Oracle® Solaris 11 – Sicherheitsbestimmungen

Teilenr.: E25814–03
März 2012

ORACLE

120424@25097

Inhalt

Vorwort

Dieses Handbuch enthält Sicherheitsrichtlinien für das Betriebssystem Betriebssystem Oracle Solaris (Oracle Solaris). Zunächst werden Sicherheitsprobleme beschrieben, die durch Unternehmensbetriebssysteme bewältigt werden müssen. Dann folgt eine Beschreibung der Standardsicherheitsfunktionen von Oracle Solaris. Schließlich werden bestimmte Schritte zur Erhöhung der Systemsicherheit sowie zur Verwendung der Oracle Solaris-Sicherheitsfunktionen aufgezeigt, mit denen Daten und Anwendungen geschützt werden sollen. Die Angaben sind als Empfehlungen zu verstehen, die an die Sicherheitsrichtlinien des jeweiligen Standorts angepasst werden können.

Zielgruppe

Oracle Solaris 11 – Sicherheitsbestimmungen richtet sich an Sicherheitsadministratoren sowie an Administratoren mit folgenden Aufgaben:

- Analysieren der Sicherheitsanforderungen
- Implementieren von Sicherheitsrichtlinien in Software
- Installieren und Konfigurieren von Oracle Solaris
- Verwalten der System- und Netzwerksicherheit

Für dieses Handbuch werden allgemeine Kenntnisse über die UNIX-Administration, ein gutes Grundlagenwissen über Softwaresicherheit und die Kenntnis der Standortsicherheitsrichtlinie vorausgesetzt.

Kontakt zum Oracle Support

Oracle-Kunden können über My Oracle Support den Onlinesupport nutzen. Informationen dazu erhalten Sie unter `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` oder unter `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` (für Hörgeschädigte).

Typografische Konventionen

In der folgenden Tabelle sind die in diesem Handbuch verwendeten typografischen Konventionen aufgeführt.

TABELLE P–1 Typografische Konventionen

Schriftart	Beschreibung	Beispiel
`AaBbCc123`	Namen von Befehlen, Dateien, Verzeichnissen sowie Bildschirmausgaben	Bearbeiten Sie Ihre `.login`-Datei. Verwenden Sie `ls -a`, um eine Liste aller Dateien zu erhalten. `machine_name% Sie haben eine neue Nachricht.`
`AaBbCc123`	Von Ihnen eingegebene Zeichen (im Gegensatz zu auf dem Bildschirm angezeigten Zeichen)	`machine_name%` **`su`** `Passwort:`
aabbcc123	Platzhalter: durch einen tatsächlichen Namen oder Wert zu ersetzen	Der Befehl zum Entfernen einer Datei lautet `rm` *Dateiname*.
AaBbCc123	Buchtitel, neue Ausdrücke und Begriffe, die hervorgehoben werden sollen	Lesen Sie hierzu Kapitel 6 im *Benutzerhandbuch*. Ein *Cache* ist eine lokal gespeicherte Kopie. Diese Datei *nicht* speichern. **Hinweis:** Einige hervorgehobene Begriffe werden online fett dargestellt.

Shell-Eingabeaufforderungen in Befehlsbeispielen

Die folgende Tabelle zeigt die standardmäßige UNIX-Systemeingabeaufforderung und Superuser-Eingabeaufforderung für Shells, die zum Betriebssystem Oracle Solaris gehören. Beachten Sie, dass die in den Befehlsbeispielen angezeigte Standard-Systemeingabeaufforderung je nach Oracle Solaris-Version variiert.

TABELLE P–2 Shell-Eingabeaufforderungen

Shell	Eingabeaufforderung
Bash-Shell, Korn-Shell und Bourne-Shell	$
Bash-Shell, Korn-Shell und Bourne-Shell für Superuser	#

TABELLE P–2 Shell-Eingabeaufforderungen *(Fortsetzung)*

Shell	Eingabeaufforderung
C-Shell	`machine_name%`
C-Shell für Superuser	`machine_name#`

◆ ◆ ◆ KAPITEL 1

1 Übersicht über die Oracle Solaris 11-Sicherheitsfunktionen

Oracle Solaris 11 gehört zu den führenden Unternehmensbetriebssystemen, bietet Stabilität und bewährte Sicherheitsfunktionen. Mit einem komplexen, netzwerkübergreifenden Sicherheitssystem, das den Zugriff auf Dateien steuert, Systemdatenbanken schützt und die Nutzung von Systemressourcen überwacht, erfüllt Oracle Solaris 11 Sicherheitsanforderungen auf jeder Ebene. Während klassische Betriebssysteme systemeigene Sicherheitsschwächen aufweisen können, ist Oracle Solaris 11 dank seiner Flexibilität an die verschiedensten Sicherheitsanforderungen von Unternehmensservern bis zu Desktopclients anpassbar. Oracle Solaris 11 wurde in umfassender Weise getestet und wird unterstützt auf verschiedenen SPARC- und x86-basierten Systemen von Oracle sowie auf anderen Hardwareplattformen von Drittanbietern.

Oracle Solaris 11-Sicherheitsschutzmechanismen

Oracle Solaris bietet Stabilität für Unternehmensdaten und Anwendungen durch Schutz von gespeicherten und übertragenen Daten. Oracle Solaris Resource Manager (bezeichnet als *Ressourcenverwaltung*) und Oracle Solaris Zones verfügen über Funktionen zur Isolierung und zum Schutz vor falscher Verwendung von Anwendungen. Durch diese Schutzfunktionen, durch über Rechte implementierte geringste Berechtigungen sowie durch die RBAC-Funktion (Role-Based Access Control) von Oracle Solaris werden Sicherheitsrisiken durch unbefugte Zugriffsversuche oder Benutzeraktionen eingedämmt. Authentifizierte und verschlüsselte Protokolle wie IPsec (Internet Protocol Security) stellen VPNs (Virtual Private Network) über das Internet sowie Tunnel über LAN oder WAN für eine sichere Datenübertragung bereit. Außerdem wird durch die Oracle Solaris-Prüffunktion sichergestellt, dass alle relevanten Aktionen festgehalten werden.

Oracle Solaris 11-Sicherheitsservices bieten eine solide Gewährleistung der Sicherheit durch Schutzschichten für System und Netzwerk. Oracle Solaris bietet Kernel-Schutz, indem mithilfe von Kernel-Dienstprogrammen die privilegierten Aktionen begrenzt werden, die das Dienstprogramm durchführen kann. Die Standardkonfiguration des Netzwerks bietet system- und netzwerkweiten Datenschutz. Zusätzlichen Schutz stellen die IP Filter-Funktion von Oracle Solaris IPsec und Kerberos bereit.

Oracle Solaris-Sicherheitsservices haben folgende Aufgaben:

- Kernel-Schutz – Kernel-Dämonen und -Geräte erhalten Schutz durch Dateiberechtigungen.
- Anmeldeschutz – Für die Anmeldung wird ein Passwort benötigt. Passwörter werden sicher verschlüsselt. Remote-Anmeldungen erfolgen zunächst nur über einen verschlüsselten und authentifizierten Kanal der Secure Shell-Funktion von Oracle Solaris. Es ist nicht möglich, sich direkt über das `root`-Konto anzumelden.
- Datenschutz – Auf Festplatten gespeicherte Daten werden durch Dateiberechtigungen geschützt. Es können weitere Schutzschichten konfiguriert werden. Beispiel: Sie können Zugriffskontrolllisten (ACL, Access Control List) erstellen, Daten in einer Zone ablegen, eine Datei verschlüsseln, einen Oracle Solaris ZFS-Datensatz verschlüsseln, einen schreibgeschützten ZFS-Datensatz erstellen und Dateisysteme einhängen, sodass `setuid`-Programme und ausführbare Dateien nicht ausgeführt werden können.

Oracle Solaris 11-Sicherheitstechnologien

Die Sicherheitsfunktionen von Oracle Solaris können so konfiguriert werden, dass Ihre Standortsicherheitsrichtlinie implementiert werden kann.

Auf den folgenden Seiten werden die Oracle Solaris-Sicherheitsfunktionen kurz vorgestellt. Die Beschreibungen enthalten Verweise auf ausführlichere Informationen und Anweisungen in diesem Handbuch sowie auf andere Oracle Solaris-Systemadministrationshandbücher, die diese Funktionen veranschaulichen.

Prüfservice

Bei der Prüfung werden Daten über die Nutzung der Systemressourcen erfasst. Die Prüfdaten stellen ein Protokoll zu sicherheitsbezogenen Systemereignissen bereit. Anhand dieser Daten können Sie anschließend die Verantwortlichkeit für die auf einem System ausgeführten Aktionen zuweisen.

Prüfungen sind eine Grundanforderung bei Sicherheitsevaluierungen, Validierungen und Zertifizierungsstellen. Sie können zudem eine abschreckende Wirkung auf potenzielle Eindringlinge haben.

Weitere Informationen finden Sie hier:

- Eine Liste von Manpages zu Prüfungen erhalten Sie in Kapitel 29, „Auditing (Reference)“ in *Oracle Solaris Administration: Security Services*.
- Richtlinien finden Sie unter „Prüfen wichtiger Ereignisse außer Anmelden/Abmelden“ auf Seite 36 und auf den Manpages.
- Eine Übersicht über das Prüfungsverfahren finden Sie in Kapitel 26, „Auditing (Overview)“ in *Oracle Solaris Administration: Security Services*.
- Prüfaufgaben finden Sie in Kapitel 28, „Managing Auditing (Tasks)“ in *Oracle Solaris Administration: Security Services*.

Basic Audit Reporting Tool

Die BART-Funktion (Basic Audit Reporting Tool) von Oracle Solaris ermöglicht eine umfassende Validierung von Systemen, indem über einen längeren Zeitraum hinweg Überprüfungen auf Dateiebene in einem System durchgeführt werden. Sie können durch die Erstellung von BART-Manifesten auf einfache, zuverlässige Weise Informationen über die Komponenten des Software-Stacks sammeln, der auf dem verteilten System installiert ist.

BART ist ein nützliches Tool für das Integritätsmanagement in einem System oder Systemnetzwerk.

Weitere Informationen finden Sie hier:

- Manpages `bart(1M)`, `bart_rules(4)` und `bart_manifest(4)`
- Richtlinien finden Sie unter „Erstellen eines BART-Schnappschusses des Systems“ auf Seite 50, „Basic Audit Reporting Tool – Verwendung“ auf Seite 53, und auf den Manpages.
- Eine Übersicht über BART finden Sie in Kapitel 6, „Verifying File Integrity by Using BART“ in *Oracle Solaris Administration: Security Services*.
- Anwendungsbeispiele zu BART finden Sie unter „Using BART (Tasks)“ in *Oracle Solaris Administration: Security Services* und auf den Manpages.

Kryptografische Services

Die Cryptographic Framework-Funktion und die KMF-Funktion (Key Management Framework) von Oracle Solaris bieten zentrale Repositorys für kryptografische Services und Schlüsselverwaltung. Hardware, Software und Endbenutzer können auf optimierte Algorithmen mühelos zugreifen. Durch die Übernahme der KMF-Schnittstellen werden die Schnittstellen der verschiedenen Speichersysteme, administrativen Dienstprogramme und Programmierungsschnittstellen für unterschiedliche PKIs (Public Key Infrastructure) vereinheitlicht.

Das Cryptographic Framework bietet Benutzern über einzelne Befehle kryptografische Services und Anwendungen, eine Programmierungsschnittstelle auf Benutzerebene, eine Schnittstelle für die Kernel-Programmierung sowie Frameworks auf Benutzer- und Kernel-Ebene. Das Cryptographic Framework stellt diese kryptografischen Services Anwendungen und Kernel-Modulen in aus Endbenutzersicht nahtlosen Weise bereit. Außerdem kann der Endbenutzer direkte kryptografische Services wie Ver- und Entschlüsselung für Dateien nutzen.

KMF bietet Tools und Programmierungsschnittstellen für die zentrale Verwaltung von Public Key-Objekten wie X.509-Zertifikaten und Public/Private Key-Paaren. Die Formate für die Speicherung dieser Objekte können variieren. KMF bietet darüber hinaus ein Tool für die Verwaltung von Richtlinien, die die Verwendung von X.509-Zertifikaten durch Anwendungen bestimmen. KMF unterstützt Plug-ins von Drittanbietern.

Weitere Informationen finden Sie hier:

- Manpages `cryptoadm(1M)`, `encrypt(1)`, `mac(1)`, `pktool(1)` und `kmfcfg(1)`
- Eine Übersicht über kryptografische Services erhalten Sie in Kapitel 11, „Cryptographic Framework (Overview)“ in *Oracle Solaris Administration: Security Services* und Kapitel 13, „Key Management Framework“ in *Oracle Solaris Administration: Security Services*.
- Anwendungsbeispiele zum Cryptographic Framework finden Sie in Kapitel 12, „Cryptographic Framework (Tasks)“ in *Oracle Solaris Administration: Security Services* und auf den Manpages.

Dateiberechtigungen und Zugriffskontrolleinträge

Objekte in einem Dateisystem sind in erster Linie durch die UNIX-Berechtigungen geschützt, die jedem Dateisystemobjekt zugewiesen sind. UNIX-Berechtigungen unterstützen u. a. eindeutige Zugriffsrechte für den Eigentümer des Objekts und für eine dem Objekt zugewiesene Gruppe. Außerdem unterstützt ZFS ACLs, die auch als ACEs (Access Control Entries) bezeichnet werden und eine feiner abgestimmte Kontrolle des Zugriffs auf einzelne Dateisystemobjekte oder Dateisystemobjektgruppen bieten.

Weitere Informationen finden Sie hier:

- Anweisungen zum Festlegen von ACLs bei ZFS-Dateien finden Sie auf der Manpage `chmod(1)`.
- Eine Übersicht über Dateiberechtigungen erhalten Sie in „Using UNIX Permissions to Protect Files“ in *Oracle Solaris Administration: Security Services*.
- Eine Übersicht und Beispiele für den Schutz von ZFS-Dateien finden Sie in Kapitel 8, „Using ACLs and Attributes to Protect Oracle Solaris ZFS Files“ in *Oracle Solaris Administration: ZFS File Systems* und auf den Manpages.

Paketfilterung

Die Paketfilterung bietet allgemeinen Schutz vor netzwerkbasierten Angriffen. Oracle Solaris umfasst die IP Filter-Funktion und TCP-Wrapper.

IP Filter

Die IP Filter-Funktion von Oracle Solaris erstellt eine Firewall, um netzwerkbasierte Angriffe abzuwenden.

IP Filter bietet insbesondere eine statusbehaftete Paketfilterung und kann Pakete nach IP-Adresse, Netzwerk, Port, Protokoll, Netzwerkschnittstelle und Netzverkehrsrichtung filtern. Darüber hinaus bietet sie eine statusfreie Paketfilterung sowie die Möglichkeit, Adresspools zu erstellen und zu verwalten. Mit IP Filter können außerdem Network Address Translation (NAT) und Port Address Translation (PAT) durchgeführt werden.

Weitere Informationen finden Sie hier:

- Manpages `ipfilter(5)`, `ipf(1M)`, `ipnat(1M)`, `svc.ipfd(1M)` und `ipf(4)`
- Eine IP Filter-Übersicht finden Sie in Kapitel 20, „IP Filter in Oracle Solaris (Overview)“ in *Oracle Solaris Administration: IP Services*.
- Anwendungsbeispiele zu IP Filter finden Sie in Kapitel 21, „IP Filter (Tasks)“ in *Oracle Solaris Administration: IP Services* sowie auf den Manpages.
- Informationen zu und Syntaxbeispiele für die IP Filter-Richtliniensprache erhalten Sie auf der Manpage `ipnat(4)`.

TCP-Wrapper

TCP-Wrapper dienen zur Implementierung der Zugriffskontrollen; dazu wird die Adresse eines Hosts, der einen bestimmten Netzwerkdienst anfordert, anhand einer Zugriffskontrollliste geprüft. Anforderungen werden dann entsprechend genehmigt oder verweigert. TCP-Wrapper bieten zudem eine hilfreiche Überwachungsfunktion, denn sie protokollieren Hostanforderungen für Netzwerkdienste. Die Secure Shell- und `sendmail`-Funktionen von Oracle Solaris sind für die Verwendung von TCP-Wrappern konfiguriert. Zu den Netzwerkdiensten, die mit einer Zugriffskontrolle belegt werden können, gehören `ftpd` und `rpcbind`.

TCP-Wrapper unterstützen eine erweiterte Richtliniensprache, mit der Organisationen Sicherheitsrichtlinien nicht nur global, sondern auch pro Service definieren können. Ein umfassenderer Zugriff auf Services kann basierend auf dem Hostnamen, der IPv4- oder IPv6-Adresse, dem Netzgruppennamen, dem Netzwerk und sogar der DNS-Domain zugelassen oder eingeschränkt werden.

Weitere Informationen finden Sie hier:

- Informationen zu TCP-Wrappern erhalten Sie in „How to Use TCP Wrappers to Control Access to TCP Services“ in *Oracle Solaris Administration: IP Services*.
- Informationen und Syntaxbeispiele für die Zugriffskontrollsprache für TCP-Wrapper finden Sie auf der Manpage `hosts_access`(4).

Passwörter und Passwortbeschränkungen

Sichere Passwörter bieten Schutz vor Brute Force-Zugriffsversuchen.

Oracle Solaris unterstützt die Passwortsicherheit mit einer Reihe von entsprechenden Funktionen. Die Passwortlänge, die verwendeten Zeichen, die Häufigkeit der Passwortänderung sowie Änderungsanforderungen können festgelegt und eine Passwortabfolge angelegt werden. Außerdem ist ein Passwortwörterbuch mit ungeeigneten Passwörtern vorhanden. Ferner sind mehrere Passwortalgorithmen verfügbar.

Weitere Informationen finden Sie hier:

- „Maintaining Login Control“ in *Oracle Solaris Administration: Security Services*
- „Securing Logins and Passwords (Tasks)“ in *Oracle Solaris Administration: Security Services*
- Manpages `passwd`(1) und `crypt.conf`(4)

Pluggable Authentication Module

Mit dem PAM-Framework (Pluggable Authentication Module) können Sie Anforderungen für die Benutzerauthentifizierung für Konten, Berechtigungsnachweise, Sitzungen und Passwörter koordinieren und konfigurieren.

Organisationen können mit dem PAM-Framework die Benutzerauthentifizierungserfahrung sowie Konten-, Sitzungs- und Passwortverwaltungsfunktionen anpassen. Systemeintragsservices wie `login` und `ftp` nutzen das PAM-Framework, um sicherzustellen, dass alle Einstiegspunkte für das System gesichert sind. Diese Architektur ermöglicht das Ersetzen oder Ändern von Authentifizierungsmodulen im Feld, sodass das System vor neuen bekannten Sicherheitsrisiken geschützt ist, ohne dass Änderungen an Systemservices, die das PAM-Framework nutzen, erforderlich sind.

Weitere Informationen finden Sie hier:

- Kapitel 14, „Using PAM“ in *Oracle Solaris Administration: Security Services*
- Manpage `pam.conf`(4)

Berechtigungen in Oracle Solaris

Berechtigungen sind fein abgestimmte, einzelne Rechte für Prozesse, welche im Kernel durchgesetzt werden. Oracle Solaris definiert über 80 Berechtigungen wie `file_read` oder Berechtigungen für einen bestimmten Zweck wie `proc_clock_highres`. Berechtigungen können einem Befehl, einem Benutzer, einer Rolle oder einem System gewährt werden. Viele Oracle Solaris-Befehle und -Dämonen werden nur mit den Berechtigungen ausgeführt, die für die Aufgabe erforderlich sind. Die Verwendung von Berechtigungen wird auch als *Prozessberechtigungsverwaltung* bezeichnet.

Berechtigungen erkennende Programme können verhindern, dass Eindringlinge mehr Berechtigungen als das Programm selbst erlangen können. Außerdem können Organisationen mithilfe von Berechtigungen bestimmen, welche Berechtigungen den auf ihren Systemen ausgeführten Services und Prozessen gewährt werden.

Weitere Informationen finden Sie hier:

- „Privileges (Overview)“ in *Oracle Solaris Administration: Security Services*
- „Using Privileges (Tasks)“ in *Oracle Solaris Administration: Security Services*
- Kapitel 2, „Developing Privileged Applications“ in *Developer's Guide to Oracle Solaris 11 Security*
- Manpages `ppriv(1)` und `privileges(5)`

Remote-Zugriff

Angriffe über Remote-Zugriff können Systemen und Netzwerken Schaden zufügen. Für die heutigen Internetumgebungen und sogar für WAN- und LAN-Umgebungen ist ein Zugriffschutz für Netzwerke erforderlich.

IPsec und IKE

Internet Protocol Security (IPsec) bietet Schutz für IP-Pakete durch die Authentifizierung und/oder Verschlüsselung der Pakete. Oracle Solaris unterstützt IPsec sowohl für IPv4 als auch IPv6. Da IPsec unterhalb der Anwendungsschicht implementiert ist, können Internetanwendungen IPsec ohne Änderungen an deren Code nutzen.

IPsec und sein Key Exchange-Protokoll IKE verwenden Cryptographic Framework-Algorithmen. Darüber hinaus stellt das Cryptographic Framework stellt einen Softtoken-Schlüsselspeicher für Anwendungen zur Verfügung, die den Metaslot nutzen. Wenn IKE so konfiguriert ist, dass es den Metaslot verwendet, können Organisationen die Schlüssel auf einer Festplatte, einem angeschlossenen Schlüsselspeichergerät oder im Softtoken-Schlüsselspeicher speichern.

Wenn es richtig vewaltet wird, ist IPsec ein wirksames Tool bei der Sicherung des Netzwerkverkehrs.

Weitere Informationen finden Sie hier:

- Kapitel 14, „IP Security Architecture (Overview)“ in *Oracle Solaris Administration: IP Services*
- Kapitel 15, „Configuring IPsec (Tasks)“ in *Oracle Solaris Administration: IP Services*
- Kapitel 17, „Internet Key Exchange (Overview)“ in *Oracle Solaris Administration: IP Services*
- Kapitel 18, „Configuring IKE (Tasks)“ in *Oracle Solaris Administration: IP Services*
- Manpages `ipsecconf`(1M) und `in.iked`(1M)

Secure Shell

Mit der Secure Shell-Funktion von Oracle Solaris können Benutzer oder Services zwischen Remote-Systemen über einen verschlüsselten Kommunikationskanal auf Dateien zugreifen oder sie übertragen. Der gesamte Netzwerkverkehr ist bei Secure Shell verschlüsselt. Secure Shell kann zudem als bedarforientiertes VPN eingesetzt werden, das X Window-Systemverkehr weiterleiten oder sich über eine authentifizierte und verschlüsselte Netzwerkverbindung zwischen einem lokalen System und Remote-Systemen mit einzelnen Portnummern verbinden kann.

So wird durch Secure Shell das Lesen abgefangener Mitteilungen durch potenzielle Eindringlinge und Spoofing-Angriffe unterbunden. Auf neu installierten Systemen kann nur Secure Shell für den Remote-Zugriff verwendet werden.

Weitere Informationen finden Sie hier:

- Kapitel 15, „Using Secure Shell“ in *Oracle Solaris Administration: Security Services*
- Manpages `ssh`(1), `sshd`(1M), `sshd_config`(4) und `ssh_config`(4)

Kerberos-Service

Die Kerberos-Funktion von Oracle Solaris ermöglicht Single Sign-On und sichere Übertragungen, auch über heterogene Netzwerke, wenn sie Kerberos ausführen.

Kerberos basiert auf dem Kerberos V5-Netzwerkauthentifizierungsprotokoll, das am MIT (Massachusetts Institute of Technology) entwickelt wurde. Der Kerberos-Service ist eine Client-Server-Architektur für sichere Netzwerktransaktionen. Der Service bietet Authentifizierung über sichere Passwörter, Integrität und Vertraulichkeit. Mit dem Kerberos-Service können Sie nach einmaliger Anmeldung sicher auf andere Rechner zugreifen, Befehle ausführen, Daten austauschen und Dateien übertragen. Darüber hinaus können Administratoren mithilfe des Service den Zugriff auf Services und Systeme einschränken.

Weitere Informationen finden Sie hier:

- Teil VI, „Kerberos Service“ in *Oracle Solaris Administration: Security Services*
- Manpages `kerberos`(5) und `kinit`(1)

Role-Based Access Control

RBAC (Role-Based Access Control) wendet das Sicherheitsprinzip der geringsten Berechtigungen an, indem es Organisationen ermöglicht, administrative Rechte bestimmten Benutzern oder Rollen entsprechend ihrer Anforderungen zu gewähren.

Die RBAC-Funktion von Oracle Solaris steuert den Benutzerzugriff auf Aufgaben, die normalerweise der `root`-Rolle vorbehalten sind. Durch das Anwenden von Sicherheitsattributen auf Prozesse und Benutzer kann RBAC administrative Rechte auf mehrere Administratoren aufteilen. Bei RBAC spricht man auch von *Verwaltung von Benutzerrechten*.

Weitere Informationen finden Sie hier:

- Teil III, „Roles, Rights Profiles, and Privileges“ in *Oracle Solaris Administration: Security Services*
- Manpages `rbac(5)`, `roleadd(1M)`, `profiles(1)` und `user_attr(4)`

Service Management Facility

Mithilfe der SMF-Funktion (Service Management Facility) von Oracle Solaris werden Services hinzugefügt, entfernt, konfiguriert und verwaltet. SMF nutzt RBAC für die Zugriffskontrolle bei systemeigenen Serviceverwaltungsfunktionen. Insbesondere nutzt SMF Autorisierungen, um zu festzustellen, welche Personen einen Service verwalten und welche Aufgaben sie durchführen können.

SMF ermöglicht Organisationen die Kontrolle über den Zugriff auf Services sowie über die Art und Weise, wie diese gestartet, gestoppt und aktualisiert werden.

Weitere Informationen finden Sie hier:

- Kapitel 6, „Managing Services (Overview)“ in *Oracle Solaris Administration: Common Tasks*
- Kapitel 7, „Managing Services (Tasks)“ in *Oracle Solaris Administration: Common Tasks*
- Manpages `svcadm(1M)`, `svcs(1)` und `smf(5)`

ZFS-Dateisystem von Oracle Solaris

ZFS ist das Standarddateisystem für Oracle Solaris 11. Das ZFS-Dateisystem ändert die Art der Verwaltung von Dateisystemen unter Oracle Solaris grundlegend. ZFS ist stabil, skalierbar und einfach zu verwalten. Da die ZFS-Dateisystemerstellung unkompliziert ist, können Sie auf einfache Weise Kontingente und Speicherplatzreservierungen erstellen. UNIX-Berechtigungen und ACE bieten Schutz für Dateien, außerdem unterstützt RBAC die delegierte Administration von ZFS-Datensätzen.

Weitere Informationen finden Sie hier:

- Kapitel 1, „Oracle Solaris ZFS File System (Introduction)“ in *Oracle Solaris Administration: ZFS File Systems*
- Kapitel 3, „Oracle Solaris ZFS and Traditional File System Differences“ in *Oracle Solaris Administration: ZFS File Systems*
- Kapitel 6, „Managing Oracle Solaris ZFS File Systems“ in *Oracle Solaris Administration: ZFS File Systems*
- Manpages `zfs`(1M) und `zfs`(7FS)

Oracle Solaris Zones

Mit der Partitionierungstechnologie von Oracle Solaris Zones können Sie bei einem Bereitstellungsmodell, das eine Anwendung pro Server vorsieht, Hardwareressourcen gemeinsam mit anderen nutzen.

Bei Zonen handelt es sich um virtualisierte Betriebssystemumgebungen, in denen mehrere voneinander isolierte Anwendungen auf derselben physischen Hardware ausgeführt werden. Durch diese Isolation wird verhindert, dass ein Prozess, der innerhalb einer Zone ausgeführt wird, Prozesse in anderen Zonen überwacht oder beeinflusst, dass Daten des anderen Prozesses angezeigt werden oder die zugrunde liegende Hardware manipuliert wird. Zonen bieten zudem eine Abstraktionsschicht, die Anwendungen von physischen Systemattributen trennt, auf denen sie verteilt werden, zum Beispiel physische Gerätepfade und Netzwerkschnittstellennamen.

Weitere Informationen finden Sie hier:

- Teil II, „Oracle Solaris Zones“ in *Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management*
- Manpages `brands`(5), `zoneadm`(1M) und `zonecfg`(1M)

Trusted Extensions

Die Trusted Extensions-Funktion von Oracle Solaris ist eine optionale Sicherheitsschicht, mit der Richtlinien zur Datensicherheit von der Dateneigentümerschaft getrennt werden können. Trusted Extensions unterstützt sowohl klassische, auf Eigentümerschaft basierende DAC-Richtlinien (Discretionary Access Control) als auch bezeichnungsbasierte MAC-Richtlinien (Mandatory Access Control). Wenn die Trusted Extensions-Schicht nicht aktiviert ist, sind alle Bezeichnungen gleich, sodass der Kernel nicht so konfiguriert wird, um die MAC-Richtlinien durchzusetzen. Werden die bezeichnungsbasierten MAC-Richtlinien aktiviert, wird der Datenfluss auf Grundlage eines Bezeichnungsvergleichs im Zusammenhang mit den Prozessen (Subjekte), die Zugriff anfordern, und den Objekten, die die Daten

enthalten, eingeschränkt. Im Gegensatz zu den meisten anderen mehrstufigen Betriebssystemen verfügt Trusted Extensions über einen mehrstufigen Desktop.

Trusted Extensions erfüllt die Anforderungen der allgemeinen Kriterien von LSPP (Labeled Security Protection Profile), RBACPP (Role-Based Access Protection Profile) und CAPP (Controlled Access Protection Profile). Die Trusted Extensions-Implementierung bietet eine beispiellos hohe Zusicherung, erzielt ein Maximum an Kompatibilität und beschränkt den Aufwand auf ein Minimum.

Weitere Informationen finden Sie hier:

- Informationen zur Konfiguration und Verwaltung von Trusted Extensions erhalten Sie in *Trusted Extensions Configuration and Administration* .
- Informationen zur Nutzung des mehrstufigen Desktops erhalten Sie in *Trusted Extensions User's Guide* .
- Manpages `trusted_extensions(5)` und `labeld(1M)`

Oracle Solaris 11-Standardsicherheitseinstellungen

Nach der Installation schützt Oracle Solaris u. a. das System vor Angriffen und überwacht Anmeldeversuche.

Eingeschränkter und überwachter Systemzugriff

Der erste Benutzer und die `root` **-Rolle –** Eine Anmeldung ist mit dem Konto des ersten Benutzers über die Konsole möglich. Die `root`-Rolle wird diesem Konto zugewiesen. Die Passwörter für beide Konten sind zunächst identisch.

- Der erste Benutzer kann nach der Anmeldung die `root`-Rolle übernehmen, um das System weiter zu konfigurieren. Bei der Übernahme der Rolle wird der Benutzer aufgefordert, das `root`-Passwort zu ändern. Beachten Sie, dass eine Anmeldung direkt über eine Rolle nicht möglich ist, auch nicht über die `root`-Rolle.
- Dem ersten Benutzer werden Standardeinstellungen der Datei `/etc/security/policy.conf` zugewiesen. Zu den Standardeinstellungen gehören die Rechteprofile "Basic Solaris User" und "Console User". Mit diesen Rechteprofilen können Benutzer eine CD oder DVD lesen und darauf schreiben, im System Befehle ohne Berechtigungen ausführen und das System über die Konsole anhalten oder neu starten.
- Das Rechteprofil "System Administrator" ist dem Konto des ersten Benutzers ebenfalls zugewiesen. Daher verfügt der erste Benutzer über administrative Rechte für beispielsweise die Installation von Software und Verwaltung des Naming Service, ohne die `root`-Rolle übernehmen zu müssen.

Passwortanforderungen – Benutzerpasswörter müssen mindestens 6 Zeichen lang sein und mindestens einen Buchstaben und eine Zahl enthalten. Bei Passwörtern wird der Hash-Algorithmus `SHA256` angewendet. Bei Passwortänderungen müssen alle Benutzer, auch Benutzer mit der `root`-Rolle, diese Anforderungen einhalten.

Eingeschränkter Zugriff auf das Netzwerk – Nach der Installation ist das System vor Angriffen über das Netzwerk geschützt. Die Remote-Anmeldung des ersten Benutzers wird über eine authentifizierte, verschlüsselte Verbindung mithilfe des `ssh`-Protokolls zugelassen. Nur dieses Netzwerkprotokoll akzeptiert eingehende Pakete. Der `ssh`-Schlüssel wird vom Algorithmus `AES128` umgeben. Durch den verschlüsselten, authentifizierten Zugriff auf das System sind Benutzer vor Abfang- und Spoofing-Angriffen geschützt und müssen keine Änderungen vornehmen.

Protokollierte Anmeldeversuche – Der Prüfservice wird für alle `login/logout`-Ereignisse (Anmeldung, Abmeldung, Benutzerwechsel, Starten und Beenden einer `ssh`-Sitzung, Bildschirmsperre) und für alle nicht zuweisbaren (fehlgeschlagenen) Anmeldeversuche aktiviert. Da mit der `root`-Rolle keine Anmeldung möglich ist, kann der Name des Benutzers, der die `root`-Rolle übernommen hat, im Prüfpfad festgestellt werden. Der erste Benutzer kann die Prüfprotokolle aufgrund eines Rechts einsehen, das durch das Rechteprofil "System Administrator" gewährt wird.

Kernel-, Datei- und Desktopschutz

Nachdem der erste Benutzer angemeldet ist, sind Kernel, Dateisysteme und Desktopanwendungen durch geringste Berechtigungen, Zugriffsrechte und RBAC geschützt.

Kernel-Schutz – Viele Dämonen und administrative Befehle werden nur die für die erfolgreiche Ausführung erforderlichen Berechtigungen zugewiesen. Viele Dämonen werden über spezielle Verwaltungskonten ausgeführt, die nicht über `root` (`UID=0`)-Berechtigungen verfügen, damit sie nicht aufgrund eines Hijacking-Angriffs andere Aufgaben ausführen. Eine Anmeldung mit diesen speziellen Verwaltungskonten ist nicht möglich. Geräte sind durch Berechtigungen geschützt.

Dateisysteme – Alle Dateisysteme sind standardmäßig ZFS-Dateisysteme. Da der `umask`-Wert des Benutzers `022` beträgt, kann eine Datei oder ein Verzeichnis, die der Benutzer erstellt hat, nur durch ihn selbst geändert werden. Mitglieder der Gruppe des Benutzers sind berechtigt, das Verzeichnis zu lesen und zu durchsuchen sowie die Datei zu lesen. Angemeldete Benutzer, die nicht zur Gruppe des Benutzers gehören, können das Verzeichnis auflisten und die Datei lesen. Die Verzeichnisberechtigungen sind `drwxr-xr-x` (`755`). Die Dateiberechtigungen sind `-rw-r--r--` (`644`).

Desktopapplets – Desktopapplets werden durch RBAC geschützt. Beispiel: Nur der erste Benutzer oder der Benutzer mit der `root`-Rolle können mithilfe des Package Manager-Applets neue Pakete installieren. Der Package Manager wird normalen Benutzern nicht angezeigt, die nicht zur Nutzung des Applets berechtigt sind.

Zusätzliche Sicherheitsfunktionen

Oracle Solaris 11 bietet Sicherheitsfunktionen, die für die Konfiguration Ihrer Systeme verwendet werden können und die Ihren Standortsicherheitsanforderungen entsprechen.

- **RBAC (Role-Based Access Control) –** Oracle Solaris bietet eine Reihe von Authentifizierungen, Berechtigungen und Rechteprofilen. Die einzige definierte Rolle ist die `root` -Rolle. Die Rechteprofile sind eine gute Grundlage für das Erstellen von Rollen. Außerdem sind für das Ausführen von einigen administrativen Befehlen RBAC-Autorisierungen erforderlich. Benutzer ohne diese Autorisierungen können keine Befehle ausführen, auch wenn sie über die erforderlichen Berechtigungen verfügen.
- **Benutzerrechte –** Benutzer erhalten wie der erste Benutzer einen Basisberechtigungssatz, Rechteprofile und Autorisierungen aus der Datei `/etc/security/policy.conf` (siehe „Eingeschränkter und überwachter Systemzugriff“ auf Seite 21). Es gibt keine Obergrenze für Anmeldeversuche; sie werden jedoch durch den Prüfservice protokolliert.
- **Systemdateischutz –** Systemdateien werden durch Dateiberechtigungen geschützt. Systemdateien können nur in der `root`-Rolle geändert werden.

Standortsicherheitsrichtlinien und deren Umsetzung

Für ein sicheres System oder Netzwerk von Systemen sind eine Sicherheitsrichtlinie und entsprechende Sicherheitsanforderungen unabdingbar.

Weitere Informationen finden Sie hier:

- Anhang 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`)

◆ ◆ ◆ KAPITEL 2

Konfigurieren der Oracle Solaris 11-Sicherheitsfunktionen

In diesem Kapitel werden die für die Konfiguration der Sicherheitsfunktionen auf Ihrem System erforderlichen Schritte beschrieben. Das Kapitel thematisiert die Installation von Paketen sowie die Konfiguration des Systems, von Subsystemen und von zusätzlichen Anwendungen, die Sie eventuell benötigen, wie IPsec.

Installieren von Oracle Solaris

Wählen Sie bei der Installation des Oracle Solaris das Medium mit dem geeigneten *Gruppen*paket:

- **Oracle Solaris Large Server** – Durch das Standardmanifest in einer AI-Installation (Automated Installer) und der Text Installer wird die Gruppe `group/system/solaris-large-server` installiert und somit eine große Oracle Solaris -Serverumgebung bereitgestellt.
- **Oracle Solaris Desktop** – Durch Live Media wird die Gruppe `group/system/solaris-desktop` installiert, wodurch eine Oracle Solaris 11-Desktopumgebung bereitgestellt wird.

  Sie können ein Desktopsystem zur zentralen Nutzung erstellen, indem Sie einem Oracle Solaris-Server die Gruppe `group/feature/multi-user-desktop` hinzufügen. Weitere Informationen erhalten Sie im Artikel Optimizing the Oracle Solaris 11 Desktop for a Multiuser Environment .

Informationen zur automatisierten Installation mithilfe des AI (Automated Installer) erhalten Sie unter Teil III, „Installing Using an Install Server“ in *Installing Oracle Solaris 11 Systems*.

Informationen zur Auswahl der Medien finden Sie in den folgenden Installationsanleitungen:

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

Systemsicherung

Sie sollten die Schritte in der vorgegebenen Reihenfolge durchführen. Zu diesem Zeitpunkt ist das Oracle Solaris 11-Betriebssystem installiert und nur der erste Benutzer, der zur Übernahme der `root`-Rolle berechtigt ist, kann auf das System zugreifen.

Aufgabe	Beschreibung	Anweisungen siehe
1. Überprüfen der Pakete im System	Dadurch wird überprüft, ob die Pakete auf dem Installationsdatenträger den installierten Paketen entsprechen.	„Überprüfen der Pakete“ auf Seite 27
2. Schutz der Hardwareeinstellungen des Systems	Die Hardware wird geschützt, indem ein Passwort für Änderungen der Hardwareeinstellungen verlangt wird.	„Controlling Access to System Hardware (Tasks)“ in *Oracle Solaris Administration: Security Services*
3. Deaktivieren nicht erforderlicher Services	Prozesse, die für den Systemablauf nicht erforderlich sind, werden nicht ausgeführt.	„Deaktivieren nicht erforderlicher Services“ auf Seite 27

Aufgabe	Beschreibung	Anweisungen siehe
4. Genehmigung der Gerätezuordnung	Die Verwendung von Wechseldatenträgern ohne ausdrückliche Genehmigung wird unterbunden. Zu Geräten zählen u. a. Mikrofone, USB-Laufwerke und CDs.	„How to Enable Device Allocation“ in *Oracle Solaris Administration: Security Services*
5. Kein Ausschalten des Systems durch den Eigentümer der Workstation	Dadurch soll vermieden werden, dass der Konsolenbenutzer das System ausschaltet oder anhält.	„Entfernen der Energieverwaltungsfunktion für Benutzer“ auf Seite 28
6. Erstellen Sie eine Anmeldewarnmeldung gemäß Ihrer Standortsicherheitsrichtlinie.	Benutzer und potenzielle Angreifer werden benachrichtigt, dass das System überwacht wird.	„Hinzufügen einer Sicherheitsmeldung zu allen Bannerdateien“ auf Seite 29 „Einfügen einer Sicherheitsmeldung in den Desktop-Anmeldebildschirm“ auf Seite 29

▼ Überprüfen der Pakete

Validieren Sie die Installation direkt nach dem Installationsvorgang, indem Sie die Pakete überprüfen.

Bevor Sie beginnen Sie müssen die `root`-Rolle übernehmen.

1. **Führen Sie den Befehl `pkg verify` aus.**

   Leiten Sie die Befehlsausgabe zur Dokumentation in eine Datei um.

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

2. **Sehen Sie in der Protokolldatei nach, ob Fehler aufgetreten sind.**

3. **Wenn Sie Fehler finden, führen Sie eine Neuinstallation vom Datenträger durch oder beheben Sie die Fehler.**

Siehe auch Weitere Informationen finden Sie auf den Manpages `pkg`(1) und `pkg`(5). Die Manpages enthalten Beispiele zur Verwendung des Befehls `pkg verify`.

▼ Deaktivieren nicht erforderlicher Services

Führen Sie diese Schritte durch, um je nach Verwendungszweck Ihres Systems nicht erforderliche Services zu deaktivieren.

Bevor Sie beginnen Sie müssen die `root`-Rolle übernehmen.

1. **Rufen Sie die Liste der Onlineservices auf.**

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

2. **Deaktivieren Sie die für das System nicht erforderlichen Services.**

   Beispiel: Wenn es sich beim System nicht um einen NFS-Server oder Webserver handelt und Services online sind, deaktivieren Sie sie.

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

Siehe auch Weitere Informationen finden Sie in Kapitel 6, „Managing Services (Overview)“ in *Oracle Solaris Administration: Common Tasks* und auf der Manpage `svcs(1)`.

▼ Entfernen der Energieverwaltungsfunktion für Benutzer

Führen Sie diese Schritte durch, damit Benutzer das System weder anhalten noch abschalten können.

Bevor Sie beginnen Sie müssen die `root`-Rolle übernehmen.

1. **Überprüfen Sie den Inhalt des Rechteprofils "Console User".**

```
% 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. **Erstellen Sie ein Rechteprofil, das Rechte im Profil "Console User" enthält, die der Benutzer behalten soll.**

   Anweisungen dazu finden Sie unter „How to Create or Change a Rights Profile“ in *Oracle Solaris Administration: Security Services*.

3. **Setzen Sie das Rechteprofil "Console User" in der Datei `/etc/security/policy.conf` in Kommentare.**

```
#CONSOLE_USER=Console User
```

4. **Weisen Sie einem Benutzer das Rechteprofil zu, das Sie unter Schritt 2 erstellt haben.**

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

Siehe auch Weitere Informationen finden Sie unter „policy.conf File“ in *Oracle Solaris Administration: Security Services* sowie auf den Manpages `policy.conf(4)` und `usermod(1M)`.

▼ Hinzufügen einer Sicherheitsmeldung zu allen Bannerdateien

Führen Sie diese Schritte durch, um Warnmeldungen zu erstellen, die Ihrer Standortsicherheitsrichtlinie entsprechen. Der Inhalt dieser Dateien wird bei der lokalen und der Remote-Anmeldung angezeigt.

Hinweis – Die hier als Beispiele angeführten Meldungen entsprechen nicht den Anforderungen der US-Behörden und wahrscheinlich auch nicht Ihrer Sicherheitsrichtlinie.

Bevor Sie beginnen Sie müssen die `root`-Rolle übernehmen. Es empfiehlt sich, den Inhalt der Sicherheitsmeldung mit dem Rechtsberater im Unternehmen zu besprechen.

1 Geben sie eine Sicherheitsmeldung in die Datei `/etc/issue` ein.

```
# 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.
```

Weitere Informationen finden Sie auf der Manpage `issue(4)`.

Das Programm `telnet` zeigt den Inhalt der Datei `/etc/issue` als Anmeldenachricht an. Informationen zur Nutzung dieser Datei durch andere Anwendungen erhalten Sie unter „Sicherheitsmeldung für `ssh` und `ftp` Nutzer anzeigen“ auf Seite 40 und „Einfügen einer Sicherheitsmeldung in den Desktop-Anmeldebildschirm“ auf Seite 29.

2 Fügen Sie der Datei `/etc/motd` eine Sicherheitsmeldung hinzu.

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

▼ Einfügen einer Sicherheitsmeldung in den Desktop-Anmeldebildschirm

Wählen Sie eine Methode zur Erstellung einer Sicherheitsmeldung, die Benutzern bei der Anmeldung angezeigt wird.

Weitere Informationen erhalten Sie durch den GNOME Help Browser (GNOME-Hilfebrowser). Klicken Sie dazu auf dem Desktop auf "System" und dann "Hilfe". Sie können stattdessen auch den Befehl `yelp` verwenden. Desktop-Anmeldeskripte werden im Abschnitt `GDM Login Scripts and Session Files` der Manpage `gdm`(1M) behandelt.

Hinweis – Die hier als Beispiel angeführte Meldung entspricht nicht den Anforderungen der US-Behörden und wahrscheinlich auch nicht Ihrer Sicherheitsrichtlinie.

Bevor Sie beginnen Sie müssen die `root`-Rolle übernehmen. Es empfiehlt sich, den Inhalt der Sicherheitsmeldung mit dem Rechtsberater im Unternehmen zu besprechen.

- **Einfügen einer Sicherheitsmeldung in den Desktop-Anmeldebildschirm**

  Ihnen stehen mehrere Optionen zur Verfügung. Die Optionen, mit denen ein Dialogfeld erstellt wird, verwenden möglicherweise die Datei `/etc/issue` aus Schritt 1 von „Hinzufügen einer Sicherheitsmeldung zu allen Bannerdateien“ auf Seite 29.

  - **Option 1: Erstellen Sie eine Desktop-Datei, durch die bei der Anmeldung eine Sicherheitsmeldung in einem Dialogfeld angezeigt wird.**

    ```
    # 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
    ```

    Nach der Authentifizierung im Anmeldebildschirm muss der Benutzer das Dialogfeld schließen, um zum Arbeitsbereich zu gelangen. Optionen des Befehls `zenity` finden Sie auf der Manpage `zenity`(1).

  - **Option 2: Passen Sie ein GDM-Initialisierungsskript so an, dass die Sicherheitsmeldung in einem Dialogfeld angezeigt wird.**

    Das Verzeichnis `/etc/gdm` enthält drei Initialisierungsskripte, die die Sicherheitsmeldung vor, während oder direkt nach der Desktop-Anmeldung anzeigen. Diese Skripte sind in der Oracle Solaris 10-Version ebenfalls verfügbar.

    - **Zeigen Sie die Sicherheitsmeldung vor dem Anmeldebildschirm an.**

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

    - **Zeigen Sie die Sicherheitsmeldung nach der Authentifizierung auf dem Anmeldebildschirm an.**

      Dieses Skript wird ausgeführt, bevor der Arbeitsbereich des Benutzers angezeigt wird. Ändern Sie zur Erstellung dieses Skripts das Skript `Default.sample`.

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

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

- **Zeigen Sie die Sicherheitsmeldung nach der Authentifizierung ganz am Anfang des Arbeitsbereichs des Benutzers an.**

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

  Hinweis – Das Dialogfeld kann durch Fenster im Arbeitsbereich des Benutzers verdeckt werden.

- **Option 3: Ändern Sie den Anmeldebildschirm, sodass die Sicherheitsmeldung über dem Eingabefeld angezeigt wird.**

  Die Größe des Anmeldefensters wird angepasst, sodass Ihre Meldung sichtbar ist. Diese Methode enthält keinen Verweis auf die Datei `/etc/issue`. Sie müssen den Text in die grafische Benutzeroberfläche eingeben.

  Hinweis – Der Anmeldebildschirm `gdm-greeter-login-window.ui` wird durch die Befehle `pkg fix` und `pkg update` überschrieben. Damit Ihre Änderungen beibehalten werden, kopieren Sie die Datei in ein Konfigurationsdateienverzeichnis, und führen Sie die Änderungen darin nach dem Systemupgrade mit der neuen Datei zusammen. Weitere Informationen erhalten Sie auf der Manpage `pkg`(5).

  a. **Wechseln Sie das Verzeichnis und gehen Sie zur Benutzeroberfläche des Anmeldefensters.**

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

  b. **(Optional) Speichern Sie eine Kopie der ursprünglichen Benutzeroberfläche des Anmeldebildschirms.**

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

  c. **Fügen Sie dem Anmeldefenster mithilfe des GNOME Toolkit interface designer (GNOME-Toolkit-Benutzeroberflächendesigner) eine Beschriftung hinzu.**

     Der Benutzeroberflächendesigner GTK+ wird durch das Programm `glade-3` geöffnet. Sie geben die Sicherheitsmeldung in eine Beschriftung ein, die über dem Eingabefeld angezeigt wird.

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

     Das Handbuch zum Benutzeroberflächendesigner finden Sie im GNOME Help Browser (GNOME-Hilfebrowser) unter "Development" (Entwicklung). Die Manpage `glade-3`(1) ist im Handbuch unter "Applications" (Anwendungen) aufgeführt.

d. (Optional) Nehmen Sie die Änderungen an der Benutzeroberfläche des Anmeldefensters vor und speichern Sie eine Kopie.

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

Beispiel 2–1 Erstellen einer kurzen Warnmeldung zur Anzeige bei der Desktop-Anmeldung

In diesem Beispiel gibt der Administrator einen kurzen Meldungstext als Argument für den Befehl `zenity` in die Desktop-Datei ein. Darüber hinaus verwendet der Administrator die Option `--warning`, durch die ein Warnsymbol zusammen mit dem Text angezeigt wird.

```
# 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
```

Schutz für Benutzer

Nur der erste Benutzer, der zur Übernahme der `root`-Rolle berechtigt ist, kann zu diesem Zeitpunkt auf das System zugreifen. Sie sollten die Schritte in der vorgegebenen Reihenfolge durchführen, bevor sich normale Benutzer anmelden können.

Aufgabe	Beschreibung	Anweisungen siehe
Sichere Passwörter und häufige Passwortänderungen	Dadurch werden die standardmäßig auf jedem System vorhandenen Passwortbeschränkungen verstärkt.	„Festlegen strikterer Passwortbeschränkungen“ auf Seite 33
Konfigurieren Sie restriktive Dateiberechtigungen für normale Benutzer.	Hierdurch wird ein restriktiverer Wert als `022` für Dateiberechtigungen der normalen Benutzer festgelegt.	„Festlegen eines restriktiveren `umask`-Werts für normale Benutzer“ auf Seite 35
Legen Sie die Kontosperre für normale Benutzer fest.	Legt bei Systemen, die nicht für die Administration verwendet werden, die Kontosperre systemweit fest und verringert die Anzahl der Anmeldeversuche bis zur Aktivierung der Sperre.	„Festlegen der Kontosperre für normale Benutzer“ auf Seite 34
Treffen Sie eine Vorauswahl zusätzlicher Prüfklassen.	Auf diese Weise können Sie potenzielle Bedrohungen des Systems überwachen und aufzeichnen.	„Prüfen wichtiger Ereignisse außer Anmelden/Abmelden“ auf Seite 36
Senden Sie Zusammenfassungen von Prüfereignissen in Textform an das Dienstprogramm `syslog`.	Enthält in Echtzeit aufgezeichnete, wichtige Prüfereignisse wie Anmeldungen und Anmeldeversuche.	„Überwachen von `lo`-Ereignissen in Echtzeit“ auf Seite 36

Aufgabe	Beschreibung	Anweisungen siehe
Erstellen Sie Rollen.	Dadurch werden einzelne administrative Aufgaben an mehrere vertrauenswürdige Benutzer verteilt, sodass das System nicht beschädigt werden kann.	„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*
Zeigen Sie zulässige Anwendungen nur auf dem Desktop des Benutzers an.	Dadurch wird vermieden, dass Benutzer Anwendungen anzeigen oder verwenden, die sie nicht nutzen dürfen.	Siehe „How to Limit a User to Desktop Applications“ in *Trusted Extensions Configuration and Administration*
Schränken Sie Benutzerrechte ein.	Dadurch werden die Basisberechtigungen entfernt, die Benutzer nicht benötigen.	„Entfernen nicht benötigter Basisberechtigungen von Benutzern“ auf Seite 37

▼ Festlegen strikterer Passwortbeschränkungen

Führen Sie diese Schritte durch, wenn die Standardwerte nicht den Sicherheitsbestimmungen Ihres Standorts entsprechen. Die Schritte richten sich nach der Liste der Einträge in der Datei `/etc/default/passwd`.

Bevor Sie beginnen

Vergewissern Sie sich vor Änderung der Standardwerte, dass sich dadurch alle Benutzer bei ihren Anwendungen und anderen Systemen im Netzwerk authentifizieren können.

Sie müssen die `root`-Rolle übernehmen.

- **Bearbeiten Sie die Datei `/etc/default/passwd` und legen Sie Folgendes fest:**

  a. **Passwortänderung durch den Benutzer frühestens alle drei Wochen, spätestens jeden Monat**

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

  b. **Passwortmindestlänge von 8 Zeichen**

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

  c. **Passwortabfolge**

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

d. Mindestabweichung vom letzten Passwort

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

e. Obligatorische Verwendung eines Großbuchstabens

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

f. Obligatorische Verwendung einer Zahl

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

Siehe auch

- Eine Liste von Variablen zur Erstellung sicherer Passwörter finden Sie in der Datei `/etc/default/passwd`. Die Standardwerte sind in der Datei angegeben.
- Informationen zu den nach der Installation wirksamen Passwortbeschränkungen finden Sie in „Eingeschränkter und überwachter Systemzugriff“ auf Seite 21.
- Manpage `passwd(1)`

▼ Festlegen der Kontosperre für normale Benutzer

Führen Sie diese Schritte durch, um normale Benutzerkonten nach einer bestimmten Anzahl von fehlgeschlagenen Anmeldeversuchen zu sperren.

Hinweis – Legen Sie keine Kontosperre für Benutzer fest, die Rollen übernehmen können, da dadurch die Rolle gesperrt werden kann.

Bevor Sie beginnen

Sie müssen die `root`-Rolle übernehmen. Legen Sie keinen systemweiten Schutz fest auf einem System, das Sie für administrative Aufgaben nutzen.

1 Legen Sie das Sicherheitsattribut `LOCK_AFTER_RETRIES` auf `YES` fest.

- **Legen Sie das Attribut systemweit fest.**

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

- **Legen Sie das Attribut für jeden Benutzer fest.**

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

2. **Legen Sie das Sicherheitsattribut `RETRIES` auf `3` fest.**

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

Siehe auch

- Eine Beschreibung der Sicherheitsattribute für Benutzer und Rollen finden Sie in Kapitel 10, „Security Attributes in Oracle Solaris (Reference)“ in *Oracle Solaris Administration: Security Services*.
- Manpages `policy.conf`(4) und `user_attr`(4)

▼ Festlegen eines restriktiveren umask-Werts für normale Benutzer

Wenn der `umask`-Standardwert `022` nicht ausreichend ist, gehen Sie folgendermaßen vor, um einen restriktiveren Wert festzulegen.

Bevor Sie beginnen Sie müssen die `root`-Rolle übernehmen.

- **Ändern Sie den unmask-Wert in den Anmeldeprofilen in den Schemaverzeichnissen für die Shells.**

  Oracle Solaris bietet Administratoren Verzeichnisse zur benutzerdefinierten Anpassung der Shell-Standardwerte des Benutzers. In diesen Schemaverzeichnissen befinden sich u. a. die Dateien `.profile` , `.bashrc` und `.kshrc`.

  Wählen Sie einen der folgenden Werte:

  - `umask 027` – bietet maßvollen Dateischutz

    (`740`) – `w` für Gruppe, `rwx` für andere
  - `umask 026` – bietet leicht erhöhten Dateischutz

    (`741`) – `w` für Gruppe, `rw` für andere
  - `umask 077` – bietet kompletten Dateischutz

    (`700`) – kein Zugriff für Gruppen oder andere Personen

Siehe auch Weitere Informationen finden Sie hier:

- „Setting Up User Accounts“ in *Oracle Solaris Administration: Common Tasks*
- „Default umask Value“ in *Oracle Solaris Administration: Security Services*
- Manpages `usermod`(1M) und `umask`(1)

▼ Prüfen wichtiger Ereignisse außer Anmelden/Abmelden

Führen Sie diese Schritte durch, um administrative Befehle, Angriffsversuche auf das System und andere in Ihrer Standortsicherheitsrichtlinie angegebenen wichtige Ereignisse zu prüfen.

Hinweis – Die Beispiele in dieser Anweisung erfüllen möglicherweise nicht die Anforderungen Ihrer Sicherheitsrichtlinie.

Bevor Sie beginnen Sie müssen die `root`-Rolle übernehmen. Sie implementieren Ihre Standortsicherheitsrichtlinie im Hinblick auf Prüfungen.

1 Prüfen Sie alle Fälle, in denen privilegierte Befehle durch Benutzer und Rollen verwendet wurden.

Fügen Sie den Vorauswahlmasken aller Benutzer und Rollen das Prüfereignis `AUE_PFEXEC` hinzu.

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

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

2 Zeichnen Sie die Argumente für Prüfbefehle auf.

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

3 Zeichnen Sie die Umgebung auf, in der Prüfbefehle ausgeführt werden.

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

Siehe auch

- Informationen zum Thema Prüfungsrichtlinien finden Sie unter „Audit Policy“ in *Oracle Solaris Administration: Security Services* .
- Beispiele für das Festlegen von Prüf-Flags finden Sie unter „Configuring the Audit Service (Tasks)“ in *Oracle Solaris Administration: Security Services* und unter „Troubleshooting the Audit Service (Tasks)“ in *Oracle Solaris Administration: Security Services* .
- Informationen zum Konfigurieren von Prüfungen erhalten Sie auf der Manpage `auditconfig(1M)`.

▼ Überwachen von lo-Ereignissen in Echtzeit

Führen Sie diese Schritte zum Aktivieren des `audit_syslog`-Plug-ins durch, um Ereignisse in Echtzeit zu überwachen.

Bevor Sie beginnen Sie müssen die `root`-Rolle übernehmen, um die Datei `syslog.conf` zu ändern. Für die weiteren Schritte muss Ihnen das Rechteprofil "Audit Configuration" zugewiesen sein.

1. **Senden Sie die Klasse `lo` an das `audit_syslog`-Plug-in und aktivieren Sie das Plug-in.**

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

2. **Fügen Sie einen `audit.notice`-Eintrag zur Datei `syslog.conf` hinzu.**

   Der Standardeintrag enthält den Speicherort der Protokolldatei.

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

3. **Erstellen Sie die Protokolldatei.**

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

4. **Aktualisieren Sie die Konfigurationsinformationen für den `syslog`-Service.**

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

5. **Aktualisieren Sie den Prüfservice.**

   Bei Aktualisierung überträgt der Prüfservice die Änderungen an das Prüf-Plug-in.

   ```
   # audit -s
   ```

Siehe auch

- Ein Beispiel für das Senden von Prüfzusammenfassungen an ein anderes System finden Sie unter „How to Configure syslog Audit Logs“ in *Oracle Solaris Administration: Security Services*.
- Die durch den Prüfservice generierte Ausgabe kann sehr umfangreich sein. Informationen zum Verwalten der Protokolle finden Sie auf der Manpage `logadm`(1M).
- Informationen zum Überwachen der Ausgabe finden Sie in „Überwachen von `audit_syslog`-Prüfzusammenfassungen“ auf Seite 55.

▼ Entfernen nicht benötigter Basisberechtigungen von Benutzern

Unter bestimmten Umständen können bis zu drei Basisberechtigungen aus einem Basissatz für normale Benutzer entfernt werden.

- `file_link_any` – Ein Prozess kann dadurch Hard Links zu Dateien erstellen, deren Eigentümer eine UID ist, die sich von der tatsächlichen UID des Prozesses unterscheidet.
- `proc_info` – Ein Prozess kann den Status anderer Prozesse untersuchen, an die er kein Signal sendet. Prozesse, die nicht untersucht werden können, werden in `/proc` nicht angezeigt und scheinen nicht vorhanden zu sein.
- `proc_session` – Ein Prozess kann außerhalb seiner Sitzung Signale senden oder Prozesse verfolgen.

Bevor Sie beginnen Sie müssen die `root`-Rolle übernehmen.

1. **Benutzer sollen eine Datei, die sie nicht besitzen, nicht verlinken können.**

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

2. **Benutzer sollen keine Prozesse untersuchen können, die sie nicht besitzen.**

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

3. **Benutzer sollen keine zweite Sitzung neben der aktuellen starten können, z. B. eine `ssh`-Sitzung.**

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

4. **Entfernen aller drei Basisberechtigungen aus einem Basissatz für normale Benutzer**

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

Siehe auch Weitere Informationen finden Sie in Kapitel 8, „Using Roles and Privileges (Overview)“ in *Oracle Solaris Administration: Security Services* und auf der Manpage `privileges`(5).

Kernel-Schutz

Zu diesem Zeitpunkt haben Sie wahrscheinlich Benutzer, die Rollen übernehmen können, und Rollen erstellt. Systemdateien können nur in der `root`-Rolle geändert werden.

Aufgabe	Beschreibung	Anweisungen siehe
Hindern Sie Programme an der Nutzung eines ausführbaren Stacks.	Eine Systemvariable wird festgelegt, die Angriffe durch Pufferüberlauf aufgrund der Nutzung von ausführbaren Stacks verhindert.	„Protecting Executable Files From Compromising Security“ in *Oracle Solaris Administration: Security Services*
Schützen Sie Core-Dateien, die möglicherweise vertrauliche Informationen enthalten.	Es wird ein Verzeichnis mit eingeschränktem Zugriff erstellt, das für Core-Dateien verwendet wird.	„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*

Konfigurieren des Netzwerks

Zu diesem Zeitpunkt haben Sie wahrscheinlich Benutzer, die Rollen übernehmen können, und Rollen erstellt. Systemdateien können nur in der `root`-Rolle geändert werden.

Führen Sie von den folgenden Schritten diejenigen durch, die zusätzliche Sicherheit gemäß den Anforderungen Ihres Standorts geben. Diese Netzwerkaufgaben benachrichtigen Benutzer, die sich über eine Remote-Verbindung beim geschützten System anmelden, und unterstützen die Protokolle IP, ARP und TCP.

Aufgabe	Beschreibung	Anweisungen siehe
Zeigen Sie Warnmeldungen an, die Ihren Standortsicherheitsrichtlinien entsprechen.	Benutzer und potenzielle Angreifer werden benachrichtigt, dass das System überwacht wird.	„Sicherheitsmeldung für `ssh` und `ftp` Nutzer anzeigen“ auf Seite 40
Deaktivieren Sie den Netzwerkrouting-Dämon.	Dadurch wird der Zugriff auf das System durch potenzielle Netzwerk-Snooper eingeschränkt.	„Deaktivieren des Netzwerkrouting-Dämons“ auf Seite 41
Unterbinden Sie die Verteilung von Informationen zur Netzwerktopologie.	Der Broadcast von Paketen wird verhindert.	„Deaktivieren von Broadcast-Paketweiterleitung“ auf Seite 41
	Es wird nicht auf Broadcast- und Multicast-Echoanforderungen reagiert.	„Deaktivieren von Antworten auf Echoanforderungen“ auf Seite 42
Aktivieren Sie Strict Source und Destination Multihoming für Systeme, die als Gateway zu anderen Domains fungieren, zum Beispiel Firewalls oder VPN-Knoten.	Pakete ohne Gateway-Adresse im Header können das Gateway nicht passieren.	„Festlegen von Strict Multihoming“ auf Seite 43
Verhindern Sie DoS-Angriffe durch Kontrolle der Anzahl an unvollständigen Systemverbindungen.	Schränkt die zulässige Anzahl unvollständiger TCP-Verbindungen für einen TCP-Listener ein.	„Festlegen einer Maximalanzahl unvollständiger TCP-Verbindungen“ auf Seite 43
Unterbinden Sie DoS-Angriffe durch Kontrolle der Anzahl an zulässigen eingehenden Verbindungen.	Gibt das standardmäßige Maximum an anstehenden TCP-Verbindungen für einen TCP-Listener an.	„Festlegen einer maximalen Anzahl an ausstehenden TCP-Verbindungen“ auf Seite 44
Erstellen Sie sichere Zufallszahlen für TCP-Erstverbindungen.	Entspricht dem durch RFC 1948 angegebenen Sequenznummergenerierungswert.	„Geben Sie eine sichere Zufallszahl für die TCP-Erstverbindung an“ auf Seite 44
Setzen Sie die Netzwerkparameter auf ihre Standardeinstellungen zurück.	Dadurch wird die Sicherheit erhöht, die durch administrative Aktionen verringert wurde.	„Zurücksetzen von Netzwerkparametern auf sichere Werte“ auf Seite 44

Aufgabe	Beschreibung	Anweisungen siehe
Fügen Sie Netzwerkdiensten TCP-Wrapper zur Beschränkung von Anwendungen auf legitime Benutzer hinzu.	Gibt Systeme an, die berechtigt sind, auf Netzwerkdienste wie FTP-Programme zuzugreifen. Die Anwendung `sendmail` ist standardmäßig durch TCP-Wrapper geschützt, wie unter „Support for TCP Wrappers From Version 8.12 of sendmail“ in *Oracle Solaris Administration: Network Services* beschrieben.	Informationen zum Aktivieren von TCP-Wrappern für alle `inetd`-Services erhalten Sie unter „How to Use TCP Wrappers to Control Access to TCP Services“ in *Oracle Solaris Administration: IP Services*. Ein Beispiel für den Schutz von FTP-Netzwerkdiensten mithilfe von TCP-Wrappern finden Sie unter „How to Start an FTP Server Using SMF“ in *Oracle Solaris Administration: Network Services*.

▼ Sicherheitsmeldung für ssh und ftp Nutzer anzeigen

Führen Sie diese Schritte durch, um bei Remote-Anmeldungen und Dateiübertragungen eine Warnung anzuzeigen.

Bevor Sie beginnen Sie müssen die `root`-Rolle übernehmen. Sie haben die Datei `/etc/issue` aus Schritt 1 von „Hinzufügen einer Sicherheitsmeldung zu allen Bannerdateien“ auf Seite 29 erstellt.

1 Gehen Sie wie folgt vor, um Benutzern eine Sicherheitsmeldung anzuzeigen, die sich mit dem Befehl `ssh` anmelden:

a. Entfernen Sie die Kommentarzeichen aus der Banneranweisung in der Datei `/etc/sshd_config`.

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

b. Aktualisieren Sie den `ssh`-Service.

```
# svcadm refresh ssh
```

Weitere Informationen finden Sie auf den Manpages `issue(4)` und `sshd_config(4)`.

2 Gehen Sie wie folgt vor, um eine Sicherheitsmeldung Benutzern anzuzeigen, die sich mit dem Befehl `ftp` anmelden:

a. Fügen Sie die Anweisung `DisplayConnect` der Datei `proftpd.conf` hinzu.

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

b. Starten Sie den `ssh`-Service neu.

```
# svcadm restart ftp
```

Weitere Informationen erhalten Sie auf der Website ProFTPD (`http://www.proftpd.org/`).

Deaktivieren des Netzwerkrouting-Dämons

Führen Sie diese Schritte durch, um Netzwerkrouting nach der Installation zu unterbinden, indem Sie einen Standard-Router angeben. Führen Sie ansonsten diese Schritte nach der manuellen Routingkonfiguration durch.

Hinweis – Bei vielen Netzwerken ist es erforderlich, dass während der Konfiguration der Routing-Dämon deaktiviert wird. Daher ist es möglich, dass Sie diesen Dämon im Rahmen einer umfangreichen Konfiguration deaktiviert haben.

Bevor Sie beginnen Das Rechteprofil "Network Management" muss Ihnen zugewiesen sein.

1 Überprüfen Sie, ob der Routing-Dämon ausgeführt wird.

```
# 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.
```

Wenn der Service nicht ausgeführt wird, entfallen weitere Schritte.

2 Deaktivieren Sie den Routing-Dämon.

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

3 Überprüfen Sie, ob der Routing-Dämon deaktiviert ist.

```
# 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.
```

Siehe auch Manpage `routeadm(1M)`

Deaktivieren von Broadcast-Paketweiterleitung

Oracle Solaris leitet Broadcast-Pakete standardmäßig weiter. Wenn Sie aufgrund Ihrer Sicherheitsrichtlinie die Bedrohung durch Broadcast-Flooding einschränken müssen, ändern Sie mithilfe dieser Schritte den Standardwert.

Hinweis – Durch das Deaktivieren der Netzwerkeigenschaft `_forward_directed_broadcasts` deaktivieren Sie auch Broadcast-Pings.

Bevor Sie beginnen Das Rechteprofil "Network Management" muss Ihnen zugewiesen sein.

1 Legen Sie den Wert der Broadcast-Paketweiterleitungseigenschaft auf 0 für IP-Pakete fest.

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

2 Prüfen Sie den aktuellen Wert.

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

Siehe auch Manpage `ipadm(1M)`

▼ Deaktivieren von Antworten auf Echoanforderungen

Führen Sie diese Schritte durch, um die Verteilung von Informationen zur Netzwerktopologie zu verhindern.

Bevor Sie beginnen Das Rechteprofil "Network Management" muss Ihnen zugewiesen sein.

1 Legen Sie den Wert der Eigenschaft für Antworten auf Broadcast-Echoanforderungen auf 0 für IP-Pakete fest und überprüfen Sie dann den aktuellen Wert.

```
# 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 Legen Sie den Wert der Eigenschaft für Antworten auf Multicast-Echoanforderungen auf 0 für IP-Pakete fest und überprüfen Sie dann den aktuellen Wert.

```
# 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
```

Siehe auch Weitere Informationen finden Sie unter „_respond_to_echo_broadcast and _respond_to_echo_multicast (ipv4 or ipv6)“ in *Oracle Solaris Tunable Parameters Reference Manual* und auf der Manpage `ipadm(1M)`.

▼ Festlegen von Strict Multihoming

Führen Sie die folgenden Schritte durch, um für Systeme, die als Gateway zu anderen Domains fungieren (beispielsweise Firewalls oder VPN-Knoten), Strict Multihoming zu aktivieren.

In der Oracle Solaris 11-Version kommt eine neue Eigenschaft hinzu: `hostmodel` für IPv4 und IPv6. Diese Eigenschaft steuert das Verhalten beim Senden und Empfangen von IP-Paketen in einem Multihoming-System.

Bevor Sie beginnen Das Rechteprofil "Network Management" muss Ihnen zugewiesen sein.

1 Legen Sie die Eigenschaft `hostmodel` auf `strong` für IP-Pakete fest.

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

2 Überprüfen Sie den aktuellen Wert und beachten Sie die möglichen Werte.

```
# 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
```

Siehe auch Weitere Informationen erhalten Sie unter „hostmodel (ipv4 or ipv6)“ in *Oracle Solaris Tunable Parameters Reference Manual* und auf der Manpage `ipadm`(1M).

Weitere Informationen über die Verwendung von Strict Multihoming finden Sie unter „How to Protect a VPN With IPsec in Tunnel Mode“ in *Oracle Solaris Administration: IP Services*.

▼ Festlegen einer Maximalanzahl unvollständiger TCP-Verbindungen

Wenden Sie DoS-Angriffe (Denial of Service) ab, indem Sie mithilfe dieser Schritte die Anzahl an ausstehenden, unvollständigen Verbindungen begrenzen.

Bevor Sie beginnen Das Rechteprofil "Network Management" muss Ihnen zugewiesen sein.

1 Legen Sie die maximale Anzahl an eingehenden Verbindungen fest.

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

2 Prüfen Sie den aktuellen Wert.

```
# 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
```

Siehe auch Weitere Informationen erhalten Sie unter „_conn_req_max_q0“ in *Oracle Solaris Tunable Parameters Reference Manual* und auf der Manpage `ipadm`(1M).

▼ Festlegen einer maximalen Anzahl an ausstehenden TCP-Verbindungen

Wenden Sie DoS-Angriffe ab, indem Sie mithilfe dieser Schritte die Anzahl der zulässigen eingehenden Verbindungen begrenzen.

Bevor Sie beginnen Das Rechteprofil "Network Management" muss Ihnen zugewiesen sein.

1 **Legen Sie die maximale Anzahl an eingehenden Verbindungen fest.**

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

2 **Prüfen Sie den aktuellen Wert.**

```
# 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
```

Siehe auch Weitere Informationen finden Sie unter „_conn_req_max_q“ in *Oracle Solaris Tunable Parameters Reference Manual* und auf der Manpage `ipadm`(1M).

▼ Geben Sie eine sichere Zufallszahl für die TCP-Erstverbindung an

Durch diesen Vorgang wird der Parameter für die TCP-Anfangssequenznummergenerierung so festgelegt, dass er RFC 1948 (`http://www.ietf.org/rfc/rfc1948.txt`) entspricht.

Bevor Sie beginnen Sie müssen die `root`-Rolle übernehmen, um eine Systemdatei zu ändern.

- **Ändern Sie den Standardwert für die Variable `TCP_STRONG_ISS`.**

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

▼ Zurücksetzen von Netzwerkparametern auf sichere Werte

Viele Netzwerkparameter, die standardmäßig ausreichenden Schutz bieten, können geändert werden. Setzen Sie diese Parameter auf ihre Standardwerte zurück, sofern dadurch nicht gegen die Sicherheitsrichtlinien verstoßen wird.

Bevor Sie beginnen Das Rechteprofil "Network Management" muss Ihnen zugewiesen sein. Der abgeänderte Wert des Parameters bietet weniger Schutz als der Standardwert.

1 Legen Sie die Eigenschaft für das Weiterleiten von Quellpaketen auf 0 für IP-Pakete fest und überprüfen Sie den aktuellen Wert.

Der Standardwert verhindert DoS-Angriffe von nachgeahmten Paketen.

```
# 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
```

Weitere Informationen finden Sie unter „forwarding (ipv4 or ipv6)“ in *Oracle Solaris Tunable Parameters Reference Manual* .

2 Legen Sie die Eigenschaft für Netzmaskenantworten auf 0 für IP-Pakete fest und überprüfen Sie den aktuellen Wert.

Durch den Standardwert wird die Verteilung von Informationen zur Netzwerktopologie verhindert.

```
# 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 Legen Sie die Eigenschaft für Zeitstempelantworten auf 0 für IP-Pakete fest und überprüfen Sie den aktuellen Wert.

Durch den Standardwert wird zusätzlicher CPU-Bedarf in Systemen sowie die Verteilung von Netzwerkinformationen unterbunden.

```
# 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 Legen Sie die Eigenschaft für Broadcast-Zeitstempelantworten auf 0 für IP-Pakete fest und überprüfen Sie den aktuellen Wert.

Durch den Standardwert wird zusätzlicher CPU-Bedarf in Systemen sowie die Verteilung von Netzwerkinformationen unterbunden.

```
# 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 **Legen Sie die Eigenschaft für das Ignorieren von Umleitungen auf 0 für IP-Pakete fest und überprüfen Sie den aktuellen Wert.**

Durch den Standardwert wird zusätzlicher CPU-Bedarf in Systemen unterbunden.

```
# 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 **Unterbinden Sie IP-Quellrouting.**

Wenn Sie zu Diagnosezwecken IP-Quellrouting durchführen müssen, deaktivieren Sie diesen Netzwerkparameter nicht.

```
# 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
```

Weitere Informationen erhalten Sie unter „_rev_src_routes“ in *Oracle Solaris Tunable Parameters Reference Manual*.

7 **Legen Sie die Eigenschaft für das Ignorieren von Umleitungen auf 0 für IP-Pakete fest und überprüfen Sie den aktuellen Wert.**

Durch den Standardwert wird zusätzlicher CPU-Bedarf in Systemen unterbunden. Bei einer guten Netzwerkplanung sind Umleitungen normalerweise nicht nötig.

```
# 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
```

Siehe auch Manpage `ipadm(1M)`

Schutz von Dateisystemen und Dateien

Das ZFS-Dateisystem ist nicht komplex und kann verschlüsselt, komprimiert sowie mit reserviertem Speicher und Festplattenspeicherbegrenzung konfiguriert werden.

Die folgenden Aufgaben bieten einen Einblick in die verfügbaren Schutzfunktionen von ZFS, dem Standarddateisystem unter Oracle Solaris. Weitere Informationen finden Sie unter „Setting ZFS Quotas and Reservations“ in *Oracle Solaris Administration: ZFS File Systems* und auf der Manpage `zfs(1M)`.

Aufgabe	Beschreibung	Anweisungen siehe
Wenden Sie DoS-Angriffe durch Verwalten und Reservieren des Speicherplatzes ab.	Gibt die Nutzung von Speicherplatz durch Dateisysteme, Benutzer oder Projekte an.	„Setting ZFS Quotas and Reservations“ in *Oracle Solaris Administration: ZFS File Systems*
Garantieren Sie eine Mindestmenge an Speicherplatz für einen Datensatz und dessen untergeordnete Datensätze.	Gewährleistet Speicherplatz nach Dateisystemen, Benutzern, Gruppen oder Projekten.	„Setting Reservations on ZFS File Systems“ in *Oracle Solaris Administration: ZFS File Systems*
Verschlüsseln Sie Daten in einem Dateisystem.	Bietet Schutz für einen Datensatz durch Verschlüsselung und Kennsatz, sodass auf den Datensatz bei seiner Erstellung zugegriffen werden kann.	„Encrypting ZFS File Systems“ in *Oracle Solaris Administration: ZFS File Systems* „Examples of Encrypting ZFS File Systems“ in *Oracle Solaris Administration: ZFS File Systems*
Geben Sie ACLs an für einen Dateischutz auf einer feiner abgestimmten Ebene, als es mit UNIX-Dateiberechtigungen möglich ist.	Erweiterte Sicherheitsattribute können sich beim Schutz von Dateien als hilfreich erweisen. Informationen zur Verwendung von ACLs siehe 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`)

Dateischutz und -änderungen

Systemdateien können nur in der `root`-Rolle geändert werden.

Aufgabe	Beschreibung	Anweisungen siehe
Konfigurieren Sie restriktive Dateiberechtigungen für normale Benutzer.	Hierdurch wird ein restriktiverer Wert als `022` für Dateiberechtigungen der normalen Benutzer festgelegt.	„Festlegen eines restriktiveren `umask`-Werts für normale Benutzer“ auf Seite 35
Unterbinden Sie die Ersetzung von Systemdateien durch Rogue-Dateien.	Sucht nach Rogue-Dateien über ein Skript oder BART.	„How to Find Files With Special File Permissions“ in *Oracle Solaris Administration: Security Services*

Schutz von Anwendungen und Services

Sie können Oracle Solaris-Sicherheitsfunktionen so konfigurieren, dass Ihre Anwendungen geschützt sind.

Erstellen von Zonen für die Aufnahme wichtiger Anwendungen

Bei Zonen handelt es sich um Container, die Prozesse isolieren. Für Anwendungen und Anwendungskomponenten sind diese Container hilfreich. Beispiel: Zonen können eingesetzt werden, um die Datenbank einer Website vom Webserver der Site zu trennen.

Informationen und Anweisungen:

- Kapitel 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*.
- Kapitel 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`*)*

Ressourcenverwaltung in Zonen

Zonen bieten eine Reihe von Tools zur Verwaltung von Zonenressourcen.

Informationen und Anweisungen:

- Kapitel 14, „Resource Management Configuration Example“ in *Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management*
- Teil I, „Oracle Solaris Resource Management“ in *Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management*

Konfigurieren von IPsec und IKE

Durch IPsec und IKE werden Netzwerkübertragungen zwischen Knoten und Netzwerken geschützt, die gemeinsam mit IPsec und IKE konfiguriert werden.

Informationen und Anweisungen:

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

Konfigurieren von IP Filter

Die IP Filter-Funktion umfasst eine Firewall.

Informationen und Anweisungen:

- Kapitel 20, „IP Filter in Oracle Solaris (Overview)“ in *Oracle Solaris Administration: IP Services*
- Kapitel 21, „IP Filter (Tasks)“ in *Oracle Solaris Administration: IP Services*

Konfigurieren von Kerberos

Sie können Ihr Netzwerk mithilfe des Kerberos-Service schützen. Durch diese Client-Server-Architektur werden Netzwerktransaktionen geschützt. Der Service bietet Authentifizierung über sichere Passwörter, Integrität und Vertraulichkeit. Mit dem Kerberos-Service können Sie sich sicher bei anderen Rechnern anmelden, Befehle ausführen, Daten austauschen und Dateien übertragen. Darüber hinaus können Administratoren mithilfe des Service den Zugriff auf Services und Systeme einschränken. Als Kerberos-Benutzer können Sie den Zugriff anderer Personen auf Ihr Konto regulieren.

Informationen und Anweisungen:

- Kapitel 20, „Planning for the Kerberos Service“ in *Oracle Solaris Administration: Security Services*
- Kapitel 21, „Configuring the Kerberos Service (Tasks)“ in *Oracle Solaris Administration: Security Services*
- Manpages `kadmin`(1M), `pam_krb5`(5) und `kclient`(1M)

Hinzufügen von SMF zu einem veralteten Service

Sie können die Anwendungskonfiguration auf vertrauenswürdige Benutzer oder Rollen einschränken, indem Sie die Anwendung der SMF-Funktion (Service Management Facility) von Oracle Solaris hinzufügen.

Informationen und Anweisungen:

- „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`).
- Manpages `smf`(5), `smf_security`(5), `svcadm`(1M) und `svccfg`(1M)

Erstellen eines BART-Schnappschusses des Systems

Nach Abschluss der Systemkonfiguration können Sie mindestens ein BART-Manifest erstellen. Ein solches Manifest enthält einen Schnappschuss des Systems. Sie können in regelmäßigen Abständen Schnappschüsse erstellen und sie vergleichen. Weitere Informationen dazu erhalten Sie unter „Basic Audit Reporting Tool – Verwendung“ auf Seite 53.

Hinzufügen einer mehrstufigen (gekennzeichneten) Sicherheit

Trusted Extensions erweitert die Oracle Solaris-Sicherheit, indem eine obligatorische MAC-Richtlinie (Mandatory Access Control) durchgesetzt wird. Empfindlichkeitsbezeichnungen werden automatisch auf alle Datenquellen (Netzwerke, Dateisysteme und Fenster) und Datennutzer (Benutzer und Prozesse) angewendet. Die Einschränkung des Dateizugriffs richtet sich nach der Beziehung zwischen der Datenbezeichnung (Objekt) und dem Nutzer (Subjekt). Die mehrschichtige Funktionalität besteht aus einer Reihe von Bezeichnungen erkennenden Services.

Dazu gehören u. a. folgende Trusted Extensions-Services:

- Gekennzeichnetes Netzwerk
- Bezeichnungen erkennendes Einhängen und gemeinsame Nutzung von Dateisystemen
- Gekennzeichneter Desktop
- Bezeichnungskonfiguration und -übersetzung
- Bezeichnungen erkennende Systemverwaltungstools
- Zuweisung von Bezeichnungen erkennenden Geräten

Die Pakete `group/feature/trusted-desktop` bieten die vertrauenswürdige Desktop-Umgebung mit mehreren Ebenen von Oracle Solaris.

Konfiguration von Trusted Extensions

Sie müssen zuerst die Trusted Extensions-Pakete installieren und anschließend das System konfigurieren. Nach der Installation der Pakete kann das System einen Desktop mit einem direkt angeschlossenem Bitmapdisplay (Laptop oder Workstation) ausführen. Ein konfiguriertes Netzwerk ist für die Kommunikation mit anderen Systemen erforderlich.

Informationen und Anweisungen:

- Teil I, „Initial Configuration of Trusted Extensions“ in *Trusted Extensions Configuration and Administration*
- Teil II, „Administration of Trusted Extensions“ in *Trusted Extensions Configuration and Administration*

Konfigurieren von Labeled IPsec

Sie können Ihre gekennzeichneten Pakete mit IPsec schützen.

Informationen und Anweisungen:

- Kapitel 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*

◆ ◆ ◆ KAPITEL 3

Überwachen und Verwalten der Oracle Solaris 11-Sicherheitsfunktionen

Oracle Solaris bietet zwei Systemtools zur Überwachung der Sicherheit: BART (Basic Audit Reporting Tool) und den Prüfservice. Auch einzelne Programme und Anwendungen können Zugangs- und Verwendungsprotokolle erstellen.

Basic Audit Reporting Tool – Verwendung

BART-Manifeste liefern einen statischen Bericht über das, was auf Ihrem System installiert wurde. Die BART-Manifeste können über einen längeren Zeitraum systemübergreifend verglichen werden, um Änderungen an installierten Systemen und Unterschiede zwischen verschiedenen Systemen nachzuvollziehen.

Informationen und Anweisungen:

- „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*

Anweisungen zum Nachverfolgen von Änderungen an installierten Systemen finden Sie unter „How to Compare Manifests for the Same System Over Time“ in *Oracle Solaris Administration: Security Services*.

Verwenden des Prüfservice

Bei der Prüfung werden Details zu der Art und Weise aufgezeichnet, in der das System verwendet wurde. Der Prüfservice bietet Tools für die Analyse der Prüfdaten.

Eine Erläuterung des Prüfservices finden Sie unter Teil VII, „Auditing in Oracle Solaris“ in *Oracle Solaris Administration: Security Services*.

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

  Eine Liste der Manpages und der dazugehörigen Links finden Sie unter „Audit Service Man Pages“ in *Oracle Solaris Administration: Security Services*.

Die folgenden Prüfserviceanweisungen können zur Erfüllung Ihrer Standortanforderungen beitragen:

- Erstellen Sie separate Rollen, um die Prüfung zu konfigurieren und einzusehen sowie den Prüfservice zu starten oder zu beenden.

  Verwenden Sie die Rechteprofile "Audit Configuration", "Audit Review" und "Audit Control" als Grundlage für Ihre Rollen.

  Informationen zum Erstellen von Rollen finden Sie unter „How to Create a Role“ in *Oracle Solaris Administration: Security Services*.
- Überwachen Sie Textzusammenfassungen überprüfter Ereignisse im `syslog`-Dienstprogramm.

  Aktivieren Sie das Plug-in `audit_syslos` und überwachen Sie dann die aufgezeichneten Ereignisse.

  Nähere Informationen hierzu finden Sie unter „How to Configure syslog Audit Logs“ in *Oracle Solaris Administration: Security Services*.
- Legen Sie Maximalgrößen für die Prüfdateien fest.

  Legen Sie dazu das Attribut `p_fsize` für das Plug-in `audit_binfile` auf eine angemessene Größe fest. Berücksichtigen Sie neben anderen Faktoren vor allem Ihren Zeitplan für die Einsicht der Prüfdateien, den verfügbaren Festplattenspeicher und die `cron`-Ausführungshäufigkeit.

  Beispiele finden Sie unter „How to Assign Audit Space for the Audit Trail“ in *Oracle Solaris Administration: Security Services*.
- Bereiten Sie die sichere Übertragung kompletter Prüfdateien in ein Dateisystem für die Dateieinsicht auf einem separaten ZFS-Pool vor.
- Sehen Sie die kompletten Prüfdateien in diesem Dateisystem ein.

Überwachen von audit_syslog-Prüfzusammenfassungen

Mit dem Plug-in `audit_syslog` können Sie Zusammenfassungen zuvor ausgewählter Prüfereignisse aufzeichnen.

Die Prüfzusammenfassungen können in einem Terminalfenster angezeigt werden, da sie durch das Ausführen eines Befehls erzeugt werden, der in etwa dem folgenden gleichkommt:

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

Einsehen und Archivieren der Prüfprotokolle

Prüfprotokolle können im Textformat oder in einem Browser im XML-Format angezeigt werden.

Informationen und Anweisungen:

- „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*

Aufspüren von Rogue-Dateien

Sie können die möglicherweise unberechtigte Verwendung der Berechtigungen `setuid` und `setgid` für Programme lokalisieren. Eine verdächtige ausführbare Datei räumt einem Benutzer statt einem Systemkonto Eigentumsrechte wie `root` oder `bin` ein.

Nähere Information zur Vorgehensweise sowie ein Beispiel finden Sie unter „How to Find Files With Special File Permissions“ in *Oracle Solaris Administration: Security Services*.

◆ ◆ ◆ ANHANG A

Literaturverzeichnis zur Oracle Solaris-Sicherheit

Folgende Referenzen enthalten hilfreiche Informationen zum Thema Sicherheit auf Oracle Solaris-Systemen. Die Informationen zur Sicherheit aus früheren Oracle Solaris-Versionen sind hilfreich, aber möglicherweise nicht mehr auf dem neuesten Stand.

Oracle Solaris 11-Referenzen

Folgende Handbücher und Artikel enthalten Beschreibungen zur Sicherheit auf Oracle Solaris 11-Systemen:

- *Oracle Solaris Administration: Security Services*

  Dieses Sicherheitshandbuch wurde von Oracle für Oracle Solaris 11-Administratoren veröffentlicht. Darin werden die Sicherheitsfunktionen Oracle Solaris und deren Verwendung bei der Systemkonfiguration beschrieben. Im Vorwort sind Links zu anderen Oracle Solaris-Systemadministrationshandbüchern aufgeführt, in denen das Thema Sicherheit behandelt wird.

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

  In diesem Artikel ist ein Schnappschuss der Oracle Solaris-Sicherheitsfunktionen für diese Version (Stand November 2010) enthalten.

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

  Dieser Artikel beinhaltet einen Schnappschuss der Oracle Solaris-Funktionen für diese Version (Stand November 2010).

Empfehlenswerte Oracle Solaris 10-Referenzen finden Sie in *Oracle Solaris 10 Security Guidelines*.