ARMOR 角色，请参见《在 Oracle Solaris 11.2 中确保用户和进程的安全 》中的“为用户指定权限”。
- 使用 `cusa` 审计类审计所有管理员。

  `cusa` 审计类中的事件涵盖会影响系统安全状况的管理操作。有关说明，请参见 `/etc/security/audit_class` 文件。有关过程，请参见如何审计除登录/注销以外的重要事件 [38]。
- 将审计记录发送到中央服务器。
  - 将审计配置为与审计远程服务器 (Audit Remote Server, ARS) 配合使用。

    请参见《在 Oracle Solaris 11.2 中管理审计 》中的“如何向远程系统信息库发送审计文件”。
  - 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。
- 在 `syslog` 实用程序中监视所选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《在 Oracle Solaris 11.2 中管理审计 》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。

有关示例，请参见《在 Oracle Solaris 11.2 中管理审计 》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。

实时监视审计记录

通过 `audit_syslog` 插件，可以记录预选审计事件的摘要。要在审计摘要生成后在终端窗口中显示它们，请运行如下命令：

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

要配置审计日志，请参见《在 Oracle Solaris 11.2 中管理审计 》中的“如何配置 syslog 审计日志”。

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：

- 《在 Oracle Solaris 11.2 中管理审计 》中的“审计日志”
- 《在 Oracle Solaris 11.2 中管理审计 》中的“防止审计迹溢出”
- 《在 Oracle Solaris 11.2 中管理审计 》中的“显示审计迹数据”

♦ ♦ ♦ 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。在早期发行版的 Oracle Solaris 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 技术网上的安全参考资料

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

- 《在 Oracle Solaris 11.2 中确保系统和连接设备的安全 》
- 《在 Oracle Solaris 11.2 中确保文件的安全和确认文件完整性 》
- 《在 Oracle Solaris 11.2 中确保网络安全 》
- 《在 Oracle Solaris 11.2 中确保用户和进程的安全 》
- 《在 Oracle Solaris 11.2 中管理加密和证书 》
- 《在 Oracle Solaris 11.2 中管理审计 》
- 《在 Oracle Solaris 11.2 中管理 Kerberos 和其他验证服务 》
- 《在 Oracle Solaris 11.2 中管理安全 Shell 访问 》
- 《Oracle Solaris 11.2 安全遵从性指南 》
- 《Using a FIPS 140 Enabled System in Oracle Solaris 11.2 》

第三方出版物中的 Oracle Solaris 安全参考资料

以下书籍包含有关 Oracle Solaris 11 系统的安全介绍：

- 《*Security Configuration Benchmark For Solaris 11 11/11 Version 1.0.0 June 11th, 2012*》

  此安全基准由 Internet 安全中心 (Center for Internet Security, CIS) http://cisecurity.org/ 发布，供安全社区使用。此文档对 Oracle Solaris 操作系统 的安全设置提供了一些建议。目标读者包括系统和应用程序管理员、安全专家、审计人员、支持工程师以及开发、安装、评估或提供 Oracle Solaris 安全解决方案的安装人员和开发者。要获取副本，请访问 CIS Security Benchmarks (http://benchmarks.cisecurity.org/)（CIS 安全基准）。

- 《*Oracle Solaris 11 System Administration: The Complete Reference*》。由 Michael Jang、Harry Foxwell、Christine Tran 和 Alan Formy-Duval 合著。2012。McGraw-Hill 出版。ISBN 978007179042。

  这本普及版图书包含 Oracle Solaris 的安全性方面的内容。
- 《*Oracle Solaris 11: First Look*》。Philip P.Brown 著。 2013。Packt Publishing 出版。ISBN 9781849688307。

  这本普及版图书向管理员介绍了 Oracle Solaris 及其安全性。
- Bill Calkins 所著的《*Oracle Solaris 11 System Administration*》。2013。Prentice Hall 出版。ISBN 9780133007114。

  这本普及版图书涵盖 Oracle Solaris 的新功能（包括安全功能）。