Oracle® Solaris 11 – Sicherheitsbestimmungen

Teilenr.: E36474–05
September 2013

130926@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 UNIX-Standardeingabeaufforderung und die Superuser-Eingabeaufforderung für Shells, die zum Betriebssystem Oracle Solaris gehören. In Befehlbeispielen zeigen die Shell-Eingabeaufforderungen an, ob der Befehl von einem regulären Benutzer oder einem Benutzer mit bestimmten Berechtigungen ausgeführt werden sollte.

TABELLE P–2 Shell-Eingabeaufforderungen

Shell	Eingabeaufforderung
Bash-Shell, Korn-Shell und Bourne-Shell	$

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

Shell	Eingabeaufforderung
Bash-Shell, Korn-Shell und Bourne-Shell für Superuser	`#`
C-Shell	`machine_name%`
C-Shell für Superuser	`machine_name#`

◆ ◆ ◆ KAPITEL 1

1 Übersicht über die Oracle Solaris-Sicherheitsfunktionen

Oracle Solaris 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 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 -Sicherheitsschutzmechanismen

Oracle Solaris bietet Stabilität für Unternehmensdaten und Anwendungen durch Schutz von gespeicherten und übertragenen Daten. Oracle Solaris 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.
- Arbeitsspeicherschutz – Adressraumlayout wird für Userland-Prozesse zufällig angeordnet.
- 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-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.

Zufällige Anordnung des Adressraumlayouts

Die zufällige Anordnung des Adressraumlayouts (ASLR) ordnet die Adressen, die von einem vorgegebenen Binärcode verwendet werden zufällig an. ASLR kann bestimmten Angriffsarten, die auf der exakten Speicherortkenntnis bestimmter Speicherbereiche basieren, vorbeugen und bereits den Versuch erkennen, wenn das ausführbare Programm gestoppt wird. Weitere Informationen erhalten Sie unter „Address Space Layout Randomization“ in *Oracle Solaris 11.1 Administration: Security Services*.

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 11.1 Administration: Security Services*.
- Richtlinien finden Sie unter „Wichtige Ereignisse außer Anmelden/Abmelden prüfen“ auf Seite 38 und auf den Manpages.
- Eine Übersicht über das Prüfungsverfahren finden Sie in Kapitel 26, „Auditing (Overview)“ in *Oracle Solaris 11.1 Administration: Security Services*.
- Prüfaufgaben finden Sie in Kapitel 28, „Managing Auditing (Tasks)“ in *Oracle Solaris 11.1 Administration: Security Services*.

Überprüfung der BART-Datei

Die BART-Funktion 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)
- Weitere Informationen zu Richtlinien erhalten Sie unter „Erstellen eines BART-Schnappschusses des Systems“ auf Seite 49, „Die Dateiintegrität mittels BART überprüfen.“ auf Seite 51 und in den Manpages.
- Eine Übersicht über BART finden Sie in Kapitel 6, „Verifying File Integrity by Using BART (Tasks)“ in *Oracle Solaris 11.1 Administration: Security Services*.
- Anwendungsbeispiele zu BART finden Sie unter „Using BART (Tasks)“ in *Oracle Solaris 11.1 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 11.1 Administration: Security Services* und Kapitel 13, „Key Management Framework“ in *Oracle Solaris 11.1 Administration: Security Services*.
- Anwendungsbeispiele zum Cryptographic Framework finden Sie in Kapitel 12, „Cryptographic Framework (Tasks)“ in *Oracle Solaris 11.1 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 11.1 Administration: Security Services*.
- Eine Übersicht und Beispiele für den Schutz von ZFS-Dateien finden Sie in Kapitel 7, „Using ACLs and Attributes to Protect Oracle Solaris ZFS Files“ in *Oracle Solaris 11.1 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 4, „IP Filter in Oracle Solaris (Overview)“ in *Securing the Network in Oracle Solaris 11.1*.
- Anwendungsbeispiele zu IP Filter finden Sie in Kapitel 5, „IP Filter (Tasks)“ in *Securing the Network in Oracle Solaris 11.1* 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 Netzwerkservices, die mit einer Zugriffskontrolle belegt werden können, gehören `proftpd` 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:

- Weitere Informationen über TCP-Wrapper erhalten Sie unter „How to Use TCP Wrappers to Control Access to TCP Services“ in *Configuring and Administering Oracle Solaris 11.1 Networks*.
- 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 11.1 Administration: Security Services*
- „Securing Logins and Passwords (Tasks)“ in *Oracle Solaris 11.1 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 Pluggable Authentication Modules“ in *Oracle Solaris 11.1 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 11.1 Administration: Security Services*
- „Using Privileges (Tasks)“ in *Oracle Solaris 11.1 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 6, „IP Security Architecture (Overview)“ in *Securing the Network in Oracle Solaris 11.1*
- Kapitel 7, „Configuring IPsec (Tasks)“ in *Securing the Network in Oracle Solaris 11.1*
- Kapitel 9, „Internet Key Exchange (Overview)“ in *Securing the Network in Oracle Solaris 11.1*
- Kapitel 10, „Configuring IKE (Tasks)“ in *Securing the Network in Oracle Solaris 11.1*
- 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 11.1 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 11.1 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 11.1 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 1, „Managing Services (Overview)“ in *Managing Services and Faults in Oracle Solaris 11.1*
- Kapitel 2, „Managing Services (Tasks)“ in *Managing Services and Faults in Oracle Solaris 11.1*
- 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, und eine Verschlüsselung der gesamten Datengruppe ist bereits bei ihrer Erstellung möglich. RBAC unterstützt die delegierte Administration von ZFS-Datensätzen.

Weitere Informationen finden Sie hier:

- Kapitel 1, „Oracle Solaris ZFS File System (Introduction)“ in *Oracle Solaris 11.1 Administration: ZFS File Systems*
- „Oracle Solaris ZFS and Traditional File System Differences“ in *Oracle Solaris 11.1 Administration: ZFS File Systems*
- Kapitel 5, „Managing Oracle Solaris ZFS File Systems“ in *Oracle Solaris 11.1 Administration: ZFS File Systems*
- „How to Remotely Administer ZFS With Secure Shell“ in *Oracle Solaris 11.1 Administration: Security Services*
- 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. Unter Oracle Solaris 11 können Sie eine schreibgeschützte Zonen-Root konfigurieren.

Weitere Informationen finden Sie hier:

- „Configuring Read-Only Zones“ in *Oracle Solaris 11.1 Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management*
- Teil II, „Oracle Solaris Zones“ in *Oracle Solaris 11.1 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 sechs Zeichen umfassen und mindestens zwei Buchstaben und ein nicht alphabetisches Zeichen 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 22). 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.

Oracle Solaris 11 Sicherheitsevaluierung

Oracle Solaris 11 wird derzeit vom Canadian Common Criteria Scheme (CCCS) gemäß Common Criteria Evaluation Assurance Level 4 (EAL4) *evaluiert* - erweitert auf EAL4+ um die Prozesse zur Schwachstellenbehebung ("Flaw Remediation"). EAL4+ stellt die höchste Evaluationsstufe dar, die kommerzielle Software erreichen kann. Ebenso stellt EAL4 die höchste Evaluationsstufe dar, die gemeinsam von 26 Ländern gemäß dem Common Criteria Recognition Arrangement (CCRA) anerkannt wird.

Die Evaluierung wird gegen das Operating System Protection Profile (OS PP) ausgeführt und beinhaltet die folgenden vier optionalen Erweiterungspakete:

- Advanced Management (AM)
- Extended Identification and Authentication (EIA)
- Labeled Security (LS)
- Virtualization (VIRT)

Hinweis – Sich im Prozess der *Evaluierung* zu befinden, bedeutet nicht automatisch, dass man die Sicherheitszertifizierung auch erhalten wird.

Weitere Informationen zur Evaluierung erhalten Sie unter:

- Oracle Security Evaluations (`http://www.oracle.com/technetwork/topics/security/security-evaluations-099357.html`)
- The Common Criteria Recognition Arrangement (`http://www.commoncriteriaportal.org/ccra/`)
- Products in Evaluation (`http://www.cse-cst.gc.ca/its-sti/services/cc/oe-pece-eng.html`)
- Operating System Protection Profile (`http://www.commoncriteriaportal.org/files/ppfiles/pp0067b_pdf.pdf`)

Standortsicherheitsrichtlinien und deren Umsetzung

Für ein sicheres System oder Netzwerk von Systemen sind eine Sicherheitsrichtlinie und entsprechende Sicherheitsanforderungen unabdingbar. Wenn Sie Programme entwickeln oder Programme anderer Hersteller installieren, müssen Sie diesbezüglich Sicherheit gewährleisten.

Weitere Informationen finden Sie hier:

- Anhang A, „Secure Coding Guidelines for Developers“ in *Developer's Guide to Oracle Solaris 11 Security*
- 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-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 folgendermaßen:

- **Oracle Solaris Large Server –** Durch das Standardmanifest in einer AI-Installation (Automated Installer) und durch 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 Desktopserver 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 einer automatisierten Installation mithilfe des AI (Automated Installer) erhalten Sie unter Teil III, „Installing Using an Install Server“ in *Installing Oracle Solaris 11.1 Systems*.

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

- *Installing Oracle Solaris 11.1 Systems*
- *Creating a Custom Oracle Solaris 11.1 Installation Image*
- *Adding and Updating Oracle Solaris 11.1 Software Packages*

Systemsicherung

Sie sollten die Schritte in der vorgegebenen Reihenfolge durchführen. Zu diesem Zeitpunkt ist das Oracle Solaris-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.	„Pakete überprüfen“ auf Seite 29
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 11.1 Administration: Security Services*
3. Deaktivieren nicht erforderlicher Services	Prozesse, die für den Systemablauf nicht erforderlich sind, werden nicht ausgeführt.	„Nicht erforderliche Services deaktivieren“ auf Seite 29

Aufgabe	Beschreibung	Anweisungen siehe
5. Kein Ausschalten des Systems durch den Eigentümer der Workstation	Dadurch soll vermieden werden, dass der Konsolenbenutzer das System ausschaltet oder anhält.	„Energieverwaltungsfunktion für Benutzer entfernen“ auf Seite 30
6. Erstellen Sie eine Anmeldewarnmeldung gemäß Ihrer Standortsicherheitsrichtlinie.	Benutzer und potenzielle Angreifer werden benachrichtigt, dass das System überwacht wird.	„Sicherheitsmeldung zu allen Bannerdateien hinzufügen“ auf Seite 31 „Sicherheitsmeldung in den Desktop-Anmeldebildschirm einfügen“ auf Seite 31

▼ Pakete überprüfen

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

Bevor Sie beginnen Sie müssen die `root`-Rolle übernehmen. Weitere Informationen finden Sie unter „How to Use Your Assigned Administrative Rights“ in *Oracle Solaris 11.1 Administration: Security Services*.

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`.

▼ Nicht erforderliche Services deaktivieren

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. Weitere Informationen finden Sie unter „How to Use Your Assigned Administrative Rights“ in *Oracle Solaris 11.1 Administration: Security Services*.

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 1, „Managing Services (Overview)“ in *Managing Services and Faults in Oracle Solaris 11.1* und auf der Manpage `svcs`(1).

▼ Energieverwaltungsfunktion für Benutzer entfernen

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

Bevor Sie beginnen Sie müssen die `root`-Rolle übernehmen. Weitere Informationen finden Sie unter „How to Use Your Assigned Administrative Rights“ in *Oracle Solaris 11.1 Administration: Security Services*.

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 a Rights Profile“ in *Oracle Solaris 11.1 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 11.1 Administration: Security Services* sowie auf den Manpages `policy.conf`(4) und `usermod`(1M).

▼ Sicherheitsmeldung zu allen Bannerdateien hinzufügen

Führen Sie diese Schritte durch, um Sicherheitsmeldungen in zwei Bannerdateien zu erstellen, die Ihrer Standortsicherheitsrichtlinie entsprechen. Der Inhalt dieser Bannerdateien 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. Es empfiehlt sich, den Inhalt der Sicherheitsmeldung mit dem Rechtsberater im Unternehmen zu besprechen.

Bevor Sie beginnen Sie müssen Administrator mit dem zugewiesenen Rechteprofil "Administrator Message Edit" sein. Weitere Informationen finden Sie unter „How to Use Your Assigned Administrative Rights“ in *Oracle Solaris 11.1 Administration: Security Services*.

1 Fügen Sie der Datei `/etc/issue` eine Sicherheitsmeldung hinzu.

```
$ pfedit /etc/issue
      ALERT   ALERT   ALERT   ALERT   ALERT

This machine is available to authorized users only.

If you are an authorized user, continue.

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

Der `login`-Befehl zeigt den Inhalt von `/etc/issue` vor der Authentifizierung an, so wie es auch die `telnet`- und FTP-Services tun. Weitere Informationen dazu, wie auch andere Anwendungen diese Datei nutzen können, finden Sie unter „Sicherheitsmeldung für Benutzern anzeigen, die sich mit dem Befehl `ssh` anmelden.“ auf Seite 42 und „Sicherheitsmeldung in den Desktop-Anmeldebildschirm einfügen“ auf Seite 31.

Weitere Informationen finden Sie auf den Manpages `issue(4)` und `pfedit(1M)`.

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

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

In Oracle Solaris zeigt die ursprüngliche Shell des Benutzers den Inhalt der `/etc/motd`-Datei an.

▼ Sicherheitsmeldung in den Desktop-Anmeldebildschirm einfügen

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. Es empfiehlt sich, den Inhalt der Sicherheitsmeldung mit dem Rechtsberater im Unternehmen zu besprechen.

Bevor Sie beginnen Zu Erstellung einer Datei müssen Sie die `root`-Rolle annehmen. Um bereits vorhandene Datei ändern zu können, müssen Sie ein Administrator mit zugewiesener `solaris.admin.edit/`*path-to-existing-file*-Autorisierung sein.

- **Fügen Sie eine Sicherheitsmeldung in den Desktopanmeldebildschirm ein, indem Sie eine der drei nachfolgenden Optionen auswählen:**

  Die Optionen, mit denen ein Dialogfeld erstellt wird, verwenden möglicherweise die Sicherheitsmeldung der Datei `/etc/issue` aus Schritt 1 von „Sicherheitsmeldung zu allen Bannerdateien hinzufügen“ auf Seite 31.

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

    ```
    # pfedit /usr/share/gdm/autostart/LoginWindow/banner.desktop
    [Desktop Entry]
    Type=Application
    Name=Banner Dialog
    Exec=/usr/bin/zenity --text-info --width=800 --height=300 \
    --title="Security Message" \
    --filename=/etc/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.**

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

Weitere Informationen über die Bearbeitung von Systemdateien als Nicht-root-Benutzer erhalten Sie über die Manpage pfedit(1M).

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

```
$ pfedit /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) Speichern Sie eine Kopie der geänderten Benutzeroberfläche des Anmeldebildschirms.

```
# 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.

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

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.	„Striktere Passwortbeschränkungen festlegen“ auf Seite 35
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 37
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.	„Kontosperre für normale Benutzer festlegen“ auf Seite 36
Treffen Sie eine Vorauswahl zusätzlicher Prüfklassen.	Auf diese Weise können Sie potenzielle Bedrohungen des Systems überwachen und aufzeichnen.	„Wichtige Ereignisse außer Anmelden/Abmelden prüfen“ auf Seite 38
Senden Sie Zusammenfassungen von Prüfereignissen in Textform an das Dienstprogramm `syslog`.	Enthält in Echtzeit aufgezeichnete, wichtige Prüfereignisse wie Anmeldungen und Anmeldeversuche.	„`lo`-Ereignisse in Echtzeit überwachen.“ auf Seite 39

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 and Managing User Accounts by Using the CLI“ in *Managing User Accounts and User Environments in Oracle Solaris 11.1* „How to Create a Role“ in *Oracle Solaris 11.1 Administration: Security Services* „How to Assign a Role“ in *Oracle Solaris 11.1 Administration: Security Services*
Verringern Sie die Anzahl der sichtbaren GNOME-Desktopanwendungen.	Dadurch wird vermieden, dass Benutzer Desktopanwendungen benutzen, die die Sicherheit beeinträchtigen können.	Siehe Kapitel 11, „Disabling Features in the Oracle Solaris Desktop System“ in *Oracle Solaris 11.1 Desktop Administrator's Guide*.
Schränken Sie Benutzerrechte ein.	Dadurch werden die Basisberechtigungen entfernt, die Benutzer nicht benötigen.	„Nicht benötigter Basisberechtigungen von Benutzern entfernen“ auf Seite 40

▼ Striktere Passwortbeschränkungen festlegen

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. Weitere Informationen finden Sie unter „How to Use Your Assigned Administrative Rights“ in *Oracle Solaris 11.1 Administration: Security Services*.

- **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 22.
- Manpage `passwd(1)`

▼ Kontosperre für normale Benutzer festlegen

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

Legen Sie keinen systemweiten Schutz fest auf einem System, das Sie für administrative Aufgaben nutzen.

Sie müssen die `root`-Rolle übernehmen. Weitere Informationen finden Sie unter „How to Use Your Assigned Administrative Rights“ in *Oracle Solaris 11.1 Administration: Security Services*.

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

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

```
# pfedit /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.**

   ```
   # pfedit /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 11.1 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. Weitere Informationen finden Sie unter „How to Use Your Assigned Administrative Rights“ in *Oracle Solaris 11.1 Administration: Security Services*.

- **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 026` – bietet maßvollen Dateischutz

    (`741`) – `r` für Gruppe, x für andere
  - `umask 027` – bietet hohen Dateischutz

    (`740`) – `r` für Gruppe, kein Zugriff für andere Personen
  - `umask 077` – bietet kompletten Dateischutz

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

Siehe auch

Weitere Informationen finden Sie hier:

- „Setting Up and Managing User Accounts by Using the CLI“ in *Managing User Accounts and User Environments in Oracle Solaris 11.1*

- „Default umask Value“ in *Oracle Solaris 11.1 Administration: Security Services*
- Manpages `usermod`(1M) und `umask`(1)

▼ Wichtige Ereignisse außer Anmelden/Abmelden prüfen

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. Weitere Informationen finden Sie unter „How to Use Your Assigned Administrative Rights“ in *Oracle Solaris 11.1 Administration: Security Services*.

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 11.1 Administration: Security Services*.
- Beispiele für das Festlegen von Prüf-Flags finden Sie unter „Configuring the Audit Service (Tasks)“ in *Oracle Solaris 11.1 Administration: Security Services* und unter „Troubleshooting the Audit Service (Tasks)“ in *Oracle Solaris 11.1 Administration: Security Services*.
- Informationen zum Konfigurieren von Prüfungen erhalten Sie auf der Manpage `auditconfig`(1M).

▼ lo-Ereignisse in Echtzeit überwachen.

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. Weitere Informationen finden Sie unter „How to Use Your Assigned Administrative Rights“ in *Oracle Solaris 11.1 Administration: Security Services*.

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

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

2. **Prüfen Sie, welche `system-log`-Serviceinstanz online ist.**

   ```
   # svcs system-log
   STATE          STIME    FMRI
   disabled       13:11:55 svc:/system/system-log:rsyslog
   online         13:13:27 svc:/system/system-log:default
   ```

   Tipp – Wenn die `rsyslog`-Serviceinstanz online ist, ändern Sie die `rsyslog.conf`-Datei.

3. **Fügen Sie den Eintrag `audit.notice` zur Datei `syslog.conf` hinzu.**

   Der Standardeintrag enthält den Speicherort der Protokolldatei.

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

4. **Erstellen Sie die Protokolldatei.**

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

5. **Aktualisieren Sie die Konfigurationsinformationen für den `system-log`-Service.**

   ```
   # svcadm refresh system-log:default
   ```

   Hinweis – Aktualisieren Sie die `system-log:rsyslog`-Serviceinstanz, wenn der `rsyslog`-Service online ist.

6. **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 11.1 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 53.

▼ Nicht benötigter Basisberechtigungen von Benutzern entfernen

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. Weitere Informationen finden Sie unter „How to Use Your Assigned Administrative Rights“ in *Oracle Solaris 11.1 Administration: Security Services*.

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 11.1 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 11.1 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 *Troubleshooting Typical Issues in Oracle Solaris 11.1* „Managing Core Files (Task Map)“ in *Troubleshooting Typical Issues in Oracle Solaris 11.1*

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 Benutzern anzeigen, die sich mit dem Befehl `ssh` anmelden.“ auf Seite 42
Deaktivieren Sie den Netzwerkrouting-Dämon.	Dadurch wird der Zugriff auf das System durch potenzielle Netzwerk-Snooper eingeschränkt.	„How to Disable the Network Routing Daemon“ in *Securing the Network in Oracle Solaris 11.1*
Unterbinden Sie die Verteilung von Informationen zur Netzwerktopologie.	Der Broadcast von Paketen wird verhindert.	„How to Disable Broadcast Packet Forwarding“ in *Securing the Network in Oracle Solaris 11.1*
	Es wird nicht auf Broadcast- und Multicast-Echoanforderungen reagiert.	„How to Disable Responses to Echo Requests“ in *Securing the Network in Oracle Solaris 11.1*

Aufgabe	Beschreibung	Anweisungen siehe
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.	„How to Set Strict Multihoming“ in *Securing the Network in Oracle Solaris 11.1*
Verhindern Sie DoS-Angriffe (Denial of Service) durch Kontrolle der Anzahl an unvollständigen Systemverbindungen.	Schränkt die zulässige Anzahl unvollständiger TCP-Verbindungen für einen TCP-Listener ein.	„How to Set Maximum Number of Incomplete TCP Connections“ in *Securing the Network in Oracle Solaris 11.1*
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.	„How to Set Maximum Number of Pending TCP Connections“ in *Securing the Network in Oracle Solaris 11.1*
Erstellen Sie sichere Zufallszahlen für TCP-Erstverbindungen.	Entspricht dem durch RFC 6528 angegebenen Sequenznummergenerierungswert.	„How to Specify a Strong Random Number for Initial TCP Connection“ in *Securing the Network in Oracle Solaris 11.1*
Setzen Sie die Netzwerkparameter auf ihre Standardeinstellungen zurück.	Dadurch wird die Sicherheit erhöht, die durch administrative Aktionen verringert wurde.	„How to Reset Network Parameters to Secure Values“ in *Securing the Network in Oracle Solaris 11.1*
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.	„So verwenden Sie TCP-Wrapper“ auf Seite 43

▼ Sicherheitsmeldung für Benutzern anzeigen, die sich mit dem Befehl `ssh` anmelden.

Führen Sie diese Schritte durch, um bei der Anmeldung mit dem `ssh`-Protokoll eine Warnung anzuzeigen.

Bevor Sie beginnen

Sie haben die Datei `/etc/issue` aus Schritt 1 von „Sicherheitsmeldung zu allen Bannerdateien hinzufügen“ auf Seite 31 erstellt.

Sie müssen Administrator mit zugewiesener `solaris.admin.edit/etc/ssh/sshd_config` -Autorisierung sein und über eines der Netzwerkrechteprofile verfügen. Die `root` -Rolle verfügt über alle diese Rechte. Weitere Informationen finden Sie unter „How to Use Your Assigned Administrative Rights“ in *Oracle Solaris 11.1 Administration: Security Services*.

- **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`.**

  ```
  $ pfedit /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)`, `sshd_config(4)`, und `pfedit(1M)`.

So verwenden Sie TCP-Wrapper

Die folgenden Schritte zeigen drei Arten, auf die TCP-Wrapper in Oracle Solaris verwendet werden oder verwendet werden können.

Bevor Sie beginnen Sie müssen Sie Rolle `root` annehmen, um ein Programm so zu ändern, dass TCP-Wrapper verwendet werden.

1. **Sie müssen die `sendmail`-Anwendung nicht mit TCP-Wrappern schützen.**

   Sie wird standardmäßig durch TCP-Wrapper geschützt, wie unter „Support for TCP Wrappers From Version 8.12 of sendmail“ in *Managing sendmail Services in Oracle Solaris 11.1* beschrieben.

2. **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 *Configuring and Administering Oracle Solaris 11.1 Networks*.**

3. **Schützen Sie den FTP-Netzwerkservice mit TCP-Wrappern.**

   a. **Befolgen Sie die Anweisungen im Modul `/usr/share/doc/proftpd/modules/mod_wrap.html`.**

   Da dieses Modul dynamisch ist, müssen Sie es laden, um TCP-Wrapper mit FTP zu verwenden.

b. Laden Sie das Modul, indem Sie die folgenden Anweisungen der Datei `/etc/proftpd.conf` hinzufügen:

```
<IfModule mod_dso.c>
    LoadModule mod_wrap.c
</IfModule>
```

c. Starten Sie den FTP-Service neu.

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

Schutz von Dateisystemen und Dateien

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

Das `tmpfs`-Dateisystem kann ohne Grenzen anwachsen. Um DoS-Attacken (Denial of Service) abzuwenden, vervollständigenSie „Die Größe des `tmpfs`-Dateisystems beschränken“ auf Seite 45.

Die folgenden Aufgaben konfigurieren eine Größenbeschränkung für `tmpfs` und 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 11.1 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 11.1 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 11.1 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 11.1 Administration: ZFS File Systems* „Examples of Encrypting ZFS File Systems“ in *Oracle Solaris 11.1 Administration: ZFS File Systems*

Aufgabe	Beschreibung	Anweisungen siehe
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`)
Beschränken Sie die Größe des `tmpfs`-Dateisystems.	Hält einen bösartigen Benutzer davon ab, große Dateien in `/tmp` zu erstellen und die Systemgeschwindigkeit zu verlangsamen.	„Die Größe des `tmpfs`-Dateisystems beschränken“ auf Seite 45

▼ Die Größe des tmpfs-Dateisystems beschränken

Die Größe des `tmpfs`-Dateisystems ist standardmäßig nicht beschränkt. Deshalb kann `tmpfs` anwachsen, um den verfügbaren Systemspeicher und Swap zu füllen. Da das `/tmp`-Verzeichnis von allen Anwendungen und Benutzern verwendet wird, ist es möglich, dass eine Anwendung den vollständigen Systemspeicher beansprucht. Gleichermaßen könnte ein nicht privilegierter Benutzer mit böswilliger Absicht zu einer Verringerung der Arbeitsgeschwindigkeit beitragen, indem er große Dateien im `/tmp`-Verzeichnis erstellt. Um Leistungseinbußen zu vermeiden, können Sie die Größe eines jeden `tmpfs`-Einhängevorgangs beschränken.

Probieren Sie mehrere verschiedene Werte aus, um die beste Systemleistung zu erreichen.

Bevor Sie beginnen Sie müssen die `root`-Rolle übernehmen. Weitere Informationen finden Sie unter „How to Use Your Assigned Administrative Rights“ in *Oracle Solaris 11.1 Administration: Security Services*.

1 Bestimmen Sie den Speicherplatz auf Ihrem System.

Hinweis – Das SPARC T3-System, das zur Veranschaulichung dieses Vorgangs (Beispiel) verwendet wird, verfügt über eine SSD-Festplatte (Solid State Disk) für schnellere E/A und hat acht Festplatten zu jeweils 279,40 MB. Das System verfügt über einen Speicher von 500 GB.

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

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

2 Berechnen Sie eine Speicherbeschränkung für `tmpfs`.

In Abhängigkeit von der Größe des Systemspeichers können Sie eine Speicherbeschränkung von etwa 20 Prozent für große und etwa 30 Prozent für kleinere Systeme berechnen.

Für ein kleineres System verwenden Sie folglich `.30` als Multiplikator.

```
10240M x .30 ≈ 340M
```

Für ein größeres System verwenden Sie `.20` als Multiplikator.

```
523776M x .20 ≈ 10475M
```

3 Erweitern Sie den `swap`-Eintrag der `/etc/vfstab` -Datei um die Größenbeschränkung.

```
# pfedit /etc/vfstab
#device       device       mount           FS      fsck    mount mount
#to mount     to fsck      point           type    pass    at boot options
#
/devices      -            /devices        devfs   -       no      -
/proc         -            /proc           proc    -       no      -
ctfs          -            /system/contract ctfs   -       no      -
objfs         -            /system/object  objfs   -       no      -
sharefs       -            /etc/dfs/sharetab  sharefs -    no      -
fd            -            /dev/fd         fd      -       no      -
swap          -            /tmp            tmpfs   -       yes     -
swap          -            tmpfs           -       yes     size=10400m
/dev/zvol/dsk/rpool/swap   -      -        swap    -       no      -
```

4 Starten Sie das System neu.

```
# reboot
```

5 Prüfen Sie, ob die Größenbeschränkung aktiviert ist.

```
# mount -v
swap on /system/volatile type tmpfs
read/write/setuid/devices/rstchown/xattr/dev=89c0006 on Fri Sep 7 14:07:27 2012
swap on /tmp type tmpfs
read/write/setuid/devices/rstchown/xattr/size=10400m/dev=89c0006 on Fri ...
```

6 Überwachen Sie die Speicherauslastung und passen Sie sie an die Anforderungen Ihrer Site an.

Der `df`-Befehl ist einigermaßen hilfreich. Der `swap`-Befehl bietet die nützlichsten Statistiken.

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

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

Weitere Informationen finden Sie auf den Manpages `tmpfs`(7FS), `mount_tmpfs`(1M), `df`(1M), und `swap`(1M).

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 37
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 11.1 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*.

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 11.1 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 6, „IP Security Architecture (Overview)“ in *Securing the Network in Oracle Solaris 11.1*
- Kapitel 9, „Internet Key Exchange (Overview)“ in *Securing the Network in Oracle Solaris 11.1*
- Kapitel 7, „Configuring IPsec (Tasks)“ in *Securing the Network in Oracle Solaris 11.1*
- Kapitel 10, „Configuring IKE (Tasks)“ in *Securing the Network in Oracle Solaris 11.1*

Konfigurieren von IP Filter

Die IP Filter-Funktion umfasst eine Firewall.

Informationen und Anweisungen:

- Kapitel 4, „IP Filter in Oracle Solaris (Overview)“ in *Securing the Network in Oracle Solaris 11.1*
- Kapitel 5, „IP Filter (Tasks)“ in *Securing the Network in Oracle Solaris 11.1*

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 11.1 Administration: Security Services*
- Kapitel 21, „Configuring the Kerberos Service (Tasks)“ in *Oracle Solaris 11.1 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 11.1 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 erhalten Sie unter „Die Dateiintegrität mittels BART überprüfen.“ auf Seite 51.

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 6, „IP Security Architecture (Overview)“ in *Securing the Network in Oracle Solaris 11.1*
- „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-Sicherheitsfunktionen

Oracle Solaris bietet zwei Systemtools zur Überwachung der Sicherheit: die BART-Funktion und den Prüfservice. Auch einzelne Programme und Anwendungen können Zugangs- und Verwendungsprotokolle erstellen.

Die Dateiintegrität mittels BART überprüfen.

BART ist ein regelbasiertes Tool zur Berichtserstellung und Dateiintegritätssuche, das kryptografische Prüfsummen und die Metadaten von Dateisystemen verwendet, um Änderungen festzuhalten.

Informationen und Anweisungen:

- „BART (Overview)“ in *Oracle Solaris 11.1 Administration: Security Services*
- „Using BART (Tasks)“ in *Oracle Solaris 11.1 Administration: Security Services*
- „BART Manifests, Rules Files, and Reports (Reference)“ in *Oracle Solaris 11.1 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 11.1 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 11.1 Administration: Security Services*.

- Kapitel 26, „Auditing (Overview)“ in *Oracle Solaris 11.1 Administration: Security Services*
- Kapitel 27, „Planning for Auditing“ in *Oracle Solaris 11.1 Administration: Security Services*
- Kapitel 28, „Managing Auditing (Tasks)“ in *Oracle Solaris 11.1 Administration: Security Services*
- Kapitel 29, „Auditing (Reference)“ in *Oracle Solaris 11.1 Administration: Security Services*

  Eine Liste der Manpages und der dazugehörigen Links finden Sie unter „Audit Service Man Pages“ in *Oracle Solaris 11.1 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 11.1 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 11.1 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 11.1 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 11.1 Administration: Security Services*
- „How to Prevent Audit Trail Overflow“ in *Oracle Solaris 11.1 Administration: Security Services*
- „Managing Audit Records on Local Systems (Tasks)“ in *Oracle Solaris 11.1 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 11.1 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-Referenzen

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

- *Oracle Solaris 11.1 Administration: Security Services*

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

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

  Diese Sicherheitsbenchmarks werden vom CIS (Center for Internet Security) veröffentlicht, dessen Sicherheitscommunity Sie unter `http://cisecurity.org/` finden können. Dieses Dokument enthält Empfehlungen zu Sicherheitseinstellungen für das Oracle Solaris. Sie richten sich an System- und Anwendungsadministratoren, Sicherheitsexperten, Auditors, Supporttechniker sowie Personen, die mit der Entwicklung, Installation, Tests oder mit der Bereitstellung von Sicherheitslösungen für Oracle Solaris betraut sind. Ein Exemplar können Sie unter CIS Security Benchmarks (`http://benchmarks.cisecurity.org/`) herunterladen.

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