

# **Oracle® Solaris 11 Security and Hardening Guidelines**



**Part No: E54807**  
November 2016



**Part No: E54807**

Copyright © 2011, 2016, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS. Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

**Documentation Accessibility**

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

**Access to Oracle Support**

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

**Référence: E54807**

Copyright © 2011, 2016, Oracle et/ou ses affiliés. Tous droits réservés.

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf stipulation expresse de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, accorder de licence, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Si ce logiciel, ou la documentation qui l'accompagne, est livré sous licence au Gouvernement des Etats-Unis, ou à quiconque qui aurait souscrit la licence de ce logiciel pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique:

U.S. GOVERNMENT END USERS. Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est pas conçu ni n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer des dommages corporels. Si vous utilisez ce logiciel ou matériel dans le cadre d'applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour ce type d'applications.

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés. Tout autre nom mentionné peut correspondre à des marques appartenant à d'autres propriétaires qu'Oracle.

Intel et Intel Xeon sont des marques ou des marques déposées d'Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. AMD, Opteron, le logo AMD et le logo AMD Opteron sont des marques ou des marques déposées d'Advanced Micro Devices. UNIX est une marque déposée d'The Open Group.

Ce logiciel ou matériel et la documentation qui l'accompagne peuvent fournir des informations ou des liens donnant accès à des contenus, des produits et des services émanant de tiers. Oracle Corporation et ses affiliés déclinent toute responsabilité ou garantie expresse quant aux contenus, produits ou services émanant de tiers, sauf mention contraire stipulée dans un contrat entre vous et Oracle. En aucun cas, Oracle Corporation et ses affiliés ne sauraient être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'accès à des contenus, produits ou services tiers, ou à leur utilisation, sauf mention contraire stipulée dans un contrat entre vous et Oracle.

**Accessibilité de la documentation**

Pour plus d'informations sur l'engagement d'Oracle pour l'accessibilité à la documentation, visitez le site Web Oracle Accessibility Program, à l'adresse <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

**Accès aux services de support Oracle**

Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> ou le site <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> si vous êtes malentendant.

# Contents

---

<b>Using This Documentation .....</b>	<b>11</b>
 <b>1 About Oracle Solaris Security .....</b>	<b>13</b>
What's New in Security Features in Oracle Solaris 11.3 .....	13
Oracle Solaris 11 Security After Installation .....	15
System Access Is Limited and Monitored .....	16
Kernel, File, and Desktop Protections Are in Place .....	16
Oracle Hardware Management Package .....	17
Oracle Solaris Configurable Security .....	17
Protecting Data .....	17
File Permissions and Access Control Entries .....	18
Cryptographic Services .....	18
Oracle Solaris ZFS File System .....	19
Protecting and Isolating Applications .....	19
Privileges in Oracle Solaris .....	20
Oracle Solaris Zones .....	20
Security Extensions .....	21
Service Management Facility .....	21
Java Cryptography Extension .....	22
Protecting Users and Assigning Additional Rights .....	22
Passwords and Password Constraints .....	22
Pluggable Authentication Modules .....	23
User Rights Management .....	23
Securing Network Communications .....	23
Packet Filtering .....	24
Remote Access .....	25
Maintaining System Security .....	27
Verified Boot .....	28
Package Integrity Verification .....	28
Audit Service .....	28
File Integrity Verification .....	29

Compliance to Security Standards .....	29
Log Files .....	29
Labeled Security .....	30
Trusted Extensions Feature in Oracle Solaris .....	30
Labeled Filesystem .....	30
Labeled Network Communications .....	31
Trusted Extensions Multilevel Desktop .....	31
Writing Applications That Run Securely .....	31
Security Standards and Evaluations .....	32
FIPS 140-2-2 Level 1 Cryptography Validation .....	32
Oracle Solaris 11 Common Criteria EAL4+ Certification .....	32
Site Security Policy and Practice .....	33
<b>2 Configuring Oracle Solaris Security .....</b>	<b>35</b>
Installing the Oracle Solaris OS .....	35
Initially Securing the System .....	36
▼ How to Verify Your Packages .....	37
▼ How to Disable Unneeded Services .....	38
▼ How to Remove Power Management Capability From Users .....	39
▼ How to Place a Security Message in Banner Files .....	40
Securing Users .....	41
▼ How to Set Stronger Password Constraints .....	41
▼ How to Set Account Locking for Regular Users .....	43
▼ How to Set a More Restrictive umask Value for Regular Users .....	45
▼ How to Audit Significant Events in Addition to Login/Logout .....	46
▼ How to Remove Unneeded Basic Privileges From Users .....	47
Protecting the Network .....	48
▼ How to Use TCP Wrappers .....	49
Protecting File Systems .....	50
▼ How to Limit the Size of the tmpfs File System .....	51
Protecting and Modifying Files .....	53
Securing System Access and Use .....	53
Protecting a Legacy Service With SMF .....	54
Configuring a Kerberos Network .....	54
Adding Labeled Multilevel Security .....	55
Configuring Trusted Extensions .....	55
Configuring Labeled IPsec .....	55
<b>3 Maintaining and Monitoring Oracle Solaris Security .....</b>	<b>57</b>

Maintaining and Monitoring System Security .....	57
Ensuring Secure Package Installation From Your Local IPS Repository .....	58
Using the Audit Service .....	58
<b>A Bibliography for Oracle Solaris Security .....</b>	<b>61</b>
Security References on the Oracle Technology Network .....	61
Oracle Solaris Security References in Third-Party Publications .....	61
<b>Index .....</b>	<b>63</b>





# Tables

---

TABLE 1	Securing the System Task Map .....	36
TABLE 2	Securing Users Task Map .....	41
TABLE 3	Configuring the Network Task Map .....	49
TABLE 4	Protecting File Systems Task Map .....	50
TABLE 5	Protecting and Modifying Files Task Map .....	53
TABLE 6	Securing System Access and Use Task Map .....	53
TABLE 7	Maintaining and Monitoring the System Task Map .....	57



## Using This Documentation

---

- **Overview** – Provides an overview of Oracle Solaris security features and the guidelines for using those features to harden and protect an installed system and its applications.
- **Audience** – System administrators, security administrators, application developers, and auditors who develop, deploy, or assess security on Oracle Solaris 11 systems.
- **Required knowledge** – Site security requirements.

## Product Documentation Library

Documentation and resources for this product and related products are available at <http://www.oracle.com/pls/topic/lookup?ctx=E53394>.

## Feedback

Provide feedback about this documentation at <http://www.oracle.com/goto/docfeedback>.



## About Oracle Solaris Security

---

Oracle Solaris is a robust, premier enterprise operating system that offers proven security features. With a sophisticated network-wide security system that controls the way users access files, protect system databases, and use system resources, Oracle Solaris 11 addresses security requirements at every layer. While traditional operating systems can contain inherent security weaknesses, the flexibility of Oracle Solaris 11 enables it to satisfy a variety of security objectives from enterprise servers to desktop clients. Oracle Solaris is fully tested and supported on a variety of SPARC and x86-based systems from Oracle and on other hardware platforms from third-party vendors.

- [“What's New in Security Features in Oracle Solaris 11.3” on page 13](#)
- [“Oracle Solaris 11 Security After Installation” on page 15](#)
- [“Protecting Data” on page 17](#)
- [“Protecting and Isolating Applications” on page 19](#)
- [“Protecting Users and Assigning Additional Rights” on page 22](#)
- [“Securing Network Communications” on page 23](#)
- [“Maintaining System Security” on page 27](#)
- [“Labeled Security” on page 30](#)
- [“Writing Applications That Run Securely” on page 31](#)
- [“Security Standards and Evaluations” on page 32](#)
- [“Site Security Policy and Practice” on page 33](#)

### What's New in Security Features in Oracle Solaris 11.3

This section highlights information for existing customers about important new security features in this release.

- Oracle Solaris protects the password to the GRUB menu. For more information, see [“Password-Protecting the GRUB Menu” in \*Booting and Shutting Down Oracle Solaris 11.3 Systems\*](#).
- On SPARC multidomain series servers where the TPM resides on the SP/SPP board, the TPM can fail over to a spare board. For more information, see [“TPM Failover Option” in \*Securing Systems and Attached Devices in Oracle Solaris 11.3\*](#).

- You can use verified boot to secure a kernel zone's boot process. Verified boot protects a kernel zone from corrupted kernel zone modules, malicious programs, and installation of unauthorized third-party kernel modules by securely loading Oracle Solaris kernel modules before execution. For more information, see [“Using Verified Boot to Secure an Oracle Solaris Kernel Zone”](#) in *Creating and Using Oracle Solaris Kernel Zones*.
- You can encrypt the live migration of zones on SPARC and x86 platforms. Called *secure live migration*, encrypted live migration is the default. For more information, see [“About Secure Live Migration”](#) in *Creating and Using Oracle Solaris Kernel Zones*.
- When you first log in to a desktop session, a dialog box informs you of your last login time and location. This notification if an unauthorized login has occurred is a good security practice and commonly required by various security policies. For more information, see the [pam\\_unix\\_session\(5\)](#) man page.
- You can create an encrypted password, or *password hash*, by using the `pwhash` command. You can then provide the password during an initial boot sequence in Automatic Installation (AI). You can also pass the hash to the `passwd` command by using the `-p` option. See the [pwhash\(1\)](#) and [passwd\(1\)](#) man pages and [“Configuring Root and User Accounts”](#) in *Installing Oracle Solaris 11.3 Systems*.
- Compliance rules that are coded with variable values enable you to create tailorings whose rules check for the precise values that satisfy site security requirements. See [“Selecting Alternate Values for Variables in Compliance Rules”](#) in *Oracle Solaris 11.3 Security Compliance Guide* and the [compliance-tailor\(1M\)](#) man page.
- You can schedule compliance assessments to run periodically. This functionality is disabled by default. See [“Running Assessments at Regular Intervals”](#) in *Oracle Solaris 11.3 Security Compliance Guide* and the [compliance\(1M\)](#) man page.
- Protecting executables from stack corruption is now a security extension in Oracle Solaris rather than the `no_exec_userstack` system variable that previously was set in the `/etc/system` file. The `nxstack` security extension is set by default. In addition, the `nxheap` security extension protects from heap corruption. For more information, see the [“Protecting the Process Heap and Executable Stacks From Compromise”](#) in *Securing Systems and Attached Devices in Oracle Solaris 11.3*.
- The Cryptographic Framework now includes the Camellia algorithm. To view the mechanisms that Camellia supports, run the `cryptoadm list -m | grep camellia` command. The SPARC T4 Series servers provide hardware acceleration for this algorithm.
- The Kernel SSL proxy supports SSLv3, but disables it by default. See [“SSL Kernel Proxy Encrypts Web Server Communications”](#) in *Securing the Network in Oracle Solaris 11.3*.
- Packet Filter supports policy-based routing (PBR). For more information, see the route-to description in [“Packet Filter Rule Optional Actions”](#) in *Securing the Network in Oracle Solaris 11.3*.
- You can use the `elfsign` utility to sign providers by using an external mechanism such as a separate central signing service. For more information, see [“Elfsign Support for External Signing”](#) in *Managing Encryption and Certificates in Oracle Solaris 11.3* and the [elfsign\(1\)](#) man page.

- The `pktool gencsr` command can now create certificates for certificate authorities that do not follow the standard [PKCS #10: Certification Request Syntax Specification \(http://www.ietf.org/rfc/rfc2986.txt\)](http://www.ietf.org/rfc/rfc2986.txt). See the `pktool(1)` man page.
- Oracle Solaris offers an `openssh` implementation of Secure Shell. This OpenSSH implementation is built on OpenSSH 6.5p1 plus additional features. The `sunssh` implementation is still the default. You use the `pkg mediator` command to switch between the two implementations. For more information, see [Chapter 1, “Using Secure Shell” in \*Managing Secure Shell Access in Oracle Solaris 11.3\*](#).
- To aid in making the transition to IPsec and IKEv2, Oracle Solaris provides the `pass` action and the `ike_version` option. The `pass` action enables a server to support IPsec and non-IPsec clients, and the `ike_version` option enables you to specify the version of the IKE protocol that an IPsec policy rule must use. This option helps a network run two versions of the IKE protocol and require the newer IKE protocol on only those systems that can support it. For information and links to examples, see [“What’s New in Network Security in Oracle Solaris 11.3” in \*Securing the Network in Oracle Solaris 11.3\*](#).
- Oracle Solaris provides an additional firewall option, the OpenBSD Packet Filter. For more information, see [Chapter 4, “OpenBSD Packet Filter Firewall in Oracle Solaris” in \*Securing the Network in Oracle Solaris 11.3\*](#).
- You can create a version or *tailoring* of an existing benchmark. Tailorings can provide an accurate assessment of the security posture of particular systems by removing failures and false positives from the assessment. For more information, see [Oracle Solaris 11.3 Security Compliance Guide](#) and the `compliance(1M)` and `compliance-tailor(1M)` man pages.
- Oracle Solaris provides the `pkg:/support/critical-patch-update/solaris-11-cpu` package to enable you to update your system to the latest critical patch updates that repair Common Vulnerabilities and Exposures (CVE). See [“Administering CVE Updates in Oracle Solaris” in \*Oracle Solaris 11.3 Security Compliance Guide\*](#) and [“Applying Support Updates” in \*Adding and Updating Software in Oracle Solaris 11.3\*](#).
- The `dax_access` privilege enables data analytics acceleration on the DAX co-processors on SPARC M7 and SPARC T7 series servers for Oracle Database 12c. A database given this privilege can offload parts of query processing to the server hardware.

## Oracle Solaris 11 Security After Installation

Oracle Solaris is installed “secure by default” (SBD). This security posture protects the system from intrusion and monitors login attempts, among other security features.

## System Access Is Limited and Monitored

**Initial user and root role accounts** – The initial user account can log in from the console. This account is assigned the root role. The password for the initial user and the root accounts is identical at installation.

- After logging in, the initial user can assume the root role to further configure the system. Upon assuming the role, the user is prompted to change the root password. Note that no role can log in directly, including the root role.
- The initial user is assigned defaults from the `/etc/security/policy.conf` file. The defaults include the Basic Solaris User rights profile and the Console User rights profile. These rights profiles enable users to read and write to a CD or DVD, run any command on the system without privilege, and stop and restart their system when sitting at the console.
- The initial user account is also assigned the System Administrator rights profile. Therefore, without assuming the root role, the initial user has some administrative rights, such as the right to install software and manage the naming service.

**Password requirements** – User passwords must be at least six characters long, and have at least two alphabetic characters and one non-alphabetic character. Passwords are hashed by using the SHA256 algorithm. When changing their password, all users including the root role must conform to these password requirements.

**Limited network access** – After installation, the system is protected from intrusion over the network. Remote login by the initial user is allowed over an authenticated, encrypted connection with the Secure Shell protocol. This is the only network protocol that accepts incoming packets. The Secure Shell key is wrapped by the AES128 algorithm. With encryption and authentication in place, the user can reach the remote system without interception, modification, or spoofing.

**Recorded login attempts** – The audit service is enabled for all login/logout events (login, logout, switching user, starting and stopping a Secure Shell session, and screen locking) and for all non-attributable (failed) logins. Because the root role cannot log in, the name of the user who is acting as root is recorded in the audit trail. The initial user can review the audit logs by a right granted through the System Administrator rights profile.

## Kernel, File, and Desktop Protections Are in Place

After the initial user is logged in, the kernel, file systems, system files, and desktop applications are protected by file permissions, privileges, and user rights. User rights are also known as *role-based access control* (RBAC).

**Kernel protections** – Many daemons and administrative commands are assigned just the privileges that enable them to succeed. Many daemons are run from special administrative



accounts that do not have root (UID=0) privileges, so they cannot be hijacked to perform other tasks. These special administrative accounts cannot log in. Devices are protected by privileges.

**File systems** – By default, all file systems are ZFS file systems. The user's umask is 022, so when a user creates a new file or directory, only the user is allowed to modify it. Members of the user's group are allowed to read and search the directory, and read the file. Logins that are outside the user's group can list the directory and read the file. The default directory permissions are drwxr-xr-x (755). The file permissions are -rw-r--r-- (644).

**System files** – System configuration files are protected by file permissions. Only the root role or a user who is assigned the right to edit a specific system file can modify a system file.

**Desktop applets** – Desktop applets are protected by rights management. Therefore, administrative actions, such as the addition of remote printers in Print Manager, are restricted to users and roles who have administrative rights for printing.

## Oracle Hardware Management Package

The Oracle Hardware Management Package provides a set of utilities for configuring, managing, and monitoring Oracle servers. This value-add set of tools for Oracle hardware is always available. It can automatically deliver certain hardware-related information to ILOM to complete the view that it has of system hardware. For information about the utilities and security, see the [Systems Management and Diagnostics Documentation](http://www.oracle.com/goto/ohmp/docs) (<http://www.oracle.com/goto/ohmp/docs>).

## Oracle Solaris Configurable Security

In addition to the solid foundation that Oracle Solaris security defaults provide, the security posture of a Oracle Solaris system is highly configurable to satisfy a range of security requirements.

The following sections provide a short introduction to the security features of Oracle Solaris. The descriptions include references to more detailed explanations and to procedures in this guide and other Oracle Solaris system administration guides that demonstrate these features.

## Protecting Data

Oracle Solaris protects data from booting through installation, use, and archiving.

## File Permissions and Access Control Entries

The first line of defense for protecting objects in a file system are the default UNIX permissions that are assigned to every file system object. UNIX permissions support assigning unique access rights to the owner of the object, to a group assigned to the object, as well as to anyone else. Additionally, the default file system, ZFS, supports access control lists (ACLs), which more finely control access to individual or groups of file system objects.

For more information, see the following:

- For an overview of file permissions, see [“Using UNIX Permissions to Protect Files” in \*Securing Files and Verifying File Integrity in Oracle Solaris 11.3\*](#).
- For a description of security-relevant ZFS file attributes, see [“Using File Attributes to Add Security to ZFS Files” in \*Securing Files and Verifying File Integrity in Oracle Solaris 11.3\*](#) and the man pages.
- For an overview and examples of protecting ZFS files, see [Chapter 9, “Using ACLs and Attributes to Protect Oracle Solaris ZFS Files” in \*Managing ZFS File Systems in Oracle Solaris 11.3\*](#) and the man pages.
- For instructions about setting ACLs on ZFS files, see the [`chmod\(1\)`](#) man page.

## Cryptographic Services

The Cryptographic Framework feature of Oracle Solaris and the Key Management Framework (KMF) feature of Oracle Solaris provide central repositories for cryptographic services and key management. Hardware, software, and end users have seamless access to optimized algorithms. KMF provides a unified interface for otherwise different storage mechanisms, administrative utilities, and programming interfaces for various public key infrastructures (PKIs).

The Cryptographic Framework provides a common store of algorithms and PKCS #11 libraries to handle cryptographic requirements. The PKCS #11 libraries are implemented according to the RSA Security Inc. PKCS #11 Cryptographic Token Interface (Cryptoki) standard. Cryptographic services, such as encryption and decryption for files, are available to regular users.

KMF provides tools and programming interfaces for centrally managing public key objects, such as X.509 certificates and public/private key pairs. The formats for storing these objects can vary. KMF also provides a tool for managing policies that define the use of X.509 certificates by applications. KMF supports third-party plugins.

For more information, see the following:

- Selected man pages include [`cryptoadm\(1M\)`](#), [`digest\(1\)`](#), [`encrypt\(1\)`](#), [`mac\(1\)`](#), [`pktool\(1\)`](#), and [`kmfcfg\(1\)`](#).

- For an overview of cryptographic services, see [Chapter 1, “Cryptographic Framework” in \*Managing Encryption and Certificates in Oracle Solaris 11.3\*](#) and [Chapter 4, “Key Management Framework” in \*Managing Encryption and Certificates in Oracle Solaris 11.3\*](#).
- For examples of using the Cryptographic Framework, see [Chapter 3, “Cryptographic Framework” in \*Managing Encryption and Certificates in Oracle Solaris 11.3\*](#) and the man pages.
- To enable the Cryptographic Framework FIPS 140-2 provider, see [“How to Create a Boot Environment with FIPS 140 Enabled” in \*Managing Encryption and Certificates in Oracle Solaris 11.3\*](#).

## Oracle Solaris ZFS File System

ZFS is the default file system for Oracle Solaris 11. The ZFS file system fundamentally changes the way Oracle Solaris file systems are administered. ZFS is robust, scalable, and easy to administer. Because file system creation in ZFS is lightweight, you can easily establish quotas and reserved space. UNIX permissions and ACLs protect files, and you can encrypt the entire dataset at creation. Oracle Solaris rights management supports the delegated administration of ZFS datasets, that is, users who are assigned a limited set of privileges can administer ZFS datasets.

For more information, see the following:

- [“User Rights Management” in \*Securing Users and Processes in Oracle Solaris 11.3\*](#)
- [Chapter 1, “Introducing the Oracle Solaris ZFS File System” in \*Managing ZFS File Systems in Oracle Solaris 11.3\*](#)
- [“Oracle Solaris ZFS Features” in \*Managing ZFS File Systems in Oracle Solaris 11.3\*](#)
- [Chapter 7, “Managing Oracle Solaris ZFS File Systems” in \*Managing ZFS File Systems in Oracle Solaris 11.3\*](#)
- [“How to Remotely Administer ZFS With Secure Shell” in \*Managing Secure Shell Access in Oracle Solaris 11.3\*](#)
- Selected man pages include [zfs\(1M\)](#) and [zfs\(7FS\)](#).

## Protecting and Isolating Applications

Applications can be entry points for malware and malicious users. In Oracle Solaris, these threats are mitigated by the use of privileges and the containment of applications within zones. Applications can run with just the privileges that the application needs, so a malicious user does not have root privileges to access the rest of the system. Zones can limit the extent of an attack. Attacks on applications in a non-global zone can affect processes in that zone only, not the zone's host system.

Security extensions, such as address space layout randomization (ASLR), `nxheap`, and `nxstack` make it difficult for intruders to compromise an executable or the heap. For more information, see [“Security Extensions” on page 21](#). The Service Management Facility (SMF) also protects applications by enabling administrators to restrict starting, stopping, and using an application.

## Privileges in Oracle Solaris

Privileges are fine-grained, discrete rights on processes that are enforced in the kernel. Oracle Solaris defines over 80 privileges, ranging from basic privileges like `file_read` to more specialized privileges like `proc_clock_highres`. Privileges can be granted to a process, a user, or a role. Many Oracle Solaris commands and daemons run with just the privileges that are required to perform their task. Privilege-aware programs can prevent intruders from gaining more privileges than the program itself uses.

The use of privileges is also called *process rights management*. Privileges enable organizations to specify, hence limit, which privileges are granted to services and processes that run on their systems.

For more information, see the following:

- [“Process Rights Management” in \*Securing Users and Processes in Oracle Solaris 11.3\*](#)
- [Chapter 2, “Developing Privileged Applications” in \*Developer’s Guide to Oracle Solaris 11 Security\*](#)
- Selected man pages include `ppriv(1)` and `privileges(5)`.

## Oracle Solaris Zones

The Oracle Solaris Zones software partitioning technology enables you to maintain the one-application-per-server deployment model while simultaneously sharing hardware resources.

Zones are virtualized operating environments that enable multiple applications to run in isolation from each other on the same physical hardware. This isolation prevents processes that run within a zone from monitoring or affecting processes that run in other zones, viewing each other's data, or manipulating the underlying hardware. Zones also provide an abstraction layer that separates applications from physical attributes of the system on which they are deployed, such as physical device paths and network interface names.

For added protection, physical global zones, called Immutable Global Zones, and virtual global zones, called Oracle Solaris Kernel Zones, can be read-only. Immutable global zones are slightly more powerful than Kernel Zones, but neither can permanently change the hardware or configuration of the system. Read-only zones boot faster and are more secure than zones that allow writes.

For maintenance, immutable global zones define a special set of processes, called the Trusted Computing Base (TCB) that can be configured through a protected login called the Trusted Path. For more information, see [Chapter 11, “Configuring and Administering Immutable Zones”](#) in *Creating and Using Oracle Solaris Zones*. For information about zone configuration resources, see *Introduction to Oracle Solaris Zones*. See also the [mwac\(5\)](#) and [tpd\(5\)](#) man pages.

Oracle Solaris Kernel Zones are useful for deploying a compliant system. For example, you can configure a compliant system, create a Unified Archive, then deploy the image as a kernel zone. For more information, see the [solaris-kz\(5\)](#) man page, *Creating and Using Oracle Solaris Kernel Zones*, “Oracle Solaris Zones Overview” in *Introduction to Oracle Solaris 11 Virtual Environments*, and *Using Unified Archives for System Recovery and Cloning in Oracle Solaris 11.3*.

For more information, see the following:

- “Configuring Read-Only Zones” in *Creating and Using Oracle Solaris Zones*
- *Introduction to Oracle Solaris Zones*
- Selected man pages include [brands\(5\)](#), [zoneadm\(1M\)](#), and [zonecfg\(1M\)](#).

## Security Extensions

Oracle Solaris security extensions are flags at the kernel level that protect the stack and the heap from compromise. Address space layout randomization (ASLR) randomizes the addresses that are used by a given program. The `nxheap` and `nxstack` security extensions prevent corruption of executables stacks and the heap by malicious code. For more information, see “Address Space Layout Randomization” in *Securing Systems and Attached Devices in Oracle Solaris 11.3* and “Protecting the Process Heap and Executable Stacks From Compromise” in *Securing Systems and Attached Devices in Oracle Solaris 11.3*. For how to use these security extensions when compiling applications, follow the links in “Writing Applications That Run Securely” on page 31.

## Service Management Facility

*Services* are persistently running applications. A service can represent a running application, the software state of a device, or a set of other services. The Service Management Facility (SMF) feature of the Oracle Solaris is used to add, remove, configure, and manage services. SMF uses rights management to control access to service management functions on the system. In particular, SMF uses authorizations to determine who can manage a service and what functions that person can perform.

SMF enables organizations to control access to services, as well as to control how those services are started, stopped, and refreshed.

For more information, see the following:

- [Managing System Services in Oracle Solaris 11.3](#)
- “How to Assign Specific Privileges to the Apache HTTP Server” in [Securing Users and Processes in Oracle Solaris 11.3](#)
- Selected man pages include [svcadm\(1M\)](#), [svcs\(1\)](#), and [smf\(5\)](#).

## Java Cryptography Extension

Java provides the Java Cryptography Extension (JCE) for developers of Java applications. For more information, see [Java SE Security \(http://www.oracle.com/technetwork/java/javase/tech/index-jsp-136007.html\)](http://www.oracle.com/technetwork/java/javase/tech/index-jsp-136007.html).

## Protecting Users and Assigning Additional Rights

Users are assigned a basic set of privileges, rights profiles, and authorizations from the `/etc/security/policy.conf` file, similar to the initial user as described in [“System Access Is Limited and Monitored” on page 16](#). These rights are configurable. You can deny basic rights and increase the rights for a user.

Oracle Solaris protects users with flexible complexity requirements for passwords, authentication that is configurable for different site requirements, and user rights management, which uses rights profiles, authorizations, and privileges to limit and distribute administrative rights to trusted users. Additionally, special shared accounts called *roles* assign the user just those administrative rights when the user assumes the role. The [Authorization Rules Managed On RBAC \(ARMOR\)](#) package provides predefined roles.

## Passwords and Password Constraints

Strong user passwords help defend against attacks involving brute force guessing. Oracle Solaris provides several features that you can use to configure user passwords to industry standards and to your site requirements.

For more information, see the following:

- [“Maintaining Login Control” in Securing Systems and Attached Devices in Oracle Solaris 11.3](#)
- [“Securing Logins and Passwords” in Securing Systems and Attached Devices in Oracle Solaris 11.3](#)
- Selected man pages include [passwd\(1\)](#) and [crypt.conf\(4\)](#).

## Pluggable Authentication Modules

The Pluggable Authentication Module (PAM) framework enables administrators to coordinate and configure user authentication requirements for accounts, credentials, sessions, and passwords without modifying the services that require authentication.

The PAM framework enables organizations to customize the user authentication experience as well as account, session, and password management functionality. System entry services such as `login` and `ssh` use the PAM framework to secure all entry points for the freshly installed system. PAM enables the replacement or modification of authentication modules in the field to secure the system against any newly found weaknesses without requiring changes to any system services that use the PAM framework.

Oracle Solaris delivers a broad set of PAM modules and configurations to meet most site policies. For more information, see the following:

- [Chapter 1, “Using Pluggable Authentication Modules” in \*Managing Kerberos and Other Authentication Services in Oracle Solaris 11.3\*](#)
- [“Writing Applications That Use PAM Services” in \*Developer’s Guide to Oracle Solaris 11 Security\*](#)
- `pam.conf(4)` man page

## User Rights Management

User rights in Oracle Solaris are governed by the security principle of least privilege. Organizations can selectively grant administrative rights to users or roles according to the unique needs and requirements of the organization. They can also deny rights to users when required. Rights are implemented as privileges on processes and authorizations on users or SMF methods. Rights profiles provide a convenient way to collect privileges and authorizations into a bundle of related rights.

For more information, see the following:

- [Securing Users and Processes in Oracle Solaris 11.3](#)
- Selected man pages include `auths(1)`, `privileges(5)`, `profiles(1)`, `rbac(5)`, `roleadd(1M)`, `roles(1)`, and `user_attr(4)`.

## Securing Network Communications

Network communications can be protected by features such as firewalls, TCP wrappers on networked applications, and encrypted and authenticated remote connections.

## Packet Filtering

Packet filtering provides basic protection against network-based attacks. Oracle Solaris includes the OpenBSD Packet Filter, the IP Filter feature, and TCP wrappers.

### OpenBSD Packet Filter Firewall

The OpenBSD Packet Filter (PF) feature of Oracle Solaris is a network firewall that captures inbound packets and evaluates them for entry to and exit from the system. PF provides stateful packet inspection. It can match packets by IP address and port number as well as by the receiving network interface.

PF is based on OpenBSD Packet Filter version 5.5, which is enhanced to work with Oracle Solaris components, such as zones with exclusive IP instances. In Oracle Solaris 11.3, both PF and IP Filter are available for filtering packets.

For more information, see the following:

- For an overview, see [Chapter 4, “OpenBSD Packet Filter Firewall in Oracle Solaris” in \*Securing the Network in Oracle Solaris 11.3\*](#).
- For examples of using PF, see [Chapter 5, “Configuring the Packet Filter Firewall” in \*Securing the Network in Oracle Solaris 11.3\*](#) and the man pages.

### IP Filter Firewall

The IP Filter feature of Oracle Solaris creates a firewall to ward off network-based attacks.

Specifically, IP Filter provides stateful packet filtering capabilities and can filter packets by IP address or network, port, protocol, network interface, and traffic direction. It also includes stateless packet filtering and the capability to create and manage address pools. In addition, IP Filter also has the capability to perform network address translation (NAT) and port address translation (PAT).

For more information, see the following:

- For an overview of IP Filter, see [Chapter 6, “IP Filter Firewall in Oracle Solaris” in \*Securing the Network in Oracle Solaris 11.3\*](#).
- For examples of using IP Filter, see [Chapter 7, “Configuring IP Filter Firewall” in \*Securing the Network in Oracle Solaris 11.3\*](#) and the man pages.
- For information and examples about the syntax of the IP Filter policy language, see the [ipnat\(4\)](#) man page.



- Selected man pages include [ipfilter\(5\)](#), [ipf\(1M\)](#), [ipnat\(1M\)](#), [svc.ipfd\(1M\)](#), and [ipf\(4\)](#).

## TCP Wrappers

TCP wrappers provide access control for internet services. When various internet (`inetd`) services are enabled, the `tcpd` daemon checks the address of a host requesting a particular network service against an ACL. Requests are granted or denied accordingly. TCP wrappers also log host requests for network services in `syslog`, which is a useful monitoring function.

The Secure Shell and `sendmail` features of Oracle Solaris are configured to use TCP wrappers. Network services that have a one-to-one mapping to executable files, such as `proftpd` and `rpcbind`, are candidates for TCP wrappers.

TCP wrappers support a rich configuration policy language that enables organizations to specify security policy not only globally but on a per-service basis. Further access to services can be permitted or restricted based upon host name, IPv4 or IPv6 address, netgroup name, network, and even DNS domain.

For information about TCP wrappers, see the following:

- [“How to Use TCP Wrappers” on page 49](#)
- For information and examples of the syntax of the access control language for TCP wrappers, see the `hosts_access(4)` man page.
- Selected man pages include `tcpd(1M)` and [inetd\(1M\)](#).

## Remote Access

Remote access attacks can damage a system and a network. Oracle Solaris provides defense in depth for network transmissions. Defense features include encryption and authentication checks for data transmission, login authentication, and the disabling of unnecessary remote services.

## IPsec and IKE

IP security (IPsec) protects network transmissions by authenticating the IP packets, by encrypting them, or by doing both. Because IPsec is implemented well below the application layer, Internet applications can take advantage of IPsec without requiring modifications to their code.

IPsec and its automatic key exchange protocol, IKE, use algorithms from the Cryptographic Framework. Additionally, the Cryptographic Framework provides a central keystore. When

IKE is configured to use the metaslot, organizations have the option of storing the keys on disk, on an attached hardware keystore, or in a software keystore called *softtoken*. Oracle Solaris supports both the IKE Version 2 (IKEv2) protocol and the IKEv1 protocol.

IPsec and IKE require configuration, so are installed but not enabled by default. When properly administered, IPsec is an effective tool in securing network traffic.

For more information, see the following:

- [Chapter 8, “About IP Security Architecture” in \*Securing the Network in Oracle Solaris 11.3\*](#)
- [Chapter 9, “Configuring IPsec” in \*Securing the Network in Oracle Solaris 11.3\*](#)
- [“IPsec and FIPS 140-2” in \*Securing the Network in Oracle Solaris 11.3\*](#)
- [Chapter 10, “About Internet Key Exchange” in \*Securing the Network in Oracle Solaris 11.3\*](#)
- [Chapter 11, “Configuring IKEv2” in \*Securing the Network in Oracle Solaris 11.3\*](#)
- Selected man pages include [ipseccomp\(1M\)](#) and [in.iked\(1M\)](#).

## Secure Shell

By default, the Secure Shell feature of Oracle Solaris is the only active remote access mechanism on a newly installed system. All other network services are either disabled or in listen-only mode.

The current Oracle Solaris release includes both the default sunssh implementation of Secure Shell and a new openssh implementation of Secure Shell that is built on OpenSSH 6.5p1 plus additional features.

Secure Shell creates an encrypted communications channel between systems. Secure Shell can also be used as an on-demand virtual private network (VPN) that can forward X Window system traffic or can connect individual port numbers between a local system and remote systems over an authenticated and encrypted network link.

Thus, Secure Shell prevents a would-be intruder from being able to read an intercepted communication and prevents an adversary from spoofing the system.

For more information, see the following:

- [Chapter 1, “Using Secure Shell” in \*Managing Secure Shell Access in Oracle Solaris 11.3\*](#)
- [“Secure Shell and FIPS 140” in \*Managing Secure Shell Access in Oracle Solaris 11.3\*](#)
- Selected man pages include [ssh\(1\)](#), [sshd\(1M\)](#), [sshd\\_config\(4\)](#), and [ssh\\_config\(4\)](#).

---

**Note** - When these man pages display online, they describe the implementation of Secure Shell that is enabled on your system.

---

## Kerberos Service

The Kerberos feature of the Oracle Solaris enables single sign-on and secure transactions, even over heterogeneous networks where systems run different operating systems and run the Kerberos service. You can install Kerberos clients by using AI, so that the client is a Kerberized system at first boot.

Kerberos is based on the Kerberos V5 network authentication protocol that was developed at the Massachusetts Institute of Technology (MIT). The Kerberos service offers strong user authentication, as well as integrity and privacy. Using the Kerberos service, you can log in once and access other systems, execute commands, exchange data, and transfer files securely. Additionally, the service enables administrators to restrict access to services and systems.

For more information, see the following:

- “How to Configure Kerberos Clients Using AI” in *Installing Oracle Solaris 11.3 Systems*[Managing Kerberos and Other Authentication Services in Oracle Solaris 11.3](#)
- [Managing Kerberos and Other Authentication Services in Oracle Solaris 11.3](#)
- “FIPS 140-2 Algorithms and Kerberos Encryption Types” in *Managing Kerberos and Other Authentication Services in Oracle Solaris 11.3*
- Selected man pages include [kadmin\(1M\)](#), [kdcmgr\(1M\)](#), [kerberos\(5\)](#), [kinit\(1\)](#), and [krb5.conf\(4\)](#).

## Maintaining System Security

Oracle Solaris provides the following features to maintain the security of a system:

- Verified boot – Secures the boot process. Verified boot is disabled by default.
- Repository verification – Verifies that your local IPS repository files are valid.
- Package verification – Verifies that the installed packages are valid.
- Audit service – Audits access and use of the system. Auditing is enabled by default.
- File integrity verification – BART manifests can list every file on the system, and comparisons of manifests are used to verify that file integrity is maintained.
- Compliance reports – Oracle Solaris provides several security benchmarks against which to assess your system. These assessments produce reports that help you evaluate the security posture of the system.
- Log files – SMF provides log files for every service. To locate the log file for a service, run the `svcs -L service` command. The `syslog` utility provides a central file for naming and configuring logs for system services and can optionally notify administrators of critical events. Other features, such as auditing, also create their own logs. For example, you can display package summary information with the `pkg history` command.

## Verified Boot

Verified boot is an Oracle Solaris feature that secures a system's boot process and protects the system from threats such as the installation of unauthorized kernel modules and trojan applications. By default, verified boot is disabled.

For more information, see [“Using Verified Boot” in \*Securing Systems and Attached Devices in Oracle Solaris 11.3\*](#) and [“Using Verified Boot to Secure an Oracle Solaris Kernel Zone” in \*Creating and Using Oracle Solaris Kernel Zones\*](#).

## Package Integrity Verification

You can verify package integrity before and after installation. If you are using a local IPS repository, you can run the `pkgrepo verify` command to verify that the repository is not corrupted. With any signature policy other than `ignore`, the command verifies that signed packages are correctly signed.

After installing or updating packages, you can run the `pkg verify` command to ensure that the packages on your system did not install files with incorrect ownership or hashes, for example. With any signature policy other than `ignore`, the command verifies that signed packages are correctly signed.

For more information, see the following:

- [“Properties for Signing Packages” in \*Adding and Updating Software in Oracle Solaris 11.3\*](#)
- [Copying and Creating Package Repositories in Oracle Solaris 11.3](#)
- `pkg(1)` man page
- [“Maintaining and Monitoring System Security” on page 57](#)
- [“How to Verify Your Packages” on page 37](#)

## Audit Service

Oracle Solaris provides an audit service that collects data about system access and use. The audit data provides a reliable time-stamped log of security-related system events. This data can then be used to assign responsibility for actions that take place on a system.

Auditing is a basic requirement for security evaluation, validation, compliance, and certification bodies. Auditing can also provide a deterrent to potential intruders.

For more information, see the following:

- For a list of audit-related man pages, see [Chapter 7, “Auditing Reference” in \*Managing Auditing in Oracle Solaris 11.3\*](#).

- For guidelines, see [“How to Audit Significant Events in Addition to Login/Logout” on page 46](#) and the man pages.
- For an overview of auditing, see [Chapter 1, “About Auditing in Oracle Solaris” in \*Managing Auditing in Oracle Solaris 11.3\*](#).
- For auditing tasks, see [Chapter 3, “Managing the Audit Service” in \*Managing Auditing in Oracle Solaris 11.3\*](#).

## File Integrity Verification

BART is a rule-based file integrity scanning and reporting tool that uses cryptographic-strength hashes and file system metadata to report changes. BART enables you to comprehensively validate systems by performing file-level checks of a system over time. After you verify that files are installed correctly, as described in [“Package Integrity Verification” on page 28](#), you can use BART to easily and reliably track file changes.

BART is a useful tool for integrity management on one system or on a network of systems. A system's files can be compared to the system's original files, and to other system's files. The reports might indicate that a system has not been patched, an intruder has installed unapproved files, or an intruder has changed the permissions or contents of system files, such as the root-owned files.

For more information, see the following:

- For an overview and examples, see [Chapter 2, “Verifying File Integrity by Using BART” in \*Securing Files and Verifying File Integrity in Oracle Solaris 11.3\*](#).
- Selected man pages include `bart(1M)`, `bart_rules(4)`, and `bart_manifest(4)`.

## Compliance to Security Standards

The `compliance assess` command provides a snapshot of your system's security posture. The reports from the assessments suggest specific changes to your system to satisfy industry security benchmarks. Additionally, you can create tailorings from these benchmarks. Tailorings are customized assessments based on security benchmarks and profiles. For more information, see [Oracle Solaris 11.3 Security Compliance Guide](#) and the `compliance(1M)` man page.

## Log Files

The Service Management Facility (SMF) feature of the Oracle Solaris logs the status of its services per service. Many services, such as auditing and Secure Shell, write their own

logs. The `syslog` or `rsyslog` daemon writes a centralized log that can inform and warn administrators of critical conditions in many services. For example, auditing can be configured to write summarized auditing records to `syslog`. See the [syslogd\(1M\)](#) and [syslog.conf\(4\)](#) man pages.

## Labeled Security

Labeled security in Oracle Solaris is provided by the Trusted Extensions feature.

### Trusted Extensions Feature in Oracle Solaris

The Trusted Extensions feature of Oracle Solaris is an optionally enabled layer of secure labeling technology that enables data security policies to be separated from data ownership. Trusted Extensions supports both traditional discretionary access control (DAC) policies based on ownership, as well as label-based mandatory access control (MAC) policies. Unless the Trusted Extensions layer is enabled, all labels are equal so the kernel is not configured to enforce the MAC policies. When the label-based MAC policies are enabled, all data flows are restricted based on a comparison of the labels associated with the processes (subjects) requesting access and the objects containing the data.

The Trusted Extensions implementation is unique in its ability to provide high assurance, while maximizing compatibility and minimizing overhead. Trusted Extensions is part of the [“Oracle Solaris 11 Common Criteria EAL4+ Certification”](#) on page 32.

Trusted Extensions meets the requirements of the Common Criteria Labeled Security Package (LSP). See [“Oracle Solaris 11 Common Criteria EAL4+ Certification”](#) on page 32.

For more information, see the following:

- For information about configuring and maintaining Trusted Extensions, see [Trusted Extensions Configuration and Administration](#).
- Selected man pages include [trusted\\_extensions\(5\)](#), [labeladm\(1M\)](#), and [labeld\(1M\)](#).

## Labeled Filesystem

By default, filesystems are assigned a single label in a zone at that same label. You can create a multilevel ZFS dataset, mount it on a Trusted Extensions system, and with appropriate permissions, upgrade and downgrade the files in that dataset. For more information, see [“Multilevel Datasets for Relabeling Files”](#) in [Trusted Extensions Configuration and Administration](#).

## Labeled Network Communications

Trusted Extensions labels network communications. Data flows are restricted based on a comparison of the labels associated with the originating network endpoint and the receiving network endpoint. Gateways and in-between hops must also be labeled to allow the passage of information at the label of the communication. NFS and multilevel ZFS datasets provide additional features on a network.

For more information, see the following:

- “Configuring the Network Interfaces in Trusted Extensions” in *Trusted Extensions Configuration and Administration*
- Chapter 15, “Trusted Networking” in *Trusted Extensions Configuration and Administration*
- Chapter 16, “Managing Networks in Trusted Extensions” in *Trusted Extensions Configuration and Administration*

## Trusted Extensions Multilevel Desktop

Unlike most other multilevel operating systems, Trusted Extensions includes a multilevel desktop. Users can be configured to see only their allowed labels. Each label can be configured to require a separate password.

For more information, see *Trusted Extensions User’s Guide*. To configure users, see Chapter 11, “Managing Users, Rights, and Roles in Trusted Extensions” in *Trusted Extensions Configuration and Administration*.

## Writing Applications That Run Securely

Developers should write and compile applications to run securely on Oracle Solaris. For general information, see the following:

- *Developer’s Guide to Oracle Solaris 11 Security*
- *Oracle Solaris 11.3 Linkers and Libraries Guide*
- `aslr`, `nxheap`, and `nxstack` runtime flags in the `ld(1)` man page

For specific suggestions, see the following:

- Appendix A, “Secure Coding Guidelines for Developers,” in *Developer’s Guide to Oracle Solaris 11 Security*
- Appendix G, “Security Considerations When Using C Functions,” in *Developer’s Guide to Oracle Solaris 11 Security*

- “Runtime Security” in *Oracle Solaris 11.3 Linkers and Libraries Guide*

## Security Standards and Evaluations

The Oracle Solaris OS is certified to comply with two security standards, Common Criteria and FIPS 140-2.

### FIPS 140-2-2 Level 1 Cryptography Validation

The Cryptographic Framework feature of Oracle Solaris is validated at FIPS 140-2-2, Level 1 for userland and kernel functions in the Oracle Solaris 11.3 SRU 5.6 release. The OpenSSL module that runs on Oracle Solaris 11.3 is also validated for FIPS 140-2-2. Any application that uses OpenSSL for its cryptography can use this validated module. For more information, see *Using a FIPS 140 Enabled System in Oracle Solaris 11.3*.

### Oracle Solaris 11 Common Criteria EAL4+ Certification

Oracle Solaris 11 is certified under the Canadian Common Criteria Scheme at Evaluation Assurance Level 4 (EAL4) and augmented by flaw remediation (EAL4+). EAL4 is the highest level of evaluation mutually recognized by 26 countries under the Common Criteria Recognition Arrangement (CCRA).

The certification is for the Operating System Protection Profile (OSPP) and includes the following extended packages:

- Advanced Management
- Extended Identification and Authentication
- Labeled Security
- Virtualization

For information about the certification, see:

- [Oracle Security Evaluations Matrix \(http://www.oracle.com/technetwork/topics/security/security-evaluations-099357.html\)](http://www.oracle.com/technetwork/topics/security/security-evaluations-099357.html)
- [The Common Criteria Recognition Arrangement \(http://www.commoncriteriaportal.org/ccra/\)](http://www.commoncriteriaportal.org/ccra/)



- Operating System Protection Profile ([http://www.commoncriteriaportal.org/files/ppfiles/pp0067b\\_pdf.pdf](http://www.commoncriteriaportal.org/files/ppfiles/pp0067b_pdf.pdf))

## Site Security Policy and Practice

For a secure system or network of systems, your site must have a security policy in place with security practices that support the policy. If you are developing programs or installing third-party programs, you must develop and install those programs securely.

For more information, review the following:

- Importance of Software Security (<https://www.oracle.com/support/assurance/index.html>)
- Appendix A, “Secure Coding Guidelines for Developers,” in *Developer’s Guide to Oracle Solaris 11 Security*
- Appendix A, “Site Security Policy,” in *Trusted Extensions Configuration and Administration*
- “Security Requirements Enforcement” in *Trusted Extensions Configuration and Administration*
- Keeping Your Code Secure ([http://blogs.oracle.com/maryanndavidson/entry/those\\_who\\_can\\_t\\_do](http://blogs.oracle.com/maryanndavidson/entry/those_who_can_t_do))



## Configuring Oracle Solaris Security

---

This chapter describes the actions to take to configure security on your system. The chapter covers installing packages, configuring the system itself, then configuring various subsystems and additional applications that you might need, such as IPsec.

- [“Installing the Oracle Solaris OS” on page 35](#)
- [“Initially Securing the System” on page 36](#)
- [“Securing Users” on page 41](#)
- [“Protecting the Network” on page 48](#)
- [“Protecting File Systems” on page 50](#)
- [“Protecting and Modifying Files” on page 53](#)
- [“Securing System Access and Use” on page 53](#)
- [“Adding Labeled Multilevel Security” on page 55](#)

## Installing the Oracle Solaris OS

The Oracle Solaris OS is installed by selecting a set of packages called a *group* from a package repository. Different groups supply packages for different uses, such as multipurpose servers, minimally installed systems, and desktop systems. Packages are signed and their secure transfer can be verified.

When you install the Oracle Solaris OS, choose the media that installs the appropriate *group* package, as follows:

- **Oracle Solaris Large Server** – Both the default manifest in an Automated Installer (AI) installation and the text installer install the `group/system/solaris-large-server` group, which provides an Oracle Solaris large server environment.
- **Oracle Solaris Small Server** – The Automated Installer (AI) installation and the text installer optionally install the `group/system/solaris-small-server` group, which provides a useful command-line environment to which you can add packages.
- **Oracle Solaris Minimal Server** – The Automated Installer (AI) installation and the text installer optionally install the `group/system/solaris-minimal-server` group, which

provides a minimal command-line environment to which you can add just the packages that you want.

- **Oracle Solaris Desktop** – The Live Media installs the group/system/solaris-desktop group, which provides an Oracle Solaris 11 desktop environment.

To create a desktop system for centralized use, add the group/feature/multi-user-desktop group to the desktop server. For more information, see the article: [Optimizing the Oracle Solaris Desktop for a Multi-User Environment](#).

For an automated installation using the Automated Installer (AI), see [Part III, “Installing Using an Install Server,” in \*Installing Oracle Solaris 11.3 Systems\*](#). You can secure Automatic Installation (AI) installations with certificates and keys for the install server, for specified client systems, for all clients of a specified install service, and for any other AI clients. See [“Increasing Security for Automated Installations” in \*Installing Oracle Solaris 11.3 Systems\*](#).

To guide your media choice, see the following installation and package content guides:

- [Installing Oracle Solaris 11.3 Systems](#)
- [Creating a Custom Oracle Solaris 11.3 Installation Image](#)
- [Adding and Updating Software in Oracle Solaris 11.3](#)
- [Oracle Solaris 11.3 Package Group Lists](#)

## Initially Securing the System

The following tasks are best performed in order. At this point, the Oracle Solaris operating system is installed and only the initial user who can assume the root role has access to the system.

**TABLE 1**      Securing the System Task Map

Task	Description	For Instructions
1. Verify the packages on the system.	Checks that the packages are valid. Also checks the signatures on signed packages.	<a href="#">“How to Verify Your Packages” on page 37</a>
2. Ensure that executables are protected.	Verifies that security extensions that protect the stack and heap from compromise are enabled.	<a href="#">“Protecting the Process Heap and Executable Stacks From Compromise” in <i>Securing Systems and Attached Devices in Oracle Solaris 11.3</i></a>
3. Safeguard the hardware settings on the system.	Protects hardware by requiring a password to change hardware settings. On an x86 system, access to the GRUB menu is controlled. On a SPARC system, the eeprom command protects the hardware.	<a href="#">“Controlling Access to System Hardware” in <i>Securing Systems and Attached Devices in Oracle Solaris 11.3</i></a>
4. Disable unneeded services.	Prevents processes that are not part of the system's required functions from running.	<a href="#">“How to Disable Unneeded Services” on page 38</a>
5. Prevent the workstation owner from powering down the system.	Prevents the Console User from shutting down or suspending the system.	<a href="#">“How to Remove Power Management Capability From Users” on page 39</a>

Task	Description	For Instructions
6. Create a login warning message that reflects your site's security policy.	Notifies users before and after authentication that the system is monitored.	<a href="#">“How to Place a Security Message in Banner Files” on page 40</a>

## ▼ How to Verify Your Packages

Verifying package integrity includes verifying package signatures. This procedure assumes that you maintain a valid and secure package repository. For a summary, see [“Ensuring Secure Package Installation From Your Local IPS Repository” on page 58](#). For instructions, see [Copying and Creating Package Repositories in Oracle Solaris 11.3](#).

**Before You Begin** You must become an administrator with the rights to manage IPS repositories and packages. For the rights that you require, see [“Repository Management Privileges” in Copying and Creating Package Repositories in Oracle Solaris 11.3](#).

### 1. Ensure that you are checking package signatures.

#### a. Display the signature policy for the image and for the publisher.

In this example, an administrator has explicitly changed the default signature policy to ignore, which has the effect of ignoring signatures for all manifests.

```
$ pkg property signature-policy
PROPERTY          VALUE
signature-policy  ignore
$ pkg publisher
...
Properties:
signature-policy = ignore
```

#### b. Change the signature policy if it is set to a weaker value than you want to implement.

The available policies are:

- **verify** – Verifies that all manifests with signatures are validly signed but does not require all installed packages to be signed.
- **require-signatures** – Requires that all newly installed packages have at least one valid signature.
- **require-names** – Follows the same requirements as **require-signatures** but also requires that the strings listed in the **signature-required-names** property are used to verify the chains of trust of the signatures.

The following command changes the signature policy for the image from ignore to the default, **verify**.

```
$ pkg set-property signature-policy verify
```

- c. **(Optional) Establish a stronger signature policy for the solaris publisher and display the new policy.**

Publishers inherit the signature policy from the image unless the publisher value is explicitly changed. For example, you might want to have a stronger policy than verify for publishers whose packages are always signed.

```
$ pkg set-publisher --set-property signature-policy=require-signatures solaris
$ pkg -publisher solaris
    Publisher: solaris
...
    Catalog Updated: Feb 8, 2015 02:01:01 AM
    Enabled: Yes
    Properties:
        signature-policy = require-signatures
```

2. **After package installation, take appropriate action on any error messages in the installation window.**
3. **Run the `pkg verify` command and send its results to a log file.**

```
# pkg verify > /var/log/filename
```

For more information, see the [pkg\(1\)](#) and [pkg\(5\)](#) man pages.

4. **Review the log for any errors.**
5. **If you find errors, reinstall or fix the errors.**

For more information, see “[Verifying Packages and Fixing Verification Errors](#)” in *Adding and Updating Software in Oracle Solaris 11.3*.

## ▼ How to Disable Unneeded Services

Use this procedure to disable services that are not required on this system.

**Before You Begin** You must assume the root role. For more information, see “[Using Your Assigned Administrative Rights](#)” in *Securing Users and Processes in Oracle Solaris 11.3*.

1. **List the online network services.**

```
# 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. Disable the services that are not required by this system.

For example, if the system is not an NFS server or a web server and their services are online, disable them.

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

**See Also** For more information, see [Chapter 1, “Introduction to the Service Management Facility”](#) in *Managing System Services in Oracle Solaris 11.3* and the `svcs(1)` man page.

# ▼ How to Remove Power Management Capability From Users

Use this procedure to prevent users on the console of a system from suspending the system or powering it down. This software solution is not effective if the system hardware can be unplugged by the console user.

**Before You Begin** You must assume the root role. For more information, see [“Using Your Assigned Administrative Rights”](#) in *Securing Users and Processes in Oracle Solaris 11.3*.

## 1. Review the contents of the Console User rights profile.

```
% 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. Create a rights profile that includes any rights in the Console User profile that you want users to retain.

For instructions, see [“How to Create a Rights Profile”](#) in *Securing Users and Processes in Oracle Solaris 11.3*.

## 3. Comment out the Console User rights profile in the `/etc/security/policy.conf` file.

```
#CONSOLE_USER=Console User
```

4. **Assign the rights profile that you created in [Step 2](#).**

- If you have many users that share a rights profile, setting this value in a rights profile can be a scalable solution.

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

- You can also assign the profile per system in the `policy.conf` file.

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

**See Also** For more information, see “[policy.conf File](#)” in *Securing Users and Processes in Oracle Solaris 11.3* and the [policy.conf\(4\)](#) and [usermod\(1M\)](#) man pages.

## ▼ How to Place a Security Message in Banner Files

Use this procedure to create security messages in two banner files that reflect your site's security policy. The `/etc/issue` file displays before authentication, for example, on your desktop and when logging in remotely with the `ssh` command. The `/etc/motd` file displays after authentication.

---

**Note** - The sample messages in this procedure do not satisfy U.S. government requirements and likely do not satisfy your security policy. Consult with your company's legal counsel about the content of the security message.

---

**Before You Begin** You must become an administrator who is assigned the Administrator Message Edit rights profile. For more information, see “[Using Your Assigned Administrative Rights](#)” in *Securing Users and Processes in Oracle Solaris 11.3*.

1. **Create the `/etc/issue` file and add a security message.**

```
# pfedit /etc/issue
ALERT  ALERT  ALERT  ALERT  ALERT
```

This system is available to authorized users only.

If you are an authorized user, continue.

Your actions are monitored, and can be recorded.

The login command displays the contents of `/etc/issue` before authentication, as do the `ssh`, `graphical-login/gdm`, `telnet`, and `FTP` services.

For more information, see the [issue\(4\)](#) and [pfedit\(1M\)](#) man pages.



## 2. Add a security message to the `/etc/motd` file.

```
# pfedit /etc/motd
```

This system serves authorized users only. Activity is monitored and reported.

In Oracle Solaris, the user's initial shell displays the contents of the `/etc/motd` file.

# Securing Users

At this point, only the initial user who can assume the root role has access to the system. The following tasks are best performed in order before regular users can log in.

**TABLE 2** Securing Users Task Map

Task	Description	For Instructions
Require strong passwords and regular password changes.	Strengthens the default password constraints on each system.	<a href="#">“How to Set Stronger Password Constraints” on page 41</a>
Configure restrictive file permissions for regular users.	Sets a more restrictive value than 022 for file permissions for regular users.	<a href="#">“How to Set a More Restrictive umask Value for Regular Users” on page 45.</a>
Set account locking for regular users.	On systems that are not used for administration, sets account locking system-wide and reduces the number of logins that activate the lock.	<a href="#">“How to Set Account Locking for Regular Users” on page 43</a>
Preselect the cusa audit class for all users.	Provides better monitoring and recording of potential threats to the system.	<a href="#">“How to Audit Significant Events in Addition to Login/Logout” on page 46</a>
Create roles.	Distributes discrete administrative tasks to several trusted users so that no one user can damage the system.  You can use predefined ARMOR roles, create your own roles, or extend ARMOR with your own roles.	<a href="#">“Managing User Accounts by Using the CLI” in <i>Managing User Accounts and User Environments in Oracle Solaris 11.3</i></a>  <a href="#">“Assigning Rights to Users” in <i>Securing Users and Processes in Oracle Solaris 11.3</i></a>
Reduce the number of visible GNOME desktop applications.	Prevents users from using desktop applications that can affect security.	See <a href="#">Chapter 11, “Disabling Features in the Oracle Solaris Desktop System” in <i>Oracle Solaris 11.3 Desktop Administrator’s Guide</i>.</a>
Limit a user’s privileges.	Removes basic privileges that users do not need.	<a href="#">“How to Remove Unneeded Basic Privileges From Users” on page 47</a>

## ▼ How to Set Stronger Password Constraints

Use this procedure if the defaults do not satisfy your site security requirements and current industry standards. The steps are in the order of the variable entries in the `/etc/default/passwd` file.

**Before You Begin** You must become an administrator who is assigned the `solaris.admin.edit/etc/default/passwd` authorization. For more information, see [“Using Your Assigned Administrative Rights” in \*Securing Users and Processes in Oracle Solaris 11.3\*](#).

**1. Review the latest password security recommendations from government and standards bodies.**

For example, go to the [National Cyber Security Centre](#) and the U.S. [Federal Trade Commission](#) web sites and search for the latest articles on passwords.

**2. Use the `pfedit` command to make the following changes in the `/etc/default/passwd` file:**

**a. Require users to change their passwords every four months, but not more frequently than every three weeks.**

```
## /etc/default/passwd
##
#MAXWEEKS=
#MINWEEKS=
MAXWEEKS=13
MINWEEKS=3
```

**b. Require a password of at least eight characters.**

```
#PASLENGTH=6
PASLENGTH=8
```

**c. Keep a password history.**

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

**d. Require a minimum difference from the last password.**

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

**e. Require at least one uppercase letter.**

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

**f. Require at least one digit.**

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

**See Also** ■ For the list of variables that constrain password creation, see the [`passwd\(1\)`](#) man page.

- For the password constraints in effect after installation, see [“System Access Is Limited and Monitored” on page 16](#).
- Review <https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes>.

## ▼ How to Set Account Locking for Regular Users

Use this procedure to lock regular user accounts after a certain number of failed login attempts.

---

**Note** - Roles are shared accounts. Do not set account locking for users who can assume roles or roles because one locked user can lock out the role.

---

**Before You Begin** Do not set this protection system-wide on a system that you use for administrative activities. Rather, monitor the administrative system for unusual use and keep it available for administrators.

You must assume the root role. For more information, see [“Using Your Assigned Administrative Rights” in \*Securing Users and Processes in Oracle Solaris 11.3\*](#).

### 1. Set the LOCK\_AFTER\_RETRIES security attribute to YES.

Choose the scope of the attribute value.

#### ■ Set system-wide.

This protection applies to any user who attempts to use the system.

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

#### ■ Set per user.

This protection applies only to the user for whom you run this command. If you have many users, this is not a scalable solution.

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

#### ■ Create and assign a rights profile.

This protection applies to any user or system where you assign this rights profile.

##### a. Create the rights profile.

```
# profiles -p shared-profile -S ldap
```

```
shared-profile: set lock_after_retries=yes
...
```

For more information on creating rights profiles, see [“Creating Rights Profiles and Authorizations” in \*Securing Users and Processes in Oracle Solaris 11.3\*](#).

**b. Assign the rights profile to users or system-wide.**

If you have many users that share a rights profile, setting this value in a rights profile can be a scalable solution.

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

You can also assign the profile per system in the `policy.conf` file.

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

**2. Set the RETRIES security attribute to 3.**

Choose the scope of the attribute value.

■ **Set system-wide.**

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

■ **Set per user.**

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

■ **Create and assign a rights profile.**

Follow the "Create and assign a rights profile" option in [Step 1](#) to create a rights profile that includes `lock_after_retries=3`.

**3. To unlock a locked user, use the `passwd` command.**

```
# passwd -u username
```

A user who is locked out cannot log in without administrative intervention. You can unlock user accounts in both the files and ldap naming services.

**See Also** ■ For a discussion of user and role security attributes, see [Chapter 8, “Reference for Oracle Solaris Rights” in \*Securing Users and Processes in Oracle Solaris 11.3\*](#).

- Selected man pages include [passwd\(1\)](#), [policy.conf\(4\)](#), [profiles\(1\)](#), [user\\_attr\(4\)](#), and [usermod\(1M\)](#).

## ▼ How to Set a More Restrictive umask Value for Regular Users

The umask utility sets the file permission bits of user-created files. If the default umask value, 022, is not restrictive enough, set a more restrictive mask by using this procedure.

**Before You Begin** You must become an administrator who is authorized to edit the skeleton files. The root role is assigned these authorizations. For more information, see [“Using Your Assigned Administrative Rights” in \*Securing Users and Processes in Oracle Solaris 11.3\*](#).

### 1. View the sample files that Oracle Solaris provides for user shell defaults.

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

### 2. Set the umask value in the /etc/skel files that you are going to assign to users.

Choose one of the following values:

- umask 026 – Provides moderate file protection  
(751) – r for group, x for others
- umask 027 – Provides strict file protection  
(750) – r for group, no access for others
- umask 077 – Provides complete file protection  
(700) – No access for group or others

**See Also** For more information, see the following:

- [“Managing User Accounts by Using the CLI” in \*Managing User Accounts and User Environments in Oracle Solaris 11.3\*](#)
- [“Default umask Value” in \*Securing Files and Verifying File Integrity in Oracle Solaris 11.3\*](#)
- Selected man pages include [useradd\(1M\)](#) and [umask\(1\)](#).

## ▼ How to Audit Significant Events in Addition to Login/Logout

Use this procedure to audit administrative commands, system access, and other significant events as specified by your site security policy.

---

**Note** - The examples in this procedure might not be sufficient to satisfy your security policy.

---

**Before You Begin** You must assume the root role. For more information, see [“Using Your Assigned Administrative Rights” in \*Securing Users and Processes in Oracle Solaris 11.3\*](#).

1. **Audit all uses of privileged commands by users who are assigned administrative rights profiles and roles.**

Add the cusa audit class to their preselection mask.

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

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

The audit classes that the cusa meta-class includes are listed in the `/etc/security/audit_class` file.

2. **Record the arguments to audited commands.**

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

3. **(Optional) Record the environment in which audited commands are executed.**

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

---

**Note** - This policy option can be useful when troubleshooting.

---

- See Also**
- For information about audit policy, see [“Audit Policy” in \*Managing Auditing in Oracle Solaris 11.3\*](#).
  - For examples of setting audit flags, see [“Configuring the Audit Service” in \*Managing Auditing in Oracle Solaris 11.3\*](#) and [“Troubleshooting the Audit Service” in \*Managing Auditing in Oracle Solaris 11.3\*](#).
  - [auditconfig\(1M\)](#) man page

## ▼ How to Remove Unneeded Basic Privileges From Users

Under particular circumstances, some basic privileges can be removed from a regular or guest user's basic set. For example, Sun Ray users might be prevented from examining the status of processes that they do not own.

**Before You Begin** You must assume the root role. For more information, see [“Using Your Assigned Administrative Rights” in \*Securing Users and Processes in Oracle Solaris 11.3\*](#).

### 1. List a full definition of the basic privilege set.

The following three basic privileges are likely candidates for removal.

```
% 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. Choose the scope of the privilege removal.

#### ■ Set system-wide.

Any user who attempts to use the system is denied these privileges. This method of privilege removal might be appropriate for a publicly available computer.

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

#### ■ Remove privileges from individual users.

##### ■ Prevent a user from linking to a file that the user does not own.

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

##### ■ Prevent a user from examining processes that the user does not own.

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

- **Prevent a user from starting a second session, such as starting an ssh session from the user's current session.**

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

- **Remove all three privileges from a user's basic set.**

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

- **Create and assign a rights profile.**

This protection applies to any user or system where you assign this rights profile.

- a. **Create the rights profile.**

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

For more information on creating rights profiles, see [“Creating Rights Profiles and Authorizations” in \*Securing Users and Processes in Oracle Solaris 11.3\*](#).

- b. **Assign the rights profile to users or system-wide.**

If you have many users that share a rights profile, such as Sun Ray or remote users, setting this value in a rights profile can be a scalable solution.

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

You can also assign the profile per system in the `policy.conf` file.

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

**See Also** For more information, see [Chapter 1, “About Using Rights to Control Users and Processes” in \*Securing Users and Processes in Oracle Solaris 11.3\*](#) and the `privileges(5)` man page.

## Protecting the Network

At this point, you might have created users who can assume roles, and have created the roles.

From the following network tasks, perform the tasks that provide additional security according to your site requirements. These network tasks strengthen the IP, ARP, and TCP protocols.



**TABLE 3** Configuring the Network Task Map

Task	Description	For Instructions
Disable the network routing daemon.	Limits access to systems by would-be network sniffers.	<a href="#">“How to Disable the Network Routing Daemon” in <i>Securing the Network in Oracle Solaris 11.3</i></a>
Prevent the dissemination of information about the network topology.	Prevents the broadcast of packets.	<a href="#">“How to Disable Broadcast Packet Forwarding” in <i>Securing the Network in Oracle Solaris 11.3</i></a>
	Prevents responses to broadcast echo requests and multicast echo requests.	<a href="#">“How to Disable Responses to Echo Requests” in <i>Securing the Network in Oracle Solaris 11.3</i></a>
For systems that are gateways to other domains, such as a firewall or a VPN node, turn on strict source and destination multihoming.	Prevents packets that do not have the address of the gateway in their header from moving beyond the gateway.	<a href="#">“How to Set Strict Multihoming” in <i>Securing the Network in Oracle Solaris 11.3</i></a>
Prevent Denial of Service (DoS) attacks by controlling the number of incomplete system connections.	Limits the allowable number of incomplete TCP connections for a TCP listener.	<a href="#">“How to Set Maximum Number of Incomplete TCP Connections” in <i>Securing the Network in Oracle Solaris 11.3</i></a>
Prevent DoS attacks by controlling the number of permitted incoming connections.	Specifies the default maximum number of pending TCP connections for a TCP listener.	<a href="#">“How to Set Maximum Number of Pending TCP Connections” in <i>Securing the Network in Oracle Solaris 11.3</i></a>
Return network parameters to their secure default values.	Increases security that was reduced by administrative actions.	<a href="#">“How to Reset Network Parameters to Secure Values” in <i>Securing the Network in Oracle Solaris 11.3</i></a>
Add TCP wrappers to network services to limit applications to legitimate users.	Specifies systems that are allowed access to network services, such as FTP.	<a href="#">“How to Use TCP Wrappers” on page 49</a>
Configure a firewall.	Uses the Packet Filter or IP Filter feature to provide a firewall.	Chapter 5, “Configuring the Packet Filter Firewall” in <i>Securing the Network in Oracle Solaris 11.3</i>  Chapter 7, “Configuring IP Filter Firewall” in <i>Securing the Network in Oracle Solaris 11.3</i>
Configure encrypted and authenticated network connections.	Uses IPsec and IKE to protect network transmissions between nodes and networks that are jointly configured with IPsec and IKE.	Chapter 9, “Configuring IPsec” in <i>Securing the Network in Oracle Solaris 11.3</i>  Chapter 11, “Configuring IKEv2” in <i>Securing the Network in Oracle Solaris 11.3</i>

## ▼ How to Use TCP Wrappers

The following steps show three ways that TCP wrappers are used or can be used in Oracle Solaris.

**Before You Begin** You must assume the root role to modify a program to use TCP wrappers.

- 1. You do not need to protect the `sendmail` application with TCP wrappers. It is protected by default.**

2. To enable TCP wrappers for all `inetd` services, see [“How to Use TCP Wrappers to Control Access to TCP Services” in \*Administering TCP/IP Networks, IPMP, and IP Tunnels in Oracle Solaris 11.3\*](#).

3. Protect the FTP network service with TCP wrappers.

- a. Follow the instructions in the `/usr/share/doc/proftpd/modules/mod_wrap.html` module.

Because this module is dynamic, you must load it to use TCP wrappers with FTP.

- b. Load the module by adding the following instructions to the `proftpd.conf` file:

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

- c. Restart the FTP service.

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

## Protecting File Systems

ZFS file systems are lightweight and can be encrypted, compressed, and configured with reserved space and disk space quotas.

The `tmpfs` file system can grow without bound. To prevent a denial of service (DoS) attack, complete [“How to Limit the Size of the `tmpfs` File System” on page 51](#).

The following tasks configure a size limit for `tmpfs` and provide a glimpse of the protections that are available in ZFS, the default file system in Oracle Solaris. For additional information, see [“Setting ZFS Quotas and Reservations” in \*Managing ZFS File Systems in Oracle Solaris 11.3\*](#) and the `zfs(1M)` man page.

**TABLE 4** Protecting File Systems Task Map

Task	Description	For Instructions
Prevent DoS attacks by managing and reserving disk space.	Specifies the use of disk space by file system, by user or group, or by project.	<a href="#">“Setting ZFS Quotas and Reservations” in <i>Managing ZFS File Systems in Oracle Solaris 11.3</i></a>
Guarantee a minimum amount of disk space to a dataset and its descendants.	Guarantees disk space by file system, by user or group, or by project.	<a href="#">“Setting Reservations on ZFS File Systems” in <i>Managing ZFS File Systems in Oracle Solaris 11.3</i></a>
Encrypt data on a file system.	Protects a dataset with encryption and a passphrase to access the dataset at dataset creation.	<a href="#">“Encrypting ZFS File Systems” in <i>Managing ZFS File Systems in Oracle Solaris 11.3</i></a>

Task	Description	For Instructions
		<a href="#">“Examples of Encrypting ZFS File Systems” in Managing ZFS File Systems in Oracle Solaris 11.3</a>
Limit the size of the tmpfs file system.	Prevents a malicious user from creating large files in /tmp to slow down the system.	<a href="#">“How to Limit the Size of the tmpfs File System” on page 51</a>

## ▼ How to Limit the Size of the tmpfs File System

The size of the tmpfs file system is not limited by default. Therefore, tmpfs can grow to fill the available system memory and swap. Because the /tmp directory is used by all applications and users, an application can fill all available system memory. Similarly, an unprivileged user with malicious intent could cause a system slowdown by creating large files in the /tmp directory. To avoid a performance impact, you can limit the size of each tmpfs mount.

You might try several values to achieve best system performance.

**Before You Begin** To edit the vfstab file, you must become an administrator who is assigned the `solaris.admin.edit/etc/vfstab` authorization. To reboot the system, you must be assigned the Maintenance and Repair rights profile. The root role has all of these rights. For more information, see [“Using Your Assigned Administrative Rights” in Securing Users and Processes in Oracle Solaris 11.3](#).

### 1. Determine the amount of memory on your system.

**Note** - The SPARC T3 series system that is used for the following example has a solid state disk (ssd) for faster I/O and has eight 279.40 MB disks. The system has around 500 GB of memory.

```
% 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. Compute a memory limit for tmpfs.

Depending on the size of the system memory, you might want to compute a memory limit of around 20 percent for large systems and around 30 percent for smaller systems.

So, for a smaller system, use `.30` as the multiplier.

**10240M x .30 ≈ 3072M**

For a larger system, use .20 as the multiplier.

**523776M x .20 ≈ 104755M**

**3. Modify the swap entry in the /etc/vfstab file with the size limit.**

```
# 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=104700m
/dev/zvol/dsk/rpool/swap -      - swap     -         no        -
```

**4. Reboot the system.**

```
# reboot
```

**5. Verify that the size limit is in effect.**

```
% 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=104700m/dev=89c0006 on Tues ...
```

**6. Monitor the memory usage and adjust it to the requirements of your site.**

The df command is somewhat useful. The swap command provides the most useful statistics.

```
% 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
```

For more information, see the [tmpfs\(7FS\)](#), [mount\\_tmpfs\(1M\)](#), [df\(1M\)](#), and [swap\(1M\)](#) man pages.

## Protecting and Modifying Files

By default, only the root role can modify system file permissions. Roles and users who are assigned the `solaris.admin.edit/path-to-system-file` authorization can modify that *system-file*. Only the root role can search for all files.

**TABLE 5** Protecting and Modifying Files Task Map

Task	Description	For Instructions
Configure restrictive file permissions for regular users.	Sets a more restrictive value than 022 for file permissions for regular users.	<a href="#">“How to Set a More Restrictive umask Value for Regular Users” on page 45</a>
Specify ACLs to protect files at a finer granularity than regular UNIX file permissions.	Extended security attributes can be useful in protecting files.	<a href="#">“Using File Attributes to Add Security to ZFS Files” in <i>Securing Files and Verifying File Integrity in Oracle Solaris 11.3</i></a>
Specify an ACL to prevent the deletion of critical files, such as Oracle database logs.	Sets the nounlink property on a file or directory so that the <code>rm</code> command fails even when run by the root role.	<a href="#">“Preventing Accidental Deletions With the nounlink Attribute” in <i>Managing ZFS File Systems in Oracle Solaris 11.3</i></a>
Maintain system file integrity.	Finds suspicious files through a script or by using BART.	<a href="#">“How to Find Files With Special File Permissions” in <i>Securing Files and Verifying File Integrity in Oracle Solaris 11.3</i></a>

## Securing System Access and Use

You can configure Oracle Solaris security features to protect your system use, including applications and services on the system and on the network.

**TABLE 6** Securing System Access and Use Task Map

Task	Description	For Instructions
Prevent programs from heap or executable stack corruption.	Verifies that security extensions that protect the stack and heap from compromise are enabled.	<a href="#">“Protecting the Process Heap and Executable Stacks From Compromise” in <i>Securing Systems and Attached Devices in Oracle Solaris 11.3</i></a>
Configure auditing.	Customizes audit configuration for coverage and file integrity.	<a href="#">“Using the Audit Service” on page 58</a>
Protect core files that might contain sensitive information.	Creates a directory with limited access that is dedicated to core files.	<a href="#">“Enabling File Paths” in <i>Troubleshooting System Administration Issues in Oracle Solaris 11.3</i></a> <a href="#">“Administering Your Core File Specifications” in <i>Troubleshooting System Administration Issues in Oracle Solaris 11.3</i></a>
Protect a web server with SSL Kernel Proxy.	The Secure Sockets Layer (SSL) protocol can be used to encrypt and accelerate web server communications.	<a href="#">Chapter 3, “Web Servers and the Secure Sockets Layer Protocol” in <i>Securing the Network in Oracle Solaris 11.3</i></a>
Protect legacy services with privileges and authorizations.	Runs applications with least privilege by assigning limited rights to the application.	<a href="#">“Protecting a Legacy Service With SMF” on page 54</a>

Task	Description	For Instructions
Create zones to contain applications.	Zones are containers that isolate processes. They can isolate applications and parts of applications. For example, zones can be used to separate a web site's database from the site's web server.	<a href="#">Introduction to Oracle Solaris Zones</a>
Manage resources in zones.	Zones provide a number of tools to manage zone resources.	<a href="#">Administering Resource Management in Oracle Solaris 11.3</a>

## Protecting a Legacy Service With SMF

You can limit application configuration to trusted users or roles by adding the application to the Service Management Facility (SMF) feature of Oracle Solaris, then requiring rights to start, refresh, and stop the service.

For services that are run by `inetd`, you should control the number of concurrent processes to prevent a security breach. For more information, see [“Recommendations for Configuring Systems That Run `inetd` Based Services” in \*Administering TCP/IP Networks, IPMP, and IP Tunnels in Oracle Solaris 11.3\*](#).

For information and procedures see the following:

- [“Locking Down Resources by Using Extended Privileges” in \*Securing Users and Processes in Oracle Solaris 11.3\*](#)
- Selected man pages include `smf(5)`, `smf_security(5)`, `svcadm(1M)`, `svcbundle(1M)`, and `svccfg(1M)`.

## Configuring a Kerberos Network

You can protect your network with the Kerberos service. This client-server architecture provides secure transactions over networks. The service offers strong user authentication, as well as integrity and privacy. Using the Kerberos service, you can log in to other systems, execute commands, exchange data, and transfer files securely. Additionally, the service enables administrators to restrict access to services and systems. As a Kerberos user, you can regulate other people's access to your account.

For information and procedures see the following:

- [Chapter 3, “Planning for the Kerberos Service” in \*Managing Kerberos and Other Authentication Services in Oracle Solaris 11.3\*](#)
- [Chapter 4, “Configuring the Kerberos Service” in \*Managing Kerberos and Other Authentication Services in Oracle Solaris 11.3\*](#)
- Selected man pages include `kadmin(1M)`, `pam_krb5(5)`, and `kclient(1M)`.

## Adding Labeled Multilevel Security

Trusted Extensions extends Oracle Solaris security by enforcing a label-based mandatory access control (MAC) policy. Sensitivity labels are automatically applied to all sources of data (networks, file systems, and windows) and consumers of data (user and processes). Access to all data is restricted based on the relationship between the label of the data (object) and the consumer (subject). The layered functionality consists of a set of label-aware services.

A partial list of Trusted Extensions services includes:

- Labeled networking
- Label-aware file system mounting and sharing
- Labeled desktop
- Label configuration and translation
- Label-aware system management tools
- Label-aware device allocation

The `system/trusted` and `system/trusted/trusted-global-zone` packages are sufficient for a headless system or a server that does not require a multilevel desktop. The `system/trusted/trusted-extensions` package provides the Oracle Solaris multilevel, trusted desktop environment.

## Configuring Trusted Extensions

You must install the Trusted Extensions packages, then configure the system. When you install the `trusted-extensions` package, the system can run a desktop with a directly connected bitmapped display, such as a laptop or workstation. Network configuration is required to communicate with other systems.

For information and procedures see the following:

- [Part 1, “Initial Configuration of Trusted Extensions,” in \*Trusted Extensions Configuration and Administration\*](#)
- [Part 2, “Administration of Trusted Extensions,” in \*Trusted Extensions Configuration and Administration\*](#)

## Configuring Labeled IPsec

You can protect your labeled packets with IPsec.

For information and procedures see the following:

- [Chapter 8, “About IP Security Architecture” in \*Securing the Network in Oracle Solaris 11.3\*](#)
- [“Administration of Labeled IPsec” in \*Trusted Extensions Configuration and Administration\*](#)
- [“Configuring Labeled IPsec” in \*Trusted Extensions Configuration and Administration\*](#)



# 3

◆ ◆ ◆ CHAPTER 3

## Maintaining and Monitoring Oracle Solaris Security

After initial installation and configuration, you can maintain and monitor the security posture of your system through the following actions:

- Updating your system to the latest Critical Patch Update (CPU) and SRU (Support Repository Update)
- Running package and file integrity checks
- Running compliance checks
- Monitoring network activity
- Regularly reviewing audit records

### Maintaining and Monitoring System Security

The tasks described in the following table maintain and monitor access and use of your system and data, and adherence to your site’s security requirements.

**TABLE 7** Maintaining and Monitoring the System Task Map

Task	Description	For Instructions
Verify that you are running the latest version of the OS.	Checks that the latest updates and security fixes are installed.	<a href="#">“Administering CVE Updates in Oracle Solaris” in Oracle Solaris 11.3 Security Compliance Guide</a>
Verify that your local IPS repository is valid.	Checks that the files in the local repository pass a series of checks. Also validates the signatures on signed packages.	<a href="#">“Ensuring Secure Package Installation From Your Local IPS Repository” on page 58</a>
Verify the packages on the system.	Checks that the packages after an update are identical to the source packages and verifies the signatures on signed packages.	<a href="#">“How to Verify Your Packages” on page 37</a>
Run compliance tests.	Assesses the system’s compliance to security benchmarks.	<a href="#">Oracle Solaris 11.3 Security Compliance Guide</a> and the <a href="#">compliance(1M)</a> man page
Verify file integrity.	After configuration, compares BART manifests at regular intervals to ensure that only files that should be changed are changed.	<a href="#">“How to Compare Manifests for the Same System Over Time” in Securing Files and Verifying File Integrity in Oracle Solaris 11.3</a>

Task	Description	For Instructions
Find suspicious files.	Locates the potentially unauthorized use of the setuid and setgid permissions on programs.	<a href="#">“How to Find Files With Special File Permissions” in <i>Securing Files and Verifying File Integrity in Oracle Solaris 11.3</i></a>
Review audit logs regularly.	Locates unusual access and use of the system.	<a href="#">“Using the Audit Service” on page 58</a>
Review audit logs for login and logout events in real time.	Identifies attempted breaches near to the time that the attempts occur.	<a href="#">“Monitoring Audit Records in Real Time” on page 59</a>

## Ensuring Secure Package Installation From Your Local IPS Repository

Maintaining a valid and secured IPS repository is essential for package installation. For secure repository creation and maintenance, follow [“Best Practices for Creating and Using Local IPS Package Repositories” in \*Copying and Creating Package Repositories in Oracle Solaris 11.3\*](#). The practices include the following:

- Ensuring that you are verifying signatures on signed packages
- Verifying that the files in the repository pass a series of checks, including that packages are signed correctly
- Verifying access to the repository

For repository configuration and maintenance procedures, see [Copying and Creating Package Repositories in Oracle Solaris 11.3](#). For verifying package installation, see [“How to Verify Your Packages” on page 37](#).

## Using the Audit Service

Auditing keeps a record of how the system is being used. The audit service includes tools to assist with the analysis of the auditing data.

The audit service is described in [Managing Auditing in Oracle Solaris 11.3](#). For a list of the man pages and links to them, see [“Audit Service Man Pages” in \*Managing Auditing in Oracle Solaris 11.3\*](#).

The following audit service procedures are useful in many secure environments:

- Create separate roles to configure auditing, review auditing, and start and stop the audit service. Assign the roles to trusted users.  
Use the Audit Configuration, Audit Review, and Audit Control rights profiles as the basis for your roles.  
To create roles or use the predefined ARMOR roles, see [“Assigning Rights to Users” in \*Securing Users and Processes in Oracle Solaris 11.3\*](#).

- Audit all administrators with the `cusa` audit class.  
Events in the `cusa` audit class cover administrative actions that affect the system's security posture. For a description, see the `/etc/security/audit_class` file. For the procedure, see [“How to Audit Significant Events in Addition to Login/Logout” on page 46](#).
- Send audit records to a central server.
  - Configure auditing to work with the Audit Remote Server (ARS).  
The audit service can use the Oracle Audit Vault to store, review, and analyze audit records. See [“Using Oracle Audit Vault and Database Firewall for Storage and Analysis of Audit Records” in \*Managing Auditing in Oracle Solaris 11.3\*](#) and [“How to Send Audit Files to a Remote Repository” in \*Managing Auditing in Oracle Solaris 11.3\*](#).
  - Schedule the secure transfer of complete audit files to an audit review file system on a separate ZFS pool.
- Monitor text summaries of selected audited events in the `syslog` utility  
Activate the `audit_syslog` plugin, then monitor the reported events.  
See [“How to Configure syslog Audit Logs” in \*Managing Auditing in Oracle Solaris 11.3\*](#).
- Limit the size of audit files.  
Set the `p_fsize` attribute for the `audit_binfile` plugin to a useful size. Consider your reviewing schedule, disk space, and `cron` job frequency, among other factors.  
For examples, see [“How to Assign Audit Space for the Audit Trail” in \*Managing Auditing in Oracle Solaris 11.3\*](#).
- Schedule the secure transfer of complete audit files to an audit review file system on a separate ZFS pool.
- Review complete audit files on the audit review file system.

## Monitoring Audit Records in Real Time

The `audit_syslog` plugin enables you to record summaries of preselected audit events. To display the audit summaries in a terminal window as they are generated, run a command similar to the following:

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

To configure the audit log, see [“How to Configure syslog Audit Logs” in \*Managing Auditing in Oracle Solaris 11.3\*](#).

## Reviewing and Archiving Audit Logs

Audit records can be viewed in text format or in a browser in XML format.

For information and procedures see the following:

- [“Audit Logs” in \*Managing Auditing in Oracle Solaris 11.3\*](#)
- [“Preventing Audit Trail Overflow” in \*Managing Auditing in Oracle Solaris 11.3\*](#)
- [“Displaying Audit Trail Data” in \*Managing Auditing in Oracle Solaris 11.3\*](#)

## ◆ ◆ ◆   A P P E N D I X   A

# Bibliography for Oracle Solaris Security

---

The following references contain useful security information for Oracle Solaris systems. Security information from earlier releases of Oracle Solaris contain some useful and some outdated information.

## Security References on the Oracle Technology Network

The following books and articles on the [Oracle Technology Network](#) web site contain descriptions of security on Oracle Solaris 11 systems:

- [Securing Systems and Attached Devices in Oracle Solaris 11.3](#)
- [Securing Files and Verifying File Integrity in Oracle Solaris 11.3](#)
- [Securing the Network in Oracle Solaris 11.3](#)
- [Securing Users and Processes in Oracle Solaris 11.3](#)
- [Managing Encryption and Certificates in Oracle Solaris 11.3](#)
- [Managing Auditing in Oracle Solaris 11.3](#)
- [Managing Kerberos and Other Authentication Services in Oracle Solaris 11.3](#)
- [Managing Secure Shell Access in Oracle Solaris 11.3](#)
- [Oracle Solaris 11.3 Security Compliance Guide](#)
- [Trusted Extensions Configuration and Administration](#)
- [Using a FIPS 140 Enabled System in Oracle Solaris 11.3](#)
- [Developer's Guide to Oracle Solaris 11 Security](#)

## Oracle Solaris Security References in Third-Party Publications

The following books contain descriptions of security on Oracle Solaris 11 systems:

- [Security Configuration Benchmark For Solaris 11 11/11 Version 1.0.0 June 11th, 2012](#)

This security benchmark is published by the Center for Internet Security ([CIS](#)) for the security community. This document recommends security settings for the Oracle Solaris operating system. The targeted audience includes system and application administrators, security specialists, auditors, support engineers, and installers and developers who develop, install, assess, or provide security solutions for Oracle Solaris. To obtain a copy, click the Security Benchmarks link on the main page.

- *Oracle Solaris 11 System Administration: The Complete Reference*. Michael Jang, Harry Foxwell, Christine Tran, and Alan Formy-Duval. 2012. McGraw-Hill. ISBN 978007179042.

This trade book includes security coverage of Oracle Solaris.

- *Oracle Solaris 11: First Look*. Philip P. Brown. 2013. Packt Publishing. ISBN 9781849688307.

This trade book introduces administrators to Oracle Solaris and its security.

- *Oracle Solaris 11 System Administration*, Bill Calkins. 2013. Prentice Hall. ISBN 9780133007114.

This trade book covers the new features of Oracle Solaris, including security features.

# Index

---

## A

- access
  - default, 16
  - remote, 25
  - to system files, 16
- accounts
  - default, 16
  - locking and unlocking, 43
  - roles, 22
- address space layout randomization (ASLR), 21
- administering *See* managing
- Administrator Message Edit rights profile, 40
- algorithms
  - AES128, 16
  - Camellia, 14
  - SHA256, 16, 22
- applications
  - authorizations and, 21
  - developed securely, 31
  - isolating in zones, 19
  - JCE and, 22
  - protecting
    - JCE, 22
    - legacy, 54
    - overview, 19, 19
    - SMF and, 54
    - with authorizations, 21
    - with TCP wrappers, 23, 25, 49
    - zones, 20
  - zones and, 20
- ARMOR roles, 22
- ASLR (address space layout randomization), 19, 21
- assessments
  - scheduled, 14
- assigning
  - rights profiles, 44, 48

- audit service
  - administrative audit events, 46
  - audit\_binfile plugin, 58
  - audit\_syslog plugin, 58
  - auditing privileged users, 46
  - cusa audit class, 46
  - default configuration, 16
  - managing, 58
  - monitoring audit records, 59
  - reviewing audit logs, 59
  - rights profiles, 58
  - significant event auditing, 46
- audit\_binfile plugin, 58
- audit\_flags keyword, 46
- audit\_syslog plugin, 58
- authentication
  - IPsec and, 25
  - Kerberos and, 27
  - PAM and user, 23
  - pluggable, 23
  - remote access and, 25
- authorizations, 13
  - See also* rights
  - solaris.admin.edit/etc/default/passwd, 41
  - solaris.admin.edit/etc/vfstab, 51

## B

- banner messages
  - configuring, 40
- BART
  - verifying file integrity, 29
- boot environment
  - verifying secure, 28

**C**

- Camellia algorithm, 14
- capabilities *See* rights
- certifications
  - Common Criteria, 30, 32
  - external security standards, 32
  - FIPS 140-2, 32
- changing
  - umask, 45
  - user file permissions, 45
- chmod S+vnounlink command, 53
- Common Criteria
  - certification, 32
- Common Vulnerabilities and Exposures (CVE)
  - monitoring, 57
- compliance
  - assessment, 29
  - benchmarks and reports, 27
  - new features, 14
  - rule variables, 14
  - scheduled assessments, 14
  - value tailoring, 14
- compliance rules
  - value tailoring, 14
- compliance tailorings, 15
- compliance-tailor command, 15
- configuring
  - banner messages, 40
  - installation, 35
  - Kerberos, 54
  - labeled IPsec, 55
  - power management, 39
  - security, 35
  - system initially, 36
  - Trusted Extensions, 55
- Console User rights profile, 39
- critical patch updates (CPU)
  - monitoring, 57
- Cryptographic Framework
  - central repository, 18
  - FIPS 140-2 and, 19, 32
  - IPsec and IKE and, 25
- cusa audit class, 46

**D**

- daemons
  - protected with privileges, 16
- data
  - protecting, 17, 53
- defaultpriv keyword, 47
- defaults
  - access, 16
  - accounts, 16
  - auditing, 16
  - desktop, 16
  - kernel protections, 16
  - network access, 16
  - password algorithm, 16
  - system, 16
  - system file access, 16
  - ZFS file system, 16
- desktop
  - defaults, 16
  - labeled, 31, 55
  - last login dialog box, 14
  - multi-user-desktop package, 36
  - multilevel, 31
  - solaris-desktop package, 35
- desktop login
  - security messages, 14, 40
- desktop package, 36
- disabling
  - unneeded services, 38

**E**

- elfsign command, 14
- encrypting, 13
  - See also* Cryptographic Framework
  - heterogeneous network communications, 27
  - IPsec and, 49
  - network access, 26
  - remote access and, 25
- /etc/default/login file, 44
- /etc/default/passwd file, 41
- /etc/issue file, 40
- /etc/motd file, 40
- /etc/proftpd.conf file, 49
- /etc/security/policy.conf file



editing, 39, 43, 47, 48  
/etc/vfstab file, 51  
evaluations *See* certifications  
events  
    auditing significant, 46  
    cusa audit class, 46

## F

features *See* security features  
file integrity checks  
    monitoring, 57  
file systems  
    labeled, 30  
    protecting, 50  
    ZFS default, 19  
files  
    banner files, 40  
    default system file access, 16  
    /etc/default/login, 44  
    /etc/default/passwd, 41  
    /etc/issue, 40  
    /etc/motd, 40  
    /etc/proftpd.conf, 49  
    /etc/vfstab, 51  
    log files, 29  
    Oracle database logs, 53  
    package verification, 28, 37, 58  
    permissions, 18  
        defaults, 16  
        protecting and modifying, 53  
    preventing accidental deletion, 53  
    syslog, 25  
    verifying integrity, 29  
FIPS 140-2  
    Cryptographic Framework provider, 19  
    IPsec and IKE consumers, 26  
    Kerberos consumer, 27  
    Secure Shell provider, 26  
    validation, 32  
firewalls  
    IP Filter, 24  
    Packet Filter, 15, 24

## G

group packages  
    Oracle Solaris, 35  
GRUB menu  
    password protection, 13  
guidelines  
    developers, for, 31

## H

hardening  
    solaris-minimal-server package, 35  
hardware  
    cryptographic acceleration and, 14  
    Oracle Hardware Management Package, 17  
    restricting user control of, 39, 40  
    SPARC T series servers, 14, 51  
    TPM and, 13  
HISTORY keyword, 41

## I

IKE *See* IPsec and IKE  
ike\_version specification  
    IPsec rules, 15  
immutable zones, 20  
inetd services  
    protecting with TCP wrappers, 25  
installing  
    group packages, 35  
    Kerberos using AI, 27  
    Oracle Solaris, 35  
    Trusted Extensions, 55  
IP Filter  
    packet filtering, 24  
IP packets  
    protecting with IP Filter, 49  
    protecting with IPsec, 25, 49  
IPS packages *See* packages  
IPsec  
    ike\_version specification, 15  
    pass option, 15  
    transitioning to IKEv2 protocol, 15  
IPsec and IKE  
    Cryptographic Framework and, 25

- FIPS 140-2 and, 26
- protecting packets, 25, 49
- isolating
  - applications in zones, 19
- issue file *See* /etc/issue file

## J

- Java Cryptography Extension (JCE), 22

## K

- Kerberos
  - configuring, 54
  - FIPS 140-2 and, 27
  - remote access protection, 27
- kernel
  - defaults, 16
  - protected by privileges, 16
- Kernel SSL proxy, 14
- kernel zones, 20
- Key Management Framework (KMF), 18
- keywords
  - audit\_flags, 46
  - defaultpriv, 47
  - HISTORY, 41
  - lock\_after\_retries, 43
  - MAXWEEKS, 41
  - MINDIFF, 41
  - MINDIGIT, 41
  - MINUPPER, 41
  - MINWEEKS, 41
  - PASSLENGTH, 41
  - RETRIES, 44

## L

- label security
  - file systems and, 30
  - network communications and, 31
  - Trusted Extensions and, 30, 55
- last login
  - notification at desktop login, 14
- legacy applications
  - protecting, 54

- limiting *See* restricting
- live migration *See* secure live migration
- lock\_after\_retries keyword, 43
- locking
  - user account automatically, 43
- log files and system security, 29
- login file *See* /etc/default/login file

## M

- maintaining
  - file integrity with BART, 29
  - system security, 27, 57
- Maintenance and Repair rights profile, 51
- managing
  - audit service, 58
  - Cryptographic Framework, 18
  - password constraints, 41
  - passwords, 22
  - public key objects, 18
- MAXWEEKS keyword, 41
- MINDIFF keyword, 41
- MINDIGIT keyword, 41
- MINUPPER keyword, 41
- MINWEEKS keyword, 41
- modifying *See* changing
- monitoring
  - memory usage, 51
  - system activity and compliance, 57
- motd file *See* /etc/motd file
- multi-user-desktop package, 36
- multilevel desktop
  - in Trusted Extensions, 31, 55
- multilevel security
  - configuring, 55

## N

- network communications
  - defense in depth, 25
  - Kerberos and, 27
  - labeled security and, 31, 55
  - protecting, 48
- nounlink ZFS attribute
  - preventing file deletion, 53

nxheap security extension, 14, 19, 21  
 nxstack security extension, 14, 19, 21

## O

OpenBSD Packet Filter *See* Packet Filter  
 openssh implementation of Secure Shell, 15, 26  
 Oracle Audit Vault, 59  
 Oracle database logs  
   preventing deletion, 53  
 Oracle Hardware Management Package, 17  
 Oracle Solaris group packages, 35

## P

package integrity checks  
   monitoring, 57  
 packages  
   automated installation, 36  
   desktop, 36  
   groups, 35  
   multi-user-desktop, 36  
   repository maintenance, 58  
   signed, 28, 37, 58  
   solaris-large-server, 35  
   solaris-minimal-server, 35  
   solaris-small-server, 35  
   trusted-extensions, 55  
   verifying, 28, 37  
 Packet Filter  
   packet filtering, 24  
 packet filter  
   firewall, 24  
 Packet Filter firewall, 15  
 PAM (Pluggable Authentication Modules)  
   user authentication framework, 23  
 pass option  
   IPsec rules, 15  
 PASSLENGTH keyword, 41  
 passwd command  
   -p option, 14  
 passwd file *See* /etc/default/passwd file  
 password hashes, 14  
 passwords  
   constraints, 22, 41  
   default hash algorithm, 16  
   GRUB menu, 13  
   locking out users, 43  
   PAM and, 23  
   requirements, 16  
   security features, 16, 22  
   SHA256 hash algorithm, 16, 22  
   unlocking user, 44  
 permissions  
   changing user file permissions, 45  
   files, 16, 18  
 PKCS #11 cryptographic library, 18  
 pktool gencsr command, 15  
 pluggable authentication modules *See* PAM  
 policy  
   audited commands, 46  
   label-based MAC policies, 30  
   site security, 33  
 policy.conf file *See* /etc/security/policy.conf  
 file  
 power management  
   configuring, 39  
 powers *See* rights  
 predefined roles, 22  
 preventing accidental file deletion, 53  
 privileges  
   daemons and, 16  
   limiting users, 47  
   Oracle Solaris and, 16, 20  
   protecting kernel processes, 16  
   removing basic, 47  
 process rights *See* privileges  
 profiles *See* rights profiles  
 proftpd.conf file *See* /etc/proftpd.conf file  
 programs *See* applications  
 protecting  
   applications  
     JCE, 22  
     overview, 19  
     with authorizations, 21  
     with TCP wrappers, 23, 25, 49  
     zones, 20  
   data, 17  
   desktop with labels, 31  
   file systems, 50  
   files, 53

- inetd applications
  - with TCP wrappers, 25
- IP packets
  - IP Filter, 49
  - IPsec and IKE, 25, 49
- kernel, 16
- network, 48
- services
  - with SMF authorizations, 21
- users, 41
- users with rights, 22
- pwhash command, 14

**R**

- references for Oracle Solaris, 61
- remote access
  - defending against, 25
- removing
  - power management capability from users, 39
  - privileges from a user, 47
- repositories
  - package verification, 28, 58
- restricting
  - access through Kerberos, 27
  - data flows with label-based MAC policies, 30
  - size of tmpfs file system, 51
  - user control of hardware, 39
  - user file permissions, 45
- RETRIES keyword, 44
- rights, 13
  - See also* authorizations, privileges, rights profiles,
  - roles
  - managing, 23
  - protecting users, 22
- rights profiles
  - Administrator Message Edit, 40
  - auditing, 58
  - Console User, 39, 39
  - creating and assigning, 43, 48
  - Maintenance and Repair, 51
- role-based access control (RBAC) *See* rights
- roles
  - ARMOR, 22
  - auditing, 58
  - predefined, 22

- root, 16
- root role
  - file permissions and, 53
  - initial assignment, 16
- running
  - secure applications, 31

## S

- scheduled assessments, 14
- secure by default, 15
- secure by default (SBD), 15
- secure live migration, 14
- Secure Shell (SSH)
  - FIPS 140-2 and, 26
  - remote access, 26
  - TCP wrappers and, 25
- security
  - label-based, 30, 55
  - maintaining system, 57
  - messages in banner files, 40
  - multilevel, 55
  - new features in this release, 13
  - policy, 33
  - references, 61
  - standards, 32
  - system access and, 53
  - users and, 41, 53
- security compliance *See* compliance
- security evaluations *See* certifications
- security extensions
  - preventing corruption, 14, 19
  - protecting the kernel, 21
- security features
  - ASLR, 19, 21
  - auditing, 28, 58
  - auditing enabled, 16
  - Automated Installer (AI), 35
  - BART, 29
  - compliance assessment and reports, 29
  - Cryptographic Framework, 18
  - immutable zones, 20
  - IP Filter firewall, 24
  - IPsec and IKE, 25
  - Java Cryptography Extension, 22
  - Kerberos, 27

- kernel zones, 20
  - Key Management Framework, 18
  - labeled desktop, 31
  - labeled file system, 30
  - labeled IPsec, 55
  - labeled network, 31
  - labeled security, 30
  - network access, limited, 16
  - nxheap security extension, 21
  - nxstack security extension, 21
  - Oracle Hardware Management Package, 17
  - Packet Filter firewall, 24
  - packet filtering, 24
  - PAM, 23
  - password requirements, 16
  - passwords, 22
  - privileges, 16, 20
  - rights, 22, 23
  - role login, no, 16
  - roles, 22
  - root role, 16
  - secure by default, 15
  - Secure Shell (SSH), 26
  - security extensions, 19
  - Service Management Facility (SMF), 21
  - TCP wrappers, 23, 25
  - Trusted Extensions, 30
  - user rights, 22
  - verified boot, 28
  - ZFS file system, 16
  - zones, 20
  - security keywords *See* keywords
  - security messages
    - on desktop at login, 14, 40
    - placing in banner files, 40
  - security policy *See* policy
  - sendmail
    - TCP wrappers and, 25
  - Service Management Facility (SMF)
    - application protection and, 54
    - rights and, 21
  - services
    - authorizations in SMF, and, 21
    - disabling unneeded, 38
    - inetd
      - protecting with TCP wrappers, 25
    - protecting
      - legacy applications, 54
      - with SMF authorizations, 21
    - svc:/network/ftp, 49
  - signature-policy
    - property on images and package publishers, 28, 37
  - signatures
    - packages and, 28
    - verifying package, 37, 58
  - site security policies
    - audit, 46
    - IP Filter, 24
    - overview, 33
    - per service with TCP wrappers, 25
  - SMF *See* Service Management Facility (SMF)
  - solaris-large-server package, 35
  - solaris-minimal-server package, 35
  - solaris-small-server package, 35
  - solaris.admin.edit/etc/default/passwd authorization, 41
  - solaris.admin.edit/etc/vfstab authorization, 51
  - SPARC T series servers
    - cryptographic acceleration and, 14
    - TMPFS configuration example, 51
    - TPM and, 13
  - SSLv3
    - Kernel SSL proxy and, 14
  - sunssh implementation of Secure Shell, 15, 26
  - Support Repository Updates (SRU)
    - monitoring, 57
  - svc:/network/ftp service, 49
  - syslog utility, 25
  - systems
    - default access, 16
    - initial configuration, 36
    - monitoring, 57, 57
    - securing access to, 16
    - security features for, 16
- T**
- tailorings, 15
  - TCP wrappers
    - protecting applications with, 23, 25, 49
  - tmpfs file system

- limiting size, 51
- Trusted Extensions
  - configuring, 55
  - labeled security and, 30, 55
- trusted-extensions package, 55

- preventing file deletion, 53
- zones
  - immutable, 20
  - isolating applications, 19, 19
  - kernel, 20
  - secure live migration, 14

## U

- umask value, making more restrictive, 45
- unlocking user account, 43
- user rights *See* rights
- users
  - auditing privileged, 46
  - file permissions
    - restricting, 45
  - locking account, 43
  - protecting, 41
  - protecting with rights, 22
  - removing basic privileges, 47
  - restricting control of hardware, 39
  - restricting file permissions, 45
  - umask value, 45
  - unlocking accounts of, 44

## V

- validations *See* certifications
- variable values
  - compliance rules, in, 14
- verified boot, 14
  - system security and, 28
- verifying
  - file integrity, 29
  - package signatures, 37, 58
  - packages, 28, 37, 58
- vfstab file *See* /etc/vfstab file

## Z

- ZFS
  - chmod S+vnounlink command, 53
  - default file system, 16
  - file systems, 19
  - file systems, protecting, 50