Oracle® Solaris 11.3 Security and Hardening Guidelines

Part No: E54807
March 2018

Oracle Solaris 11.3 Security and Hardening Guidelines

Part No: E54807

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

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

Tables

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=E53394-01`.

Feedback

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

♦ ♦ ♦ CHAPTER 1

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

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 Trusted Path Module (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*.
- Elliptic Curve Cryptography (ECC) is available in OpenSSL.
- 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*.
- You can implement smart cards and smart card readers in Oracle Solaris to provide two-factor user authentication (2FA) and nonrepudiation for a range of security solutions, including local login, remote login over a network, secure web communication and secure email. Logging in with a smart card in Oracle Solaris provides much stronger security than network login processes that depend on traditional passwords only. See Chapter 7, "Using Smart Cards for Multifactor Authentication in Oracle Solaris" in *Managing Kerberos and Other Authentication Services in Oracle Solaris 11.3*.
- Oracle Solaris implements one-time passwords (OTP) that can be used with mobile authenticators that conform to RFC 4226 for HMAC-based OTPs and RFC 6238 for time-based OTPs. For more information, see Chapter 8, "Using One-Time Passwords for Multifactor Authentication in Oracle Solaris" in *Managing Kerberos and Other Authentication Services in Oracle Solaris 11.3* and the `otpadm`(1M) and `pam_otp_auth`(5) man pages.
- 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.

- 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.
- 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 and SPARC T8 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*.
- The `pktool gencsr` command can now create certificates for certificate authorities that do not follow the standard PKCS #10: Certification Request Syntax Specification Version 1.7, RFC 2986 (`https://www.rfc-editor.org/info/rfc2986`). See the `pktool`(1) man page.
- When a certificate from a Certificate Authority (CA) is missing or corrupted, you can fix the resulting problem by adding or removing certificates from the Oracle Solaris keystore. For more information, see "Adding CA Certificates to the Oracle Solaris CA Keystore" in *Managing Encryption and Certificates in Oracle Solaris 11.3*.
- Oracle Solaris provides client support for KMIP version 1.1, enabling clients to communicate with Key Management Interoperability Protocol (KMIP)-compliant servers such as the Oracle Key Vault (OKV). PKCS #11 applications, as clients, can communicate with KMIP-compliant servers to create and use asymmetric keys. See Chapter 5, "KMIP and PKCS #11 Client Applications" in *Managing Encryption and Certificates in Oracle Solaris 11.3*.
- Oracle Solaris offers an `openssh` implementation of Secure Shell. This OpenSSH implementation is built on OpenSSH 7.2p2 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 "OpenSSH Implementation of 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 (PF). For more information, see Chapter 4, "OpenBSD Packet Filter Firewall in Oracle Solaris" in *Securing the Network in Oracle Solaris 11.3*.

  PF 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*.

  PF adds the `pflogd` logging facility to PF. For more information, see "Packet Filter Logging" in *Securing the Network in Oracle Solaris 11.3* and the `pflogd`(1M) man page.
- You can verify whether a binary is protected by Oracle Solaris security extensions by running the `elfdump -d` *app-path* command. See "Protecting Against Malware With Security Extensions" in *Securing Systems and Attached Devices in Oracle Solaris 11.3*.
- The Kerberos implementation in Oracle Solaris is based on the latest version of the Kerberos V5 network authentication protocol from the Massachusetts Institute of Technology (MIT). The Oracle Solaris implementation takes advantage of Oracle Solaris features, such as IPS, SMF, and Automated Installation (AI). For more information, see "Introduction to MIT Kerberos on Oracle Solaris" in *Managing Kerberos and Other Authentication Services in Oracle Solaris 11.3*. For information about storing delegated GSS-API credentials, see "Per-Session GSS-API Credentials" in *Managing Secure Shell Access in Oracle Solaris 11.3*.
- 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 servers 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. For more information, see "Passwords and Password Policy" on page 24.

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" (`https://www.oracle.com/technetwork/documentation/sys-mgmt-networking-190072.html#hwmgmt`).

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 2, "Using ACLs and Attributes to Protect Oracle Solaris ZFS Files" in *Securing Files and Verifying File Integrity 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, “Cryptography in Oracle Solaris” in *Managing Encryption and Certificates in Oracle Solaris 11.3* and Chapter 4, “Managing Certificates in Oracle Solaris” in *Managing Encryption and Certificates in Oracle Solaris 11.3*.
- For examples of using the Cryptographic Framework, see Chapter 3, “Using the 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 140-2 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 22. 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 11.3 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.

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:

- Chapter 11, “Configuring and Administering Immutable 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 "Protecting Against Malware With Security Extensions" 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 34.

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 (`https://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 17. 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 ARMOR package provides predefined roles. For more information, see "Using ARMOR Roles" in *Securing Users and Processes in Oracle Solaris 11.3*.

Passwords and Password Policy

Your password change policy should follow industry standards. System administration logins, such as `root`, must be carefully controlled. Administration should be through roles, users with rights profiles, or `sudo`. These administrative methods use least privilege and write administrative events to the audit trail.

Note - The passwords for users who can assume roles must not be subject to any password aging constraints.

For more information, see the following:

- "Controlling Logins" 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 11.3 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 51
- 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 `ipsecconf`(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*
- "OpenSSH and FIPS 140-2" 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*
- "Kerberos and FIPS 140-2 Mode" 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 59
- "How to Verify Your Packages" on page 39

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 47 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 30, 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 3, "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 34.

Trusted Extensions meets the requirements of the Common Criteria Labeled Security Package (LSP). See "Oracle Solaris 11 Common Criteria EAL4+ Certification" on page 34.

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 11.3 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 11.3 Security*
- Appendix G, "Security Considerations When Using C Functions," in *Developer's Guide to Oracle Solaris 11.3 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 Level 1 Cryptography Validation

The Cryptographic Framework feature of Oracle Solaris is validated at FIPS 140-2, 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. Any application that uses OpenSSL for its cryptography can use this validated module. For more information, see *Using a FIPS 140-2 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 (`https://www.oracle.com/technetwork/topics/security/security-evaluations-099357.html`)
- The Common Criteria Recognition Arrangement (`https://www.commoncriteriaportal.org/ccra/index.cfm?`)
- Operating System Protection Profile (`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 11.3 Security*
- Appendix A, "Site Security Policy," in *Trusted Extensions Configuration and Administration*
- "Security Requirements Enforcement" in *Trusted Extensions Configuration and Administration*
- What Is Assurance and Why Does It Matter? (`https://blogs.oracle.com/oraclesecurity/what-is-assurance-and-why-does-it-matter`)

♦ ♦ ♦ CHAPTER 2

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

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 3, "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.	"How to Verify Your Packages" on page 39
2. Ensure that executables are protected.	Verifies that security extensions that protect the stack and heap from compromise are enabled.	"Protecting the Process Heap and Executable Stacks From Compromise" in *Securing Systems and Attached Devices in Oracle Solaris 11.3*
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.	"Controlling Access to System Hardware" in *Securing Systems and Attached Devices in Oracle Solaris 11.3*

Task	Description	For Instructions
4. Disable unneeded services.	Prevents processes that are not part of the system's required functions from running.	"How to Disable Unneeded Services" on page 40
5. Prevent the workstation owner from powering down the system.	Prevents the Console User from shutting down or suspending the system.	"How to Remove Power Management Capability From Users" on page 41
6. Create a login warning message that reflects your site's security policy.	Notifies users before and after authentication that the system is monitored.	"How to Place a Security Message in Banner Files" on page 42

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 60. 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
Configure restrictive file permissions for regular users.	Sets a more restrictive value than `022` for file permissions for regular users.	"How to Set a More Restrictive `umask` Value for Regular Users" on page 46.
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.	"How to Set Account Locking for Regular Users" on page 44
Preselect the `cusa` audit class for all users.	Provides better monitoring and recording of potential threats to the system.	"How to Audit Significant Events in Addition to Login/Logout" on page 47
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.	"Managing User Accounts by Using the CLI" in *Managing User Accounts and User Environments in Oracle Solaris 11.3* "Assigning Rights to Users" in *Securing Users and Processes in Oracle Solaris 11.3*

Task	Description	For Instructions
Reduce the number of visible GNOME desktop applications.	Prevents users from using desktop applications that can affect security.	See Chapter 11, "Disabling Features in the Oracle Solaris Desktop System" in *Oracle Solaris 11.3 Desktop Administrator's Guide*.
Limit a user's privileges.	Removes basic privileges that users do not need.	"How to Remove Unneeded Basic Privileges From Users" on page 48

▼ 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 -1a /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.	"How to Disable the Network Routing Daemon" in *Securing the Network in Oracle Solaris 11.3*
Prevent the dissemination of information about the network topology.	Prevents the broadcast of packets.	"How to Disable Broadcast Packet Forwarding" in *Securing the Network in Oracle Solaris 11.3*
	Prevents responses to broadcast echo requests and multicast echo requests.	"How to Disable Responses to Echo Requests" in *Securing the Network in Oracle Solaris 11.3*
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.	"How to Set Strict Multihoming" in *Securing the Network in Oracle Solaris 11.3*
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.	"How to Set Maximum Number of Incomplete TCP Connections" in *Securing the Network in Oracle Solaris 11.3*
Prevent DoS attacks by controlling the number of permitted incoming connections.	Specifies the default maximum number of pending TCP connections for a TCP listener.	"How to Set Maximum Number of Pending TCP Connections" in *Securing the Network in Oracle Solaris 11.3*
Return network parameters to their secure default values.	Increases security that was reduced by administrative actions.	"How to Reset Network Parameters to Secure Values" in *Securing the Network in Oracle Solaris 11.3*
Add TCP wrappers to network services to limit applications to legitimate users.	Specifies systems that are allowed access to network services, such as FTP.	"How to Use TCP Wrappers" on page 51
Configure a firewall.	Uses the Packet Filter or IP Filter feature to provide a firewall.	Chapter 5, "Configuring the Packet Filter Firewall" in *Securing the Network in Oracle Solaris 11.3* Chapter 7, "Configuring IP Filter Firewall" in *Securing the Network in Oracle Solaris 11.3*
Configure encrypted and authenticated network connections.	Uses IPsec and IKE to protect network transmissions between nodes and networks	Chapter 9, "Configuring IPsec" in *Securing the Network in Oracle Solaris 11.3*

Task	Description	For Instructions
	that are jointly configured with IPsec and IKE.	Chapter 11, "Configuring IKEv2" in *Securing the Network in Oracle Solaris 11.3*

▼ 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 52.

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.	"Setting ZFS Quotas and Reservations" in *Managing ZFS File Systems in Oracle Solaris 11.3*
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.	"Setting Reservations on ZFS File Systems" in *Managing ZFS File Systems in Oracle Solaris 11.3*
Encrypt data on a file system.	Protects a dataset with encryption and a passphrase to access the dataset at dataset creation.	"Encrypting ZFS File Systems" in *Managing ZFS File Systems in Oracle Solaris 11.3* "Examples of Encrypting ZFS File Systems" in *Managing ZFS File Systems in Oracle Solaris 11.3*
Limit the size of the tmpfs file system.	Prevents a malicious user from creating large files in /tmp to slow down the system.	"How to Limit the Size of the tmpfs File System" on page 52

▼ 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.	"How to Set a More Restrictive umask Value for Regular Users" on page 46
Specify ACLs to protect files at a finer granularity than regular UNIX file permissions.	Extended security attributes can be useful in protecting files.	"Using File Attributes to Add Security to ZFS Files" in *Securing Files and Verifying File Integrity in Oracle Solaris 11.3*
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 rm command fails even when run by the root role.	"Preventing Accidental Deletions With the nounlink Attribute" in *Securing Files and Verifying File Integrity in Oracle Solaris 11.3*
Maintain system file integrity.	Finds suspicious files through a script or by using BART.	"How to Find Files With Special File Permissions" in *Securing Files and Verifying File Integrity in Oracle Solaris 11.3*

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.	"Protecting the Process Heap and Executable Stacks From Compromise" in *Securing Systems and Attached Devices in Oracle Solaris 11.3*
Configure auditing.	Customizes audit configuration for coverage and file integrity.	"Using the Audit Service" on page 60
Protect core files that might contain sensitive information.	Creates a directory with limited access that is dedicated to core files.	"Enabling File Paths" in *Troubleshooting System Administration Issues in Oracle Solaris 11.3* "Administering Your Core File Specifications" in *Troubleshooting System Administration Issues in Oracle Solaris 11.3*
Protect a web server with SSL Kernel Proxy.	The Secure Sockets Layer (SSL) protocol can be used to encrypt and accelerate web server communications.	Chapter 3, "Web Servers and the Secure Sockets Layer Protocol" in *Securing the Network in Oracle Solaris 11.3*
Protect legacy services with privileges and authorizations.	Runs applications with least privilege by assigning limited rights to the application.	"Protecting a Legacy Service With SMF" on page 55
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.	*Introduction to Oracle Solaris Zones*
Create and administer immutable zones.	You can administer an immutable zone, but you must take specific steps to enable administration.	"Administering Immutable Non-Global Zones" in *Creating and Using Oracle Solaris Zones*
Manage resources in zones.	Zones provide a number of tools to manage zone resources.	*Administering Resource Management in Oracle Solaris 11.3*

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 that are specific to MIT Kerberos on an Oracle Solaris system, 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).

Tip - Type `man` *man-page* at the command line for the Oracle Solaris versions of MIT Kerberos man pages.

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*

♦ ♦ ♦ 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.	"Administering CVE Updates in Oracle Solaris" in *Oracle Solaris 11.3 Security Compliance Guide*
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.	"Ensuring Secure Package Installation From Your Local IPS Repository" on page 60
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.	"How to Verify Your Packages" on page 39
Run compliance tests.	Assesses the system's compliance to security benchmarks.	*Oracle Solaris 11.3 Security Compliance Guide* and the `compliance`(1M) man page

Task	Description	For Instructions
Verify file integrity.	After configuration, compares BART manifests at regular intervals to ensure that only files that should be changed are changed.	"How to Compare Manifests for the Same System Over Time" in *Securing Files and Verifying File Integrity in Oracle Solaris 11.3*
Find suspicious files.	Locates the potentially unauthorized use of the `setuid` and `setgid` permissions on programs.	"How to Find Files With Special File Permissions" in *Securing Files and Verifying File Integrity in Oracle Solaris 11.3*
Review audit logs regularly.	Locates unusual access and use of the system.	"Using the Audit Service" on page 60
Review audit logs for login and logout events in real time.	Identifies attempted breaches near to the time that the attempts occur.	"Monitoring Audit Records in Real Time" on page 61

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 39.

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 47.
- 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*

♦ ♦ ♦ APPENDIX A

Site Security Policy and Enforcement

This appendix discusses site security policy issues. It covers the following topics:

For additional references, see Appendix B, “Bibliography for Oracle Solaris Security”.

Creating and Managing a Security Policy

Each Oracle Solaris site is unique and must determine its own security policy. Perform the following tasks when creating and managing a security policy.

- Establish a security team. The security team needs to have representation from top-level management, personnel management, computer system management and administrators, and facilities management. The team must review administrators' policies and procedures, and recommend general security policies that apply to all system users.
- Educate management and administration personnel about the site security policy. All personnel involved in the management and administration of the site must be educated about the security policy. Security policies must not be made available to regular users because this policy information has direct bearing on the security of the computer systems.
- Educate users about Oracle Solaris software and the security policy. Because the users are usually the first to know when a system is not functioning normally, the user must become acquainted with the system and report any problems to a system administrator. A secure environment needs the users to notify the system administrators immediately if they notice any of the following:

  - A discrepancy in the last login time that is reported at the beginning of each session
  - An unusual change to file data
  - The inability to operate a user function
  - A lost or stolen printout
  - A lost or stolen mobile device
  - Reported login from unusual sites
  - Emails that request the user to log in to an unusual website or that request sensitive information
- Enforce the security policy. If the security policy is not followed and enforced, the data on your computers is not secure. Establish procedures to record any problems and the measures you took to resolve the incidents.
- Periodically review the security policy. The security team must perform a periodic review of the security policy and all incidents that occurred since the last review. Adjustments to the policy can then lead to increased security.

Site Security Policy and Oracle Solaris

The security administrator must design the network based on the site's security policy. The security policy for Oracle Solaris systems dictates configuration decisions, such as the following:

- How much auditing is done for all users and for which classes of events
- How much auditing is done for users in roles and for which classes of events
- How audit data is managed, archived, and reviewed

  See *Managing Auditing in Oracle Solaris 11.3*.

Computer Security Recommendations

Consider the following list of guidelines when you develop a security policy for your site.

- Update your Oracle Solaris systems to the latest SRU in a timely manner.
- Perform package verification and compliance checks regularly.

  See *Oracle Solaris 11.3 Security Compliance Guide*.
- Perform file verification regularly.

  See Chapter 3, “Verifying File Integrity by Using BART” in *Securing Files and Verifying File Integrity in Oracle Solaris 11.3*.

- Minimize the number of administration IDs.
- Eliminate third-party setuid and setgid programs. Use rights profiles and roles to execute programs and to prevent misuse.
- Encrypt sensitive data on disk and archive media to avoid breaches if hardware or media is lost or stolen.

  See *Managing ZFS File Systems in Oracle Solaris 11.3*.
- Encrypt network traffic with Kerberos, TLS, or IPsec.

  See *Managing Kerberos and Other Authentication Services in Oracle Solaris 11.3* and *Securing the Network in Oracle Solaris 11.3*.
- Isolate appropriate services or applications in different zones or virtual machines.

  See *Introduction to Oracle Solaris Zones*.
- Protect encryption keys and certificates against exposure or loss.

  See *Managing Encryption and Certificates in Oracle Solaris 11.3*.
- Restrict access to shared file systems and network servers to known hosts, users, or network groups which require access.

  See *Managing Secure Shell Access in Oracle Solaris 11.3* and *Managing Network File Systems in Oracle Solaris 11.3*.
- Assign privileges to programs only when they need the privileges to do their work, and only when the programs have been scrutinized and proven to be trustworthy in their use of privilege. Review the privileges on existing Oracle Solaris programs as a guide to setting privileges on new programs.

  If possible, assign at least two individuals to administer Oracle Solaris systems. Assign one person security-related responsibilities, such as assigning passwords and clearances. Assign the other person the System Administrator rights profile for system management tasks.

  See *Securing Users and Processes in Oracle Solaris 11.3*.
- Restrict operating manuals and administrator documentation to individuals with a valid need for access to that information.
- Document file system damage, and analyze all affected files for potential security policy violations.
- Report and document unusual or unexpected behavior of any Oracle Solaris software, and determine the cause.
- Review and analyze audit information regularly. Investigate any irregular events to determine the cause of the event.

  See *Managing Auditing in Oracle Solaris 11.3*.
- Manually record system reboots, power failures, and shutdowns in a site log.
- Establish a regular backup routine.

Physical Security Recommendations

Consider the following list of guidelines when you develop a security policy for your site.

- Restrict access to your systems. The most secure locations are generally interior rooms that are not on the ground floor.
- Monitor and document access to systems.
- Consider removable storage media for sensitive information. Lock up all removable media when the media are not in use.
- Store system backups and archives in a secure location that is separate from the location of the systems.
- Restrict physical access to the backup and archival media in the same manner as you restrict access to the systems.
- Install a high-temperature alarm in the computer facility to indicate when the temperature is outside the range of the manufacturer's specifications. A suggested range is 10°C to 32°C (50°F to 90°F).
- Install a water alarm in the computer facility to indicate water on the floor, in the subfloor cavity, and in the ceiling.
- Install a smoke alarm to indicate fire, and install a fire-suppression system.
- Install a humidity alarm to indicate too much or too little humidity.
- Consider emission security, shielding machines from leaking emanations, including unintentional radio or electrical signals, sounds, and vibrations. This shielding might be appropriate for facility walls, floors, and ceilings.
- Allow only certified technicians to open and close emission security equipment to ensure its ability to shield electromagnetic radiation.
- Check for physical gaps that allow entrance to the facility or to the rooms that contain computer or networking equipment. Look for openings under raised floors, in suspended ceilings, in roof ventilation equipment, and in adjoining walls between original and secondary additions.
- Prohibit eating, drinking, and smoking in computer facilities or near computer equipment. Establish areas where these activities can occur without threat to the computer equipment.
- Protect architectural drawings and diagrams of the computer facility.
- Restrict the use of building diagrams, floor maps, and photographs of the computer facility.

Personnel Security Recommendations

Consider the following list of guidelines when you develop a security policy for your site.

- Inspect packages, documents, and storage media when they arrive and before they leave a secure site.
- Require identification badges on all personnel and visitors at all times.
- Use identification badges that are difficult to copy or counterfeit.
- Establish areas that are prohibited for visitors, and clearly mark the areas.
- Escort visitors at all times.

Equipment Retirement Recommendations

Consider the following list of guidelines when you develop a security policy for your site. Also, refer to Guidelines for Media Sanitization, NIST 800-88r1.

- Do not re-purpose a system with sensitive data to a network that carries less sensitive data.
- Clear and purge hardware disks before destroying them.
  - For hardware disk purging methods, see *Managing Devices in Oracle Solaris 11.3*.
  - For scrubbing a USB, run the `dd` command several times. You have a couple of options:

    ```
    # dd if=/dev/zero of=/dev/sdx iflag=nocache oflag=direct bs=4096

    # dd if=/dev/urandom of=/dev/sdx iflag=nocache oflag=direct bs=4096
    ```
  - For scrubbing solid state devices (SSDs), obtain OS-specific secure erase utilities from the vendor of your SSDs. You can also use a third-party scrubbing application, such as the `sg_sanitize`(8) utility.
- Forbid the use of flash drives and USBs that could carry sensitive information off-site.

Common Security Violations

Because no computer is completely secure, a computer facility is only as secure as the people who use it. Most actions that violate security are easily resolved by careful users or additional equipment. However, the following list gives examples of problems that can occur:

- Users give passwords to other individuals who should not have access to the system.

- Users write down passwords, and lose or leave the passwords in insecure locations.
- Users set their passwords to easily guessed words or easily guessed names.
- Users learn passwords by watching other users type a password.
- Users leave their systems unattended without locking the screen.
- Users change the permissions on a file to allow other users to read the file.
- On a labeled file system, users change the labels on a file to allow other users to read the file.
- Users discard sensitive hardcopy documents without shredding them, or users leave sensitive hardcopy documents in insecure locations.
- Users store sensitive data on unauthorized cloud services.
- Users forward email to unprotected mail servers.
- Users use insecure applications to transfer sensitive data.
- Users leave access doors unlocked.
- Users lose their keys.
- Users lose their laptops and mobile devices.
- Users do not lock up removable storage media.
- Computer screens are visible through exterior windows.
- Unauthorized users remove, replace, or physically tamper with hardware.
- Unauthorized users gain access by plugging their laptop into an ethernet port.
- Unauthorized users connect to wireless networks whose signal extends outside the building.
- Network cables are tapped.
- Wireless network signals are monitored.
- Electronic eavesdropping captures signals emitted from computer equipment.
- External electromagnetic radiation interference such as sun-spot activity scrambles files.
- Power outages, surges, and spikes destroy data.
- Earthquakes, floods, tornadoes, hurricanes, and lightning destroy data.

Security Requirements Enforcement

To ensure that the security of the system is not compromised, administrators need to protect passwords, files, and audit data. You must train users to do their part. To be consistent with the requirements for an evaluated configuration, follow the guidelines in this section.

Users and Security Requirements

Each site's security administrator ensures that users are trained in security procedures. The security administrator needs to communicate the following rules to new employees and remind existing employees of these rules on a regular basis:

- Do not tell anyone your password.

  Anyone who knows your password can access the same information that you can without being identified and therefore without being accountable.
- Do not write your password down or include it in an email message.
- Choose passwords that are hard to guess.
- Do not send your password to anyone by email.
- Do not leave your computer unattended without locking the screen or logging off.
- Do not leave your laptop or other mobile devices unattended in an insecure location.
- Remember that administrators do not rely on email to send instructions to users. Never follow emailed instructions from an administrator without first double-checking with the administrator.

  Be aware that sender information in email can be forged.
- Because you are responsible for the access permissions on files and directories that you create, make sure that the permissions on your files and directories are set appropriately. Do not allow unauthorized users to read a file, to change a file, to list the contents of a directory, or to add to a directory.

Your site might provide additional suggestions.

Email Usage Guidelines

It is an unsafe practice to use email to instruct users to take an action.

Warn users not to trust email with instructions that purport to come from an administrator. Doing so prevents the possibility that spoofed email messages could be used to fool users into changing a password to a certain value or divulging the password, which could subsequently be used to log in and compromise the system.

Password Enforcement

The System Administrator role must specify a unique user name and user ID when creating a new account. When choosing the name and ID for a new account, you must ensure that both the user name and associated ID are not duplicated anywhere on the network and have not been previously used. See also "Passwords and Password Policy" on page 24.

The Security Administrator role is responsible for specifying the original password for each account and for communicating the passwords to users of new accounts. You must consider the following information when administering passwords:

- Make sure that the accounts for users who are able to assume the Security Administrator role are configured so that the account cannot be locked. This practice ensures that at least one account can always log in and assume the Security Administrator role to reopen everyone's account if all other accounts are locked.
- Communicate the password to the user of a new account in such a way that the password cannot be eavesdropped by anyone else.
- Change an account's password if you have any suspicion that the password has been discovered by someone who should not know it.
- Never reuse user names or user IDs over the lifetime of the system.

  Ensuring that user names and user IDs are not reused prevents possible confusion about the following:

  - Which actions were performed by which user when audit records are analyzed
  - Which user owns which files when archived files are restored

Information Protection

You as an administrator are responsible for correctly setting up and maintaining discretionary access control (DAC) and mandatory access control (MAC) protections for security-critical files. Critical files include the following:

- `shadow` **file** – Contains encrypted passwords. See the `shadow`(4) man page.
- `auth_attr` **file** – Contains custom authorizations. See the `auth_attr`(4) man page.
- `prof_attr` **file** – Contains custom rights profiles. See the `prof_attr`(4) man page.
- `exec_attr` **file** – Contains commands with security attributes that the site has added to rights profiles. See the `exec_attr`(4) man page.
- **Audit trail** – Contains the audit records that the audit service has collected. See the `audit.log`(4) man page.

Password Protection

In local files, passwords are protected from viewing by DAC and from modifications by both DAC and MAC. Passwords for local accounts are maintained in the `/etc/shadow` file, which is readable only by `root`. For more information, see the `shadow`(4) man page.

Group Administration Practices

The System Administrator role needs to verify on the local system and on the network that all groups have a unique group ID (GID).

When a local group is deleted from the system, the System Administrator role must ensure the following:

- All objects with the GID of the deleted group must be deleted or assigned to another group.
- All users who have the deleted group as their primary group must be reassigned to another primary group.

User Deletion Practices

When an account is deleted from the system, the System Administrator role and the Security Administrator role must take the following actions:

- Delete the account's home directories in every zone.
- Delete any processes or jobs that are owned by the deleted account:
  - Delete any objects that are owned by the account, or assign the ownership to another user.
  - Delete any `at` or `batch` jobs that are scheduled on behalf of the user. For details, see the `at`(1) and `crontab`(1) man pages.
- Never reuse the user name or user ID.

♦ ♦ ♦ APPENDIX B

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 Solaris 11 Documentation 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 140-2 Enabled System in Oracle Solaris 11.3*
- *Developer's Guide to Oracle Solaris 11.3 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,* BiIl Calkins. 2013. Prentice Hall. ISBN 9780133007114.

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

Index