Oracle® Solaris 11 Security Guidelines

Part No: 819–3195–11
March 2012

120305@25097

Contents

Preface

This guide presents security guidelines for the Oracle Solaris operating system (Oracle Solaris OS). First, the guide describes security issues that an enterprise OS must address. Then, it describes the default security features of the Oracle Solaris OS. Finally, the guide provides specific steps to take to harden the system and to use Oracle Solaris security features to protect your data and applications. You can tailor the recommendations in this guide to your site security policy.

Audience

Oracle Solaris 11 Security Guidelines is intended for security administrators and other administrators who perform the following tasks:

- Analyze security requirements
- Implement site security policy in software
- Install and configure the Oracle Solaris OS
- Maintain system and network security

To use this guide, you must have general knowledge of UNIX administration, a good foundation in software security, and knowledge of your site security policy.

Access to Oracle Support

Oracle customers 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.

Typographic Conventions

The following table describes the typographic conventions that are used in this book.

TABLE P–1 Typographic Conventions

Typeface	Description	Example
`AaBbCc123`	The names of commands, files, and directories, and onscreen computer output	Edit your `.login` file. Use `ls -a` to list all files. `machine_name% you have mail.`

`AaBbCc123`	What you type, contrasted with onscreen computer output	`machine_name%` **`su`**
		`Password:`

aabbcc123	Placeholder: replace with a real name or value	The command to remove a file is `rm` *filename*.
AaBbCc123	Book titles, new terms, and terms to be emphasized	Read Chapter 6 in the *User's Guide*. A *cache* is a copy that is stored locally. Do *not* save the file. **Note:** Some emphasized items appear bold online.

Shell Prompts in Command Examples

The following table shows the default UNIX system prompt and superuser prompt for shells that are included in the Oracle Solaris OS. Note that the default system prompt that is displayed in command examples varies, depending on the Oracle Solaris release.

TABLE P–2 Shell Prompts

Shell	Prompt
Bash shell, Korn shell, and Bourne shell	`$`
Bash shell, Korn shell, and Bourne shell for superuser	`#`
C shell	`machine_name%`
C shell for superuser	`machine_name#`

CHAPTER 1

Overview of Oracle Solaris 11 Security

Oracle Solaris 11 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 11 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.

- "Oracle Solaris 11 Security Protections" on page 9
- "Oracle Solaris 11 Security Technologies" on page 10
- "Oracle Solaris 11 Security Defaults" on page 18
- "Site Security Policy and Practice" on page 20

Oracle Solaris 11 Security Protections

Oracle Solaris provides a solid foundation for company data and applications by protecting data on disk and in transit. Oracle Solaris Resource Manager, referred to as *resource management*, and Oracle Solaris Zones provide features that separate and protect applications from misuse. This containment, together with least privilege implemented through privileges and the role-based access control (RBAC) feature of Oracle Solaris, reduce the security risk of intruder or regular user actions. Authenticated and encrypted protocols such as IP security (IPsec) provide virtual private networks (VPNs) across the Internet, as well as tunnels within a LAN or a WAN for safe data delivery. Additionally, the auditing feature of Oracle Solaris ensures that records are kept of any activity of interest.

Oracle Solaris 11 security services provide defense in depth by offering layers of protection for the system and the network. Oracle Solaris protects the kernel by limiting, within kernel utilities, what privileged actions the utility can perform. The default network configuration provides data protection on the system and across the wire. IPsec, the IP Filter feature of Oracle Solaris, and Kerberos can provide additional protections.

Oracle Solaris security services include:

- Protecting the kernel – Kernel daemons and devices are protected by file permissions and by privileges.
- Protecting logins – Logins require passwords. Passwords are strongly encrypted. Remote logins are initially limited to an encrypted and authenticated channel through the Secure Shell feature of Oracle Solaris. The `root` account cannot log in directly.
- Protecting data – Data on disk is protected by file permissions. Additional layers of protection can be configured. For example, you can use access control lists (ACLs), place data in a zone, encrypt a file, encrypt an Oracle Solaris ZFS dataset, create a read-only ZFS dataset, and mount file systems so that `setuid` programs cannot be run and executable files cannot be executed.

Oracle Solaris 11 Security Technologies

The security features of Oracle Solaris can be configured to implement your site's security policy.

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.

Audit Service

Auditing is the collecting of data about the use of system resources. The audit data provides a record 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, 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 29, "Auditing (Reference)," in *Oracle Solaris Administration: Security Services*.
- For guidelines, see "Audit Significant Events in Addition to Login/Logout" on page 30 and the man pages.
- For an overview of auditing, see Chapter 26, "Auditing (Overview)," in *Oracle Solaris Administration: Security Services*.
- For auditing tasks, see Chapter 28, "Managing Auditing (Tasks)," in *Oracle Solaris Administration: Security Services*.

Basic Audit Reporting Tool

The Basic Audit Reporting Tool (BART) feature of Oracle Solaris enables you to comprehensively validate systems by performing file-level checks of a system over time. By creating BART manifests, you can easily and reliably gather information about the components of the software stack that is installed on deployed systems.

BART is a useful tool for integrity management on one system or on a network of systems.

For more information, see the following:

- Selected man pages include `bart`(1M), `bart_rules`(4), and `bart_manifest`(4).
- For guidelines, see "Creating a BART Snapshot of the System" on page 43, "Using the Basic Audit Reporting Tool" on page 45, and the man pages.
- For an overview of BART, see Chapter 6, "Verifying File Integrity by Using BART," in *Oracle Solaris Administration: Security Services*.
- For examples of using BART, see "Using BART (Tasks)" in *Oracle Solaris Administration: Security Services* and the man pages.

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. The different storage mechanisms, administrative utilities, and programming interfaces for various public key infrastructures (PKIs) can use a unified interface when they adopt KMF interfaces.

The Cryptographic Framework provides cryptographic services to users and applications through individual commands, a user-level programming interface, a kernel programming interface, and user-level and kernel-level frameworks. The Cryptographic Framework provides these cryptographic services to applications and kernel modules in a manner seamless to the end user. It also brings direct cryptographic services, like encryption and decryption for files, to the end user.

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)`, `encrypt(1)`, `mac(1)`, `pktool(1)`, and `kmfcfg(1)`.
- For an overview of cryptographic services, see Chapter 11, "Cryptographic Framework (Overview)," in *Oracle Solaris Administration: Security Services* and Chapter 13, "Key Management Framework," in *Oracle Solaris Administration: Security Services*.
- For examples of using the Cryptographic Framework, see Chapter 12, "Cryptographic Framework (Tasks)," in *Oracle Solaris Administration: Security Services* and the man pages.

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, ZFS supports access control lists (ACLs), also called access control entries (ACEs), which more finely control access to individual or groups of file system objects.

For more information, see the following:

- For instructions on setting ACLs on ZFS files, see the `chmod(1)` man page.
- For an overview of file permissions, see "Using UNIX Permissions to Protect Files" in *Oracle Solaris Administration: Security Services*.
- For an overview and examples of protecting ZFS files, see Chapter 8, "Using ACLs and Attributes to Protect Oracle Solaris ZFS Files," in *Oracle Solaris Administration: ZFS File Systems* and the man pages.

Packet Filtering

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

IP Filter

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:

- Selected man pages include `ipfilter(5)`, `ipf(1M)`, `ipnat(1M)`, `svc.ipfd(1M)`, and `ipf(4)`.
- For an overview of IP Filter, see Chapter 20, "IP Filter in Oracle Solaris (Overview)," in *Oracle Solaris Administration: IP Services*.
- For examples of using IP Filter, see Chapter 21, "IP Filter (Tasks)," in *Oracle Solaris Administration: IP Services* and the man pages.
- For information and examples about the syntax of the IP Filter policy language, see the `ipnat(4)` man page.

TCP Wrappers

TCP wrappers provide a way of implementing access controls by checking 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, which is a useful monitoring function. The Secure Shell and `sendmail` features of Oracle Solaris are configured to use TCP wrappers. Network services that might be placed under access control include `ftpd` and `rpcbind`.

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 more information, see the following:

- For information about TCP wrappers, see "How to Use TCP Wrappers to Control Access to TCP Services" in *Oracle Solaris Administration: IP Services*.
- For information and examples of the syntax of the access control language for TCP wrappers, see the `hosts_access`(4) man page.

Passwords and Password Constraints

Strong user passwords help defend against attacks involving brute force guessing.

Oracle Solaris has a number of features that can be used to promote strong user passwords. Password length, content, frequency of change, and modification requirements can be set, and a password history can be kept. A password dictionary of passwords to be avoided is provided. Several possible password algorithms are available.

For more information, see the following:

- "Maintaining Login Control" in *Oracle Solaris Administration: Security Services*
- "Securing Logins and Passwords (Tasks)" in *Oracle Solaris Administration: Security Services*

- Selected man pages include `passwd(1)` and `crypt.conf(4)`.

Pluggable Authentication Module

The Pluggable Authentication Module (PAM) framework enables you to coordinate and configure user authentication requirements for accounts, credentials, sessions, and passwords.

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 `ftp` use the PAM framework to ensure that all entry points for the system have been secured. This architecture 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.

For more information, see the following:

- Chapter 14, "Using PAM," in *Oracle Solaris Administration: Security Services*
- `pam.conf(4)` man page

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 command, a user, a role, or a system. Many Oracle Solaris commands and daemons run with only those privileges that are required to perform their task. The use of privileges is also called *process rights management*.

Privilege-aware programs can prevent intruders from gaining more privileges than the program itself uses. Additionally, privileges enable organizations to limit which privileges are granted to services and processes that run on their systems.

For more information, see the following:

- "Privileges (Overview)" in *Oracle Solaris Administration: Security Services*
- "Using Privileges (Tasks)" in *Oracle Solaris Administration: Security Services*
- Chapter 2, "Developing Privileged Applications," in *Developer's Guide to Oracle Solaris 11 Security*
- Selected man pages include `ppriv(1)` and `privileges(5)`.

Remote Access

Remote access attacks can damage a system and a network. Securing network access is necessary in today's Internet environment, and is useful even in WAN and LAN environments.

IPsec and IKE

IP security (IPsec) protects IP packets by authenticating the packets, by encrypting the packets, or by doing both. Oracle Solaris supports IPsec for both IPv4 and IPv6. 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 key exchange protocol, IKE, use algorithms from the Cryptographic Framework. Additionally, the Cryptographic Framework provides a softtoken keystore for applications that use the metaslot. 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 the softtoken keystore.

When properly administered, IPsec is an effective tool in securing network traffic.

For more information, see the following:

- Chapter 14, "IP Security Architecture (Overview)," in *Oracle Solaris Administration: IP Services*
- Chapter 15, "Configuring IPsec (Tasks)," in *Oracle Solaris Administration: IP Services*
- Chapter 17, "Internet Key Exchange (Overview)," in *Oracle Solaris Administration: IP Services*
- Chapter 18, "Configuring IKE (Tasks)," in *Oracle Solaris Administration: IP Services*
- Selected man pages include `ipsecconf`(1M) and `in.iked`(1M).

Secure Shell

The Secure Shell feature of Oracle Solaris enables users or services to access or transfer files between remote systems over an encrypted communications channel. In Secure Shell, all network traffic is encrypted. 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. By default, Secure Shell is the only active remote access mechanism on a newly installed system.

For more information, see the following:

- Chapter 15, "Using Secure Shell," in *Oracle Solaris Administration: Security Services*
- Selected man pages include `ssh`(1), `sshd`(1M), `sshd_config`(4), and `ssh_config`(4).

Kerberos Service

The Kerberos feature of the Oracle Solaris enables single sign-on and secure transactions, even over heterogeneous networks that run the Kerberos service.

Kerberos is based on the Kerberos V5 network authentication protocol that was developed at the Massachusetts Institute of Technology (MIT). The Kerberos service is a client-server architecture that 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 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:

- Part VI, "Kerberos Service," in *Oracle Solaris Administration: Security Services*
- Selected man pages include `kerberos(5)` and `kinit(1)`.

Role-Based Access Control

RBAC applies the security principle of least privilege by enabling organizations to selectively grant administrative rights to users or roles according to their unique needs and requirements.

The role-based access control (RBAC) feature of Oracle Solaris controls user access to tasks that would normally be restricted to the `root` role. By applying security attributes to processes and to users, RBAC can distribute administrative rights among several administrators. RBAC is also called *user rights management*.

For more information, see the following:

- Part III, "Roles, Rights Profiles, and Privileges," in *Oracle Solaris Administration: Security Services*
- Selected man pages include `rbac(5)`, `roleadd(1M)`, `profiles(1)`, and `user_attr(4)`.

Service Management Facility

The Service Management Facility (SMF) feature of the Oracle Solaris is used to add, remove, configure, and manage services. SMF uses RBAC 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:

- Chapter 6, "Managing Services (Overview)," in *Oracle Solaris Administration: Common Tasks*
- Chapter 7, "Managing Services (Tasks)," in *Oracle Solaris Administration: Common Tasks*
- Selected man pages include `svcadm(1M)`, `svcs(1)`, and `smf(5)`.

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 ACE protect files, and RBAC supports the delegated administration of ZFS datasets.

For more information, see the following:

- Chapter 1, "Oracle Solaris ZFS File System (Introduction)," in *Oracle Solaris Administration: ZFS File Systems*
- Chapter 3, "Oracle Solaris ZFS and Traditional File System Differences," in *Oracle Solaris Administration: ZFS File Systems*
- Chapter 6, "Managing Oracle Solaris ZFS File Systems," in *Oracle Solaris Administration: ZFS File Systems*
- Selected man pages include `zfs`(1M) and `zfs`(7FS).

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 more information, see the following:

- Part II, "Oracle Solaris Zones," in *Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management*
- Selected man pages include `brands`(5), `zoneadm`(1M), and `zonecfg`(1M).

Trusted Extensions

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. Unlike most other multilevel operating systems, Trusted Extensions includes a multilevel desktop.

Trusted Extensions meets the requirements of the Common Criteria Labeled Security Protection Profile (LSPP), the Role-Based Access Protection Profile (RBACPP) and the Controlled Access Protection Profile (CAPP). However, the Trusted Extensions implementation is unique in its ability to provide high assurance, while maximizing compatibility and minimizing overhead.

For more information, see the following:

- For information about configuring and maintaining Trusted Extensions, see *Trusted Extensions Configuration and Administration*.
- For information about using the multilevel desktop, see *Trusted Extensions User's Guide*.
- Selected man pages include `trusted_extensions(5)` and `labeld(1M)`.

Oracle Solaris 11 Security Defaults

After installation, Oracle Solaris 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 two accounts is initially identical.

- 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 one alphabetic character and one numeric character. Passwords are hashed by using the `SHA256` algorithm. When changing their password, all users including the `root` role must conform to these password requirements.

Limited network access – After installation, the system is protected from intrusion over the network. Remote login by the initial user is allowed over an authenticated, encrypted connection with the `ssh` protocol. This is the only network protocol that accepts incoming packets. The `ssh` key is wrapped by the `AES128` algorithm. With encryption and authentication in place, the user can reach the 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 an `ssh` 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` can be traced 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, and desktop applications are protected by least privilege, permissions, and 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 directory permissions are `drwxr-xr-x` (`755`). The file permissions are `-rw-r--r--` (`644`).

Desktop applets – Desktop applets are protected by RBAC. For example, only the initial user or the `root` role can use the Package Manager applet to install new packages. The Package Manager is not displayed to regular users who are not assigned the rights to use it.

Additional Security Features Are in Place

Oracle Solaris 11 provides security features that can be used to configure your systems and users to satisfy site security requirements.

- **Role-based access control (RBAC) –** Oracle Solaris provides a number of authorizations, privileges, and rights profiles. `root` is the only defined role. The rights profiles provide a good basis for roles that you create. Also, some administrative commands require RBAC authorizations to succeed. Users without the authorizations cannot run the commands, even if the users have the required privileges.

- **User rights –** Users are assigned a basic set of privileges, rights profiles, and authorizations from the /etc/security/policy.conf file, just like the initial user as described in "System Access Is Limited and Monitored" on page 18. User login attempts are not limited, but all failed logins are logged by the audit service.
- **System file protection –** System files are protected by file permissions. Only the root role can modify system configuration files.

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.

For more information, review the following:

- Appendix A, "Site Security Policy," in *Trusted Extensions Configuration and Administration*
- "Security Requirements Enforcement" in *Trusted Extensions Configuration and Administration*
- Keeping Your Code Secure (http://blogs.oracle.com/maryanndavidson/entry/those_who_can_t_do)

◆ ◆ ◆ CHAPTER 2

Configuring Oracle Solaris 11 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

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

- **Oracle Solaris Large Server –** 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 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 an Oracle Solaris server. For more information, see the article Optimizing the Oracle Solaris 11 Desktop for a Multiuser Environment.

For automated installation using the Automated Installer (AI), see Part III, "Installing Using an Install Server," in *Installing Oracle Solaris 11 Systems*.

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

- *Installing Oracle Solaris 11 Systems*
- *Creating a Custom Oracle Solaris 11 Installation Image*
- *Adding and Updating Oracle Solaris 11 Software Packages*

Securing the System

The following tasks are best performed in order. At this point, the Oracle Solaris 11 OS is installed and only the initial user who can assume the root role has access to the system.

Task	Description	For Instructions
1. Verify the packages on the system.	Checks that the packages from the installation media are identical to the installed packages.	"Verify Your Packages" on page 22
2. Safeguard the hardware settings on the system.	Protects hardware by requiring a password to change hardware settings.	"Controlling Access to System Hardware (Tasks)" in *Oracle Solaris Administration: Security Services*
3. Disable unneeded services.	Prevents processes that are not part of the system's required functions from running.	"Disable Unneeded Services" on page 23
4. Require device allocation.	Prevents the use of removable media without explicit authorization. Devices include microphones, USB drives, and CDs.	"How to Enable Device Allocation" in *Oracle Solaris Administration: Security Services*
5. Prevent the workstation owner from powering down the system.	Prevents the Console User from shutting down or suspending the system.	"Remove Power Management Capability From Users" on page 23
6. Create a login warning message that reflects your site's security policy.	Notifies users and would-be attackers that the system is monitored.	"Place Security Message in Banner Files" on page 24 "Place Security Message on the Desktop Login Screen" on page 25

▼ Verify Your Packages

Immediately after installation, validate the installation by verifying your packages.

Before You Begin You must be in the root role.

1 **Run the `pkg verify` command.**

To keep a record, send the command output to a file.

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

2 **Review the log for any errors.**

3 **If you find errors, reinstall from the media or fix the errors.**

See Also For more information, see the `pkg`(1) and `pkg`(5) man pages. The man pages contain examples of using the `pkg verify` command.

▼ Disable Unneeded Services

Use this procedure to disable services that are not required, given the purpose of your system.

Before You Begin You must be in the `root` role.

1 **List the online services.**

```
# svcs | grep network
online          Sep_07   svc:/network/loopback: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 the 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 6, "Managing Services (Overview)," in *Oracle Solaris Administration: Common Tasks* and the `svcs`(1) man page.

▼ Remove Power Management Capability From Users

Use this procedure to prevent users of this system from suspending the system or powering it down.

Before You Begin You must be in the `root` role.

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

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

2. **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 or Change a Rights Profile" in *Oracle Solaris Administration: Security Services*.

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

   ```
   #CONSOLE_USER=Console User
   ```

4. **Assign users the rights profile that you created in Step 2.**

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

See Also For more information, see "policy.conf File" in *Oracle Solaris Administration: Security Services* and the `policy.conf(4)` and `usermod(1M)` man pages.

▼ Place Security Message in Banner Files

Use this procedure to create warning messages that reflect your site's security policy. The contents of these files display at local and remote login.

Note – The sample messages in this procedure do not satisfy U.S. government requirements and likely do not satisfy your security policy.

Before You Begin You must be in the `root` role. Best practice is to consult with your company's legal counsel about the content of the security message.

1. **Type a security message into the `/etc/issue` file.**

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

   This machine is available to authorized users only.

   If you are an authorized user, continue.

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

   For more information, see the `issue(4)` man page.

   The `telnet` program displays the contents of the `/etc/issue` file as its login message. For use of this file by other applications, see "Display Security Message to `ssh` and `ftp` Users" on page 34 and "Place Security Message on the Desktop Login Screen" on page 25.

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

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

▼ Place Security Message on the Desktop Login Screen

Choose from several methods to create a security message for users to review at login.

For more information, click the System > Help menu on the desktop to bring up the GNOME Help Browser. You can also use the `yelp` command. Desktop login scripts are discussed in the `GDM Login Scripts and Session Files` section of the `gdm`(1M) man page.

Note – The sample message in this procedure does not satisfy U.S. government requirements and likely does not satisfy your security policy.

Before You Begin You must be in the `root` role. Best practice is to consult with your company's legal counsel about the content of the security message.

● **Place a security message on the desktop login screen.**

You have several options. The options that create a dialog box can use the `/etc/issue` file from Step 1 of "Place Security Message in Banner Files" on page 24.

- **OPTION 1: Create a desktop file that displays the security message in a dialog box at login.**

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

  After being authenticated in the login window, the user must close the dialog box to reach the workspace. For the options to the `zenity` command, see the `zenity`(1) man page.

- **OPTION 2: Modify a GDM initialization script to display the security message in a dialog box.**

  The `/etc/gdm` directory contains three initialization scripts that display the security message before, during, or immediately after desktop login. These scripts are also available in the Oracle Solaris 10 release.

  - **Display the security message before the login screen appears.**

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

- **Display the security message on the login screen after authentication.**

  This script runs before the user workspace appears. You modify the `Default.sample` script to create this script.

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

- **Display the security message in the user's initial workspace after authentication.**

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

  Note – The dialog box can be covered by windows on the user's workspace.

- **OPTION 3: Modify the login window to display the security message above the entry field.**

  The login window expands to fit your message. This method does not point to the `/etc/issue` file. You must type the text into the GUI.

  Note – The login window, `gdm-greeter-login-window.ui`, is overwritten by the `pkg fix` and `pkg update` commands. To preserve your changes, copy the file to a configuration files directory, and merge its changes with the new file after upgrading the system. For more information, see the `pkg`(5) man page.

  ---

  a. **Change directory to the login window user interface.**

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

  b. **(Optional) Save a copy of the original login window UI.**

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

  c. **Add a label to the login window by using the GNOME Toolkit interface designer.**

  The `glade-3` program opens the GTK+ interface designer. You type the security message into a label that displays above the user entry field.

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

  To review the guide to the interface designer, click Development in the GNOME Help Browser. The `glade-3`(1) man page is listed under Applications in the Manual Pages.

  d. **(Optional) After modifying the login window GUI, save a copy.**

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

Example 2–1 Creating a Short Warning Message at Desktop Login

In this example, the administrator types a short message as an argument to the `zenity` command in the desktop file. The administrator also uses the `--warning` option, which displays a warning icon with the message.

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

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.

Task	Description	For Instructions
Require strong passwords and frequent password changes.	Strengthens the default password constraints on each system.	"Set Stronger Password Constraints" on page 28
Configure restrictive file permissions for regular users.	Sets a more restrictive value than `022` for file permissions for regular users.	"Set More Restrictive `umask` Value for Regular Users" on page 30.
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.	"Set Account Locking for Regular Users" on page 29
Preselect additional audit classes.	Provides better monitoring and recording of potential threats to the system.	"Audit Significant Events in Addition to Login/Logout" on page 30
Send text summaries of audit events to the `syslog` utility.	Provides real-time coverage of significant audit events, such as logins and attempted logins.	"Monitor `lo` Events in Real Time" on page 31
Create roles.	Distributes discrete administrative tasks to several trusted users so that no one user can damage the system.	"Setting Up User Accounts" in *Oracle Solaris Administration: Common Tasks* "How to Create a Role" in *Oracle Solaris Administration: Security Services* "How to Assign a Role" in *Oracle Solaris Administration: Security Services*.
Show permitted applications only on a user's desktop.	Prevents users from seeing or using applications that they are not authorized to use.	See "How to Limit a User to Desktop Applications" in *Trusted Extensions Configuration and Administration*.

Task	Description	For Instructions
Limit a user's privileges.	Removes basic privileges that users do not need.	“Remove Unneeded Basic Privileges From Users” on page 32

▼ Set Stronger Password Constraints

Use this procedure if the defaults do not satisfy your site security requirements. The steps follow the list of entries in the `/etc/default/passwd` file.

Before You Begin Before changing the defaults, ensure that the changes allow all users to authenticate to their applications and to other systems on the network.

You must be in the `root` role.

● **Edit the `/etc/default/passwd` file.**

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

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

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

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

c. **Keep a password history.**

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

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

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

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

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

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

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

See Also

- For the list of variables that constrain password creation, see the /etc/default/passwd file. The defaults are indicated in the file.
- For the password constraints in effect after installation, see "System Access Is Limited and Monitored" on page 18.
- passwd(1) man page

▼ Set Account Locking for Regular Users

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

Note – Do not set account locking for users who can assume roles because you can lock out the role.

Before You Begin You must be in the root role. Do not set this protection system-wide on a system that you use for administrative activities.

1 **Set the LOCK_AFTER_RETRIES security attribute to YES.**

- **Set system-wide.**

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

- **Set per user.**

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

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

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

See Also

- For a discussion of user and role security attributes, see Chapter 10, "Security Attributes in Oracle Solaris (Reference)," in *Oracle Solaris Administration: Security Services*.
- Selected man pages include policy.conf(4) and user_attr(4).

▼ Set More Restrictive umask Value for Regular Users

If the default umask value, 022, is not restrictive enough, set a more restrictive mask by using this procedure.

Before You Begin You must be in the root role.

● **Modify the umask value in the login profiles in the skeleton directories for the various shells.**

Oracle Solaris provides directories for administrators to customize user shell defaults. These skeleton directories include files such as .profile, .bashrc and .kshrc.

Choose one of the following values:

- umask 027 – Provides moderate file protection

  (740) – w for group, rwx for others
- umask 026 – Provides slightly stricter file protection

  (741) – w for group, rw for others
- umask 077 – Provides complete file protection

  (700) – No access for group or others

See Also For more information, see the following:

- "Setting Up User Accounts" in *Oracle Solaris Administration: Common Tasks*
- "Default umask Value" in *Oracle Solaris Administration: Security Services*
- Selected man pages include usermod(1M) and umask(1).

▼ Audit Significant Events in Addition to Login/Logout

Use this procedure to audit administrative commands, attempts to invade the system, 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 be in the root role. You are implementing your site's security policy with regard to auditing.

1 **Audit all uses of privileged commands by users and roles.**

For all users and roles, add the AUE_PFEXEC audit event to their preselection mask.

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

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

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

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

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

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

See Also

- For information about audit policy, see "Audit Policy" in *Oracle Solaris Administration: Security Services*.
- For examples of setting audit flags, see "Configuring the Audit Service (Tasks)" in *Oracle Solaris Administration: Security Services* and "Troubleshooting the Audit Service (Tasks)" in *Oracle Solaris Administration: Security Services*.
- To configure auditing, see the auditconfig(1M) man page.

▼ Monitor lo Events in Real Time

Use this procedure to activate the audit_syslog plugin for events that you want to monitor as they happen.

Before You Begin You must be in the root role to modify the syslog.conf file. Other steps require you to be assigned the Audit Configuration rights profile.

1 **Send the lo class to the audit_syslog plugin, and make the plugin active.**

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

2 **Add an audit.notice entry to the syslog.conf file.**

The default entry includes the location of the log file.

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

3 **Create the log file.**

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

4 **Refresh the configuration information for the syslog service.**

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

5 **Refresh the audit service.**

The audit service reads the changes to the audit plugin upon refresh.

```
# audit -s
```

See Also

- To send the audit summaries to another system, see the example following "How to Configure syslog Audit Logs" in *Oracle Solaris Administration: Security Services*.

- The audit service can generate extensive output. To manage the logs, see the `logadm(1M)` man page.
- To monitor the output, see "Monitoring `audit_syslog` Audit Summaries" on page 46.

Remove Unneeded Basic Privileges From Users

Under particular circumstances, one or more of three basic privileges can be removed from a regular user's basic set.

- `file_link_any` – Allows a process to create hard links to files owned by a UID different from the effective UID of the process.
- `proc_info` – Allows a process to examine the status of processes other than those it can send signals to. Processes that 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.

Before You Begin You must be in the `root` role.

1. **Prevent a user from linking to a file that the user does not own.**

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

2. **Prevent a user from examining processes that the user does not own.**

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

3. **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
```

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

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

See Also For more information, see Chapter 8, "Using Roles and Privileges (Overview)," in *Oracle Solaris Administration: Security Services* and the `privileges(5)` man page.

Securing the Kernel

At this point, you might have created users who can assume roles, and have created the roles. Only the root role can modify system files.

Task	Description	For Instructions
Prevent programs from exploiting an executable stack.	Sets a system variable that prevents the exploitation of buffer overflows that exploit the executable stack.	"Protecting Executable Files From Compromising Security" in *Oracle Solaris Administration: Security Services*
Protect core files that might contain sensitive information.	Creates a directory with limited access that is dedicated to core files.	"How to Enable a Global Core File Path" in *Oracle Solaris Administration: Common Tasks* "Managing Core Files (Task Map)" in *Oracle Solaris Administration: Common Tasks*

Configuring the Network

At this point, you might have created users who can assume roles, and have created the roles. Only the root role can modify system files.

From the following network tasks, perform the tasks that provide additional security according to your site requirements. These network tasks notify users who are logging in remotely that the system is protected, and strengthen the IP, ARP, and TCP protocols.

Task	Description	For Instructions
Display warning messages that reflect your site's security policy.	Notifies users and would-be attackers that the system is monitored.	"Display Security Message to ssh and ftp Users" on page 34
Disable the network routing daemon.	Limits access to systems by would-be network sniffers.	"Disable the Network Routing Daemon" on page 35
Prevent the dissemination of information about the network topology.	Prevents the broadcast of packets.	"Disable Broadcast Packet Forwarding" on page 35
	Prevents responses to broadcast echo requests and multicast echo requests.	"Disable Responses to Echo Requests" on page 36
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.	"Set Strict Multihoming" on page 37
Prevent DOS attacks by controlling the number of incomplete system connections.	Limits the allowable number of incomplete TCP connections for a TCP listener.	"Set Maximum Number of Incomplete TCP Connections" on page 37

Task	Description	For Instructions
Prevent DOS attacks by controlling the number of permitted incoming connections.	Specifies the default maximum number of pending TCP connections for a TCP listener.	"Set Maximum Number of Pending TCP Connections" on page 38
Generate strong random numbers for initial TCP connections.	Complies with the sequence number generation value specified by RFC 1948.	"Specify a Strong Random Number for Initial TCP Connection" on page 38
Return network parameters to their secure default values.	Increases security that was reduced by administrative actions.	"Reset Network Parameters to Secure Values" on page 38
Add TCP wrappers to network services to limit applications to legitimate users.	Specifies systems that are allowed access to network services, such as FTP. By default, the `sendmail` application is protected with TCP wrappers, as described in "Support for TCP Wrappers From Version 8.12 of sendmail" in *Oracle Solaris Administration: Network Services*.	To enable TCP wrappers for all `inetd` services, see "How to Use TCP Wrappers to Control Access to TCP Services" in *Oracle Solaris Administration: IP Services*. For an example of TCP wrappers protecting the FTP network service, see "How to Start an FTP Server Using SMF" in *Oracle Solaris Administration: Network Services*.

▼ Display Security Message to ssh and ftp Users

Use this procedure to display warnings at remote login and file transfer.

Before You Begin You must be in the `root` role. You created the `/etc/issue` file in Step 1 of "Place Security Message in Banner Files" on page 24.

1 **To display a security message to users who are logging in by using `ssh`, do the following:**

a. **Uncomment the Banner directive in the `/etc/sshd_config` file.**

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

b. **Refresh the `ssh` service.**

```
# svcadm refresh ssh
```

For more information, see the `issue`(4) and `sshd_config`(4) man pages.

2 **To display a security message to users who are logging in by using `ftp`, do the following:**

a. **Add the `DisplayConnect` directive to the `proftpd.conf` file.**

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

b. **Restart the `ftp` service.**

```
# svcadm restart ftp
```

For more information, see the ProFTPD (`http://www.proftpd.org/`) web site.

▼ Disable the Network Routing Daemon

Use this procedure to prevent network routing after installation by specifying a default router. Otherwise, perform this procedure after configuring routing manually.

Note – Many network configuration procedures require that the routing daemon be disabled. Therefore, you might have disabled this daemon as part of a larger configuration procedure.

Before You Begin You must be assigned the Network Management rights profile.

1 **Verify that the routing daemon is running.**

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

If the service is not running, you can stop here.

2 **Disable the routing daemon.**

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

3 **Verify that the routing daemon is disabled.**

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

See Also `routeadm`(1M) man page

▼ Disable Broadcast Packet Forwarding

By default, Oracle Solaris forwards broadcast packets. If your site security policy requires you to reduce the possibility of broadcast flooding, change the default by using this procedure.

Note – When you disable the `_forward_directed_broadcasts` network property, you are disabling broadcast pings.

Before You Begin You must be assigned the Network Management rights profile.

1. **Set the broadcast packet forwarding property to 0 for IP packets.**

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

2. **Verify the current value.**

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

See Also `ipadm`(1M) man page

▼ Disable Responses to Echo Requests

Use this procedure to prevent the dissemination of information about the network topology.

Before You Begin You must be assigned the Network Management rights profile.

1. **Set the response to broadcast echo requests property to 0 for IP packets, then verify the current value.**

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

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

2. **Set the response to multicast echo requests property to 0 for IP packets, then verify the current value.**

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

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

See Also For more information, see "_respond_to_echo_broadcast and _respond_to_echo_multicast (ipv4 or ipv6)" in *Oracle Solaris Tunable Parameters Reference Manual* and the `ipadm`(1M) man page.

▼ Set Strict Multihoming

For systems that are gateways to other domains, such as a firewall or a VPN node, use this procedure to turn on strict multihoming.

The Oracle Solaris 11 release introduces a new property, `hostmodel`, for IPv4 and IPv6. This property controls the send and receive behavior for IP packets on a multihomed system.

Before You Begin You must be assigned the Network Management rights profile.

1 **Set the `hostmodel` property to `strong` for IP packets.**

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

2 **Verify the current value and note the possible values.**

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

See Also For more information, see "hostmodel (ipv4 or ipv6)" in *Oracle Solaris Tunable Parameters Reference Manual* and the ipadm(1M) man page.

For more information about the use of strict multihoming, see "How to Protect a VPN With IPsec in Tunnel Mode" in *Oracle Solaris Administration: IP Services*.

▼ Set Maximum Number of Incomplete TCP Connections

Use this procedure to prevent denial of service (DOS) attacks by controlling the number of pending connections that are incomplete.

Before You Begin You must be assigned the Network Management rights profile.

1 **Set the maximum number of incoming connections.**

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

2 **Verify the current value.**

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

See Also For more information, see "_conn_req_max_q0" in *Oracle Solaris Tunable Parameters Reference Manual* and the ipadm(1M) man page.

▼ Set Maximum Number of Pending TCP Connections

Use this procedure to prevent DOS attacks by controlling the number of permitted incoming connections.

Before You Begin You must be assigned the Network Management rights profile.

1 **Set the maximum number of incoming connections.**

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

2 **Verify the current value.**

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

See Also For more information, see "_conn_req_max_q" in *Oracle Solaris Tunable Parameters Reference Manual* and the `ipadm(1M)` man page.

▼ Specify a Strong Random Number for Initial TCP Connection

This procedure sets the TCP initial sequence number generation parameter to comply with RFC 1948 (`http://www.ietf.org/rfc/rfc1948.txt`).

Before You Begin You must be in the `root` role to modify a system file.

● **Change the default value for the `TCP_STRONG_ISS` variable.**

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

▼ Reset Network Parameters to Secure Values

Many network parameters that are secure by default are tunable, so they can be changed. If site conditions permit, return the following tunable parameters to their default values.

Before You Begin You must be assigned the Network Management rights profile. The current value of the parameter is less secure than the default value.

1 **Set the source packet forwarding property to 0 for IP packets, then verify the current value.**

The default value prevents DOS attacks from spoofed packets.

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

For more information, see "forwarding (ipv4 or ipv6)" in *Oracle Solaris Tunable Parameters Reference Manual*.

2 **Set the netmask response property to 0 for IP packets, then verify the current value.**

The default value prevents the dissemination of information about the network topology.

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

3 **Set the timestamp response property to 0 for IP packets, then verify the current value.**

The default value removes additional CPU demands on systems and prevents the dissemination of information about the network.

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

4 **Set the broadcast timestamp response property to 0 for IP packets, then verify the current value.**

The default value removes additional CPU demands on systems and prevents dissemination of information about the network.

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

5 **Set the ignore redirects property to 0 for IP packets, then verify the current value.**

The default value prevents additional CPU demands on systems.

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

6 **Prevent IP source routing.**

If you need IP source routing for diagnostic purposes, do not disable this network parameter.

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

For more information, see "_rev_src_routes" in *Oracle Solaris Tunable Parameters Reference Manual*.

7 **Set the ignore redirects property to 0 for IP packets, then verify the current value.**

The default value prevents additional CPU demands on systems. Redirects are typically not necessary on a well-designed network.

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

See Also `ipadm(1M)` man page

Protecting File Systems and Files

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

The following tasks provide a glimpse of the protections that are available in ZFS, the default file system of Oracle Solaris. For additional information, see "Setting ZFS Quotas and Reservations" in *Oracle Solaris Administration: ZFS File Systems* and the `zfs(1M)` man page.

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 *Oracle Solaris Administration: ZFS File Systems*
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 *Oracle Solaris Administration: ZFS File Systems*
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 *Oracle Solaris Administration: ZFS File Systems* "Examples of Encrypting ZFS File Systems" in *Oracle Solaris Administration: ZFS File Systems*

Task	Description	For Instructions
Specify ACLs to protect files at a finer granularity than regular UNIX file permissions.	Extended security attributes can be useful in protecting files. For a caution about using ACLs, see Hiding Within the Trees (`http://www.usenix.org/publications/login/2004-02/pdfs/brunette.pdf`).	ZFS End-to-End Data Integrity (`http://blogs.oracle.com/bonwick/entry/zfs_end_to_end_data`)

Protecting and Modifying Files

Only the `root` role can modify system files.

Task	Description	For Instructions
Configure restrictive file permissions for regular users.	Sets a more restrictive value than `022` for file permissions for regular users.	"Set More Restrictive `umask` Value for Regular Users" on page 30
Prevent the replacement of system files with rogue files.	Finds rogue files through a script or by using BART.	"How to Find Files With Special File Permissions" in *Oracle Solaris Administration: Security Services*

Securing Applications and Services

You can configure Oracle Solaris security features to protect your applications.

Creating Zones to Contain Critical Applications

Zones are containers that isolate processes. They are useful containers for applications and parts of applications. For example, zones can be used to separate a web site's database from the site's web server.

For information and procedures see the following:

- Chapter 15, "Introduction to Oracle Solaris Zones," in *Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management*
- "Summary of Zones by Function" in *Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management*
- "Capabilities Provided by Non-Global Zones" in *Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management*
- "Setting Up Zones on Your System (Task Map)" in *Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management*.

- Chapter 16, "Non-Global Zone Configuration (Overview)," in *Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management*.
- *Hardening Oracle Database with Oracle Solaris Security Technologies* (`http://www.oracle.com/technetwork/server-storage/solaris/solaris-security-hardening-db-167784.pdf`)

Managing Resources in Zones

Zones provide a number of tools to manage zone resources.

For information and procedures see the following:

- Chapter 14, "Resource Management Configuration Example," in *Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management*
- Part I, "Oracle Solaris Resource Management," in *Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management*

Configuring IPsec and IKE

IPsec and IKE protect network transmissions between nodes and networks that are jointly configured with IPsec and IKE.

For information and procedures see the following:

- Chapter 14, "IP Security Architecture (Overview)," in *Oracle Solaris Administration: IP Services*
- Chapter 17, "Internet Key Exchange (Overview)," in *Oracle Solaris Administration: IP Services*
- Chapter 15, "Configuring IPsec (Tasks)," in *Oracle Solaris Administration: IP Services*
- Chapter 18, "Configuring IKE (Tasks)," in *Oracle Solaris Administration: IP Services*

Configuring IP Filter

The IP Filter feature provides a firewall.

For information and procedures see the following:

- Chapter 20, "IP Filter in Oracle Solaris (Overview)," in *Oracle Solaris Administration: IP Services*
- Chapter 21, "IP Filter (Tasks)," in *Oracle Solaris Administration: IP Services*

Configuring Kerberos

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

For information and procedures see the following:

- Chapter 20, "Planning for the Kerberos Service," in *Oracle Solaris Administration: Security Services*
- Chapter 21, "Configuring the Kerberos Service (Tasks)," in *Oracle Solaris Administration: Security Services*
- Selected man pages include `kadmin`(1M), `pam_krb5`(5), and `kclient`(1M).

Adding SMF to a Legacy Service

You can limit application configuration to trusted users or roles by adding the application to the Service Management Facility (SMF) feature of Oracle Solaris.

For information and procedures see the following:

- "How to Add RBAC Properties to Legacy Applications" in *Oracle Solaris Administration: Security Services*
- Securing MySQL using SMF - the Ultimate Manifest (`http://blogs.oracle.com/bobn/entry/securing_mysql_using_smf_the`).
- Selected man pages include `smf`(5), `smf_security`(5), `svcadm`(1M), and `svccfg`(1M).

Creating a BART Snapshot of the System

After configuring the system, you can create one or more BART manifests. These manifests provide snapshots of the system. Then, you can schedule regular snapshots and comparisons. For more information, see "Using the Basic Audit Reporting Tool" on page 45.

Adding Multilevel (Labeled) Security

Trusted Extensions extends Oracle Solaris security by enforcing a 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 `group/feature/trusted-desktop` packages provide the Oracle Solaris multilevel, trusted desktop environment.

Configuring Trusted Extensions

You must install the Trusted Extensions packages, then configure the system. After package installation, 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 I, "Initial Configuration of Trusted Extensions," in *Trusted Extensions Configuration and Administration*
- Part II, "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 14, "IP Security Architecture (Overview)," in *Oracle Solaris Administration: IP Services*
- "Administration of Labeled IPsec" in *Trusted Extensions Configuration and Administration*
- "Configuring Labeled IPsec (Task Map)" in *Trusted Extensions Configuration and Administration*

CHAPTER 3

Monitoring and Maintaining Oracle Solaris 11 Security

Oracle Solaris provides two system tools to monitor security, the Basic Audit Reporting Tool (BART) feature and the audit service. Individual programs and applications can also create access and usage logs.

- "Using the Basic Audit Reporting Tool" on page 45
- "Using the Audit Service" on page 46
- "Finding Rogue Files" on page 47

Using the Basic Audit Reporting Tool

BART manifests provide a static record of what is installed on your system. Over time and across systems, BART manifests can be compared to track changes to installed systems and differences between systems.

For information and procedures, see the following:

- "BART (Overview)" in *Oracle Solaris Administration: Security Services*
- "Using BART (Tasks)" in *Oracle Solaris Administration: Security Services*
- "BART Manifests, Rules Files, and Reports (Reference)" in *Oracle Solaris Administration: Security Services*

For specific instructions on tracking changes to installed systems, see "How to Compare Manifests for the Same System Over Time" in *Oracle Solaris Administration: Security Services*.

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 Part VII, "Auditing in Oracle Solaris," in *Oracle Solaris Administration: Security Services*.

- Chapter 26, "Auditing (Overview)," in *Oracle Solaris Administration: Security Services*
- Chapter 27, "Planning for Auditing," in *Oracle Solaris Administration: Security Services*
- Chapter 28, "Managing Auditing (Tasks)," in *Oracle Solaris Administration: Security Services*
- Chapter 29, "Auditing (Reference)," in *Oracle Solaris Administration: Security Services*

  For a list of the man pages and links to them, see "Audit Service Man Pages" in *Oracle Solaris Administration: Security Services*.

To satisfy your site requirements, the following audit service procedures might be useful:

- Create separate roles to configure auditing, review auditing, and start and stop the audit service.

  Use the Audit Configuration, Audit Review, and Audit Control rights profiles as the basis for your roles.

  To create a role, see "How to Create a Role" in *Oracle Solaris Administration: Security Services*.
- Monitor text summaries of audited events in the `syslog` utility

  Activate the `audit_syslog` plugin, then monitor the reported events.

  See "How to Configure syslog Audit Logs" in *Oracle Solaris Administration: Security Services*.
- 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 *Oracle Solaris Administration: Security Services*.
- 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_syslog Audit Summaries

The `audit_syslog` plugin enables you to record summaries of preselected audit events.

You can display the audit summaries in a terminal window as they are generated by running a command similar to the following:

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

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 *Oracle Solaris Administration: Security Services*
- "How to Prevent Audit Trail Overflow" in *Oracle Solaris Administration: Security Services*
- "Managing Audit Records on Local Systems (Tasks)" in *Oracle Solaris Administration: Security Services*

Finding Rogue Files

You can locate the potentially unauthorized use of the setuid and setgid permissions on programs. A suspicious executable file grants ownership to a user rather than to a system account, such as root or bin.

For the procedure and an example, see "How to Find Files With Special File Permissions" in *Oracle Solaris Administration: Security Services*.

APPENDIX A

Bibliography for Oracle Solaris Security

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

Oracle Solaris 11 References

The following book and articles contain descriptions of security on Oracle Solaris 11 systems:

- *Oracle Solaris Administration: Security Services*

  This security guide is published by Oracle for Oracle Solaris 11 administrators. This guide describes the security features of Oracle Solaris and how to use them when configuring your systems. The preface contains links to other Oracle Solaris system administration guides that can contain security information.

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

  This article provides a snapshot of Oracle Solaris security features for the November 2010 version of this release.

- ORACLE SOLARIS 11 EXPRESS 2010.11 (`http://www.oracle.com/technetwork/server-storage/solaris11/documentation/solaris-express-whatsnew-201011-175308.pdf`)

  This article provides a snapshot of Oracle Solaris features for the November 2010 version of this release.

For Oracle Solaris 10 references that might be useful, see *Oracle Solaris 10 Security Guidelines*.