Oracle® Solaris 11 - Sicherheitsbestimmungen

Teilenr.: E53926-02
Sep 2014

Inhalt

Tabellen

Verwendung dieser Dokumentation

- **Überblick** – Bietet einen Überblick über die Oracle Solaris-Sicherheitsfunktionen sowie Richtlinien, wie installierte Systeme und ihre Anwendungen mit ihnen geschützt und gesichert werden.
- **Zielgruppe** – Systemadministratoren, Sicherheitsadministratoren, Anwendungsentwickler und Prüfer, die Sicherheitsfunktionen auf Oracle Solaris 11-Systemen entwickeln, bereitstellen oder bewerten.
- **Benötigte Vorkenntnisse** – Standortsicherheitsanforderungen.

Produktdokumentationsbibliothek

Aktuelle Informationen und bekannte Probleme mit diesem Produkt finden Sie in der Dokumentationsbibliothek unter http://www.oracle.com/pls/topic/lookup?ctx=E56340.

Zugriff auf Oracle Support

Oracle-Kunden haben Zugriff auf elektronischen Support unter My Oracle Support. Besuchen Sie dazu die Website http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info bzw. die Website http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs für Hörgeschädigte.

Feedback

Unter http://www.oracle.com/goto/docfeedback können Sie uns Feedback zu dieser Dokumentation geben.

♦ ♦ ♦ KAPITEL 1

Sicherheit in Oracle Solaris

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.

Neue Sicherheitsfunktionen in Oracle Solaris 11.2

In diesem Abschnitt werden für bestehende Kunden Informationen zu wichtigen neuen Sicherheitsfunktionen in diesem Release erläutert.

- Sie können die Compliance Ihres System mit Sicherheitsstandards mithilfe des neuen Befehls `compliance` bewerten. Damit können Sie einschätzen und melden, inwieweit Ihr System mit den Sicherheitsstandards der Branche, einschließlich PCI-DSS, konform ist. Einzelheiten finden Sie im „Oracle Solaris 11.2 Handbuch zur Sicherheitscompliance “ sowie auf der Manpage `compliance`(1M).

- Die Cryptographic Framework-Funktion von Oracle Solaris wird in FIPS 140-2, Level 1 für Userland- und Kernel-Funktionen in den Oracle Solaris 11.1 SRU 5.5- und Oracle Solaris 11.1 SRU 3-Releases validiert.
  - Eine Liste der Oracle FIPS 140-validierten Produkte finden Sie in Oracle FIPS 140 Software Validations (http://www.oracle.com/technetwork/topics/security/fips140-software-validations-1703049.html).
  - Informationen zur Aktivierung von FIPS 140-Modus auf Ihrem System finden Sie in „Using a FIPS 140 Enabled System in Oracle Solaris 11.2 “.
- Oracle Solaris 11.1 ist für das kanadische Common Criteria Scheme zertifiziert. Siehe „Oracle Solaris 11 Common Criteria EAL4+-Zertifizierung“ [29]
- Mit dem Prüfservice können über Oracle Audit Vault Prüfdatensätze gespeichert, überprüft und analysiert werden. Siehe „Using Oracle Audit Vault and Database Firewall for Storage and Analysis of Audit Records“ in „Managing Auditing in Oracle Solaris 11.2 “.
- Durch die Funktion "Verified Boot" (geprüfter Startvorgang) wird der Startvorgang auf Oracle SPARC T5-Servern und Oracle SPARC T7-Servern vor Bedrohungen geschützt. Weitere Informationen finden Sie unter „Using Verified Boot“ in „Securing Systems and Attached Devices in Oracle Solaris 11.2 “.
- Sie können AI-Installationen (Automatic Installation) auf dem Installationsserver, auf bestimmten Clientsystemen, auf allen Clients eines bestimmten Installationsservice und auf sonstigen AI-Clients über Zertifikate und Schlüssel sichern. Bei einer sicheren AI-Installation wird die Übertragung von Oracle Solaris-Packages auf Ihre Systeme geschützt. Siehe „Increasing Security for Automated Installations“ in „Installing Oracle Solaris 11.2 Systems “.
- Ein neues Gruppeninstallationspackage ist verfügbar, `pkg:/group/system/solaris-minimal-server`. In „Oracle Solaris 11.2 Package Group Lists “ wird der Inhalt des Gruppenpackages beschrieben und verglichen.
- Sie können Kerberos-Clients über eine AI-Installation installieren, sodass das System beim ersten Hochfahren ein kerberisiertes System ist. Siehe „How to Configure Kerberos Clients Using AI“ in „Installing Oracle Solaris 11.2 Systems “.
- In diesem Release können physische globale Zonen, auch als unveränderbare globale Zonen (Immutable Global Zones) bezeichnet, sowie virtuelle globale Zonen, auch als Oracle Solaris Kernel-Zonen bezeichnet, schreibgeschützt sein. Unveränderbare globale Zonen bieten eine leicht bessere Sicherheit als Kernel-Zonen, keine von beiden können jedoch die Hardware oder die Konfiguration des Systems dauerhaft ändern. Schreibgeschützte Zonen können schneller hochgefahren werden und bieten mehr Sicherheit als Zonen ohne Schreibschutz.

  Über unveränderbare globale Zonen wird zu Verwaltungszwecken ein spezieller Satz an Prozessen, auch Trusted Computing Base (TCB) genannt, definiert, der über eine als Trusted Path bezeichnete geschützte Anmeldung konfiguriert werden kann. Weitere Informationen erhalten Sie in Kapitel 12, „Configuring and Administering Immutable Zones“ in „Creating and Using Oracle Solaris Zones “. Informationen zu Ressourcen zur Zonenkonfiguration finden Sie in „Introduction to Oracle Solaris Zones “. Siehe auch die Manpages `mwac`(5) und `tpd`(5).

Oracle Solaris Kernel-Zonen sind nützlich beim Deployment eines konformen Systems. Beispiel: Sie können ein konformes System konfigurieren, ein einheitliches Archiv (Unified Archive) erstellen und das Image dann als Kernel-Zone bereitstellen. Weitere Informationen finden Sie auf der Manpage `solaris-kz`(5), unter „Creating and Using Oracle Solaris Kernel Zones “ in Abschnitt „Oracle Solaris Zones Overview“ in „Introduction to Oracle Solaris 11.2 Virtualization Environments “ und „Using Unified Archives for System Recovery and Cloning in Oracle Solaris 11.2 “.

- Die neuen Funktionen zu Benutzer- und Vorgangsrechten umfassen Folgendes:
  - Zeitbasierte und ortsbasierte Zugriffskontrolle auf PAM-Services
  - Vordefinierte ARMOR-Rollen (Authorization Roles Managed on RBAC)
  - Rechteprofile, die Benutzer vor der Ausführung einer privilegierten Aktion zur Eingabe eines Passworts zwingen
  - Rechteprofile zur Beobachtung von Netzwerk und System zur Ausführung der Diagnosebefehle `ipstat`, `tcpstat`, `snoop` und `intrstat` mit Berechtigung und ohne `root` zu sein

  Nähere Einzelheiten finden Sie unter „What’s New in Rights in Oracle Solaris 11.2“ in „Securing Users and Processes in Oracle Solaris 11.2 “.
- IKE Version 2 (IKEv2) stellt das aktuelle IKE-Protokoll zur automatischen Schlüsselverwaltung von durch IPsec geschützten Netzwerkpaketen bereit. Nähere Einzelheiten finden Sie unter „What’s New in Network Security in Oracle Solaris 11.2“ in „Securing the Network in Oracle Solaris 11.2 “.
- Das Oracle Hardware Management Pack (HMP) stellt Befehlszeilentools für die Konfiguration und das Update von Firmware bereit. Informationen zur sicheren Verwendung von HMP mit anderen Oracle-Hardwareprodukten wie Netzwerk-Switches und NICs finden Sie in „Oracle Hardware Management Pack for Oracle Solaris - Sicherheitshandbuch “.

Oracle Solaris 11 - Sicherheit nach der Installation

Oracle Solaris wird mit standardmäßiger Sicherheit (Secure by Default, SBD) installiert. Diese Sicherheitsfunktion schützt unter anderem 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. Bei der Installation ist das Passwort für den Erstbenutzer und die `root`-Konten 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 Remote-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, wird der Name des Benutzers, der die `root`-Rolle übernommen hat, im Audittrail aufgezeichnet. Der erste Benutzer kann die Prüfprotokolle aufgrund eines Rechts einsehen, das durch das Rechteprofil "System Administrator" gewährt wird.

Kernel-, Datei- und Desktopschutz

Sobald der erste Benutzer angemeldet ist, werden Kernel, Dateisystem, Systemdateien und Desktopanwendungen durch Dateiberechtigungen, Berechtigungen und Benutzerrechte geschützt. Benutzerrechte werden auch als *rollenbasierte Zugriffskontrolle* (Role-Based Access Control, RBAC) bezeichnet.

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` lautet, 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 Standardverzeichnisberechtigungen sind `drwxr-xr-x` (`755`). Die Dateiberechtigungen sind `-rw-r--r--` (`644`).

Systemdateien – Die Konfigurationsdateien des Systems werden durch Dateiberechtigungen geschützt. Eine Systemdatei kann nur über die `root`-Rolle oder durch einen Benutzer, dem das Recht zur Bearbeitung eines bestimmten Dateisystems zugewiesen wurde, geändert werden.

Desktopapplets – Desktopapplets werden durch Rechteverwaltung geschützt. Administrative Aktionen wie das Hinzufügen von Remote-Druckern in Print Manager sind daher nur Benutzern und Rollen gestattet, die Admin-Rechte zum Drucken besitzen.

Oracle Hardware Management Package

Das Oracle Hardware Management Package bietet eine Reihe an Dienstprogrammen zum Konfigurieren, Verwalten und Überwachen von Oracle-Servern. Auf diesen Mehrwertsatz an Tools für Oracle-Hardware kann jederzeit zugegriffen werden. Dadurch können bestimmte hardwarebezogene Informationen automatisch an ILOM geliefert werden, um dessen Überblick über die Systemhardware zu vervollständigen. Informationen zu Dienstprogrammen und Sicherheit finden Sie unter Systems Management and Diagnostics Documentation"> (http://www.oracle.com/goto/ohmp/docs).

Konfigurierbare Sicherheit in Oracle Solaris

Neben der soliden Basis an Sicherheitsstandardeinstellungen, die Oracle Solaris bietet, kann die Sicherheit eines Oracle Solaris-Systems durch zahlreiche weitere Konfigurationsmöglichkeiten an weitere Sicherheitsanforderungen angepasst werden.

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.

Schützen von Daten

Oracle Solaris schützt Daten vom Systemstart über Installation und Verwendung bis hin zur Archivierung.

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. Darüber hinaus unterstützt das Standarddateisystem ZFS Zugriffskontrolllisten (Access Control Lists, ACLs), über die der Zugriff auf einzelne oder Gruppen von Dateisystemobjekten noch genauer gesteuert werden kann.

Weitere Informationen finden Sie hier:

- Einen Überblick über Dateiberechtigungen finden Sie unter „Using UNIX Permissions to Protect Files“ in „Securing Files and Verifying File Integrity in Oracle Solaris 11.2 “.
- 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 „Managing ZFS File Systems in Oracle Solaris 11.2 “ und auf den Manpages.
- Anweisungen zum Festlegen von ACLs bei ZFS-Dateien finden Sie auf der Manpage `chmod`(1).

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. KMF bietet eine einheitliche Schnittstelle für ansonsten unterschiedliche Speichermechanismen, administrative Dienstprogramme und Programmierschnittstellen und für verschiedene Public Key-Infrastrukturen (PKIs).

Cryptographic Framework stellt eine Reihe gängiger Algorithmen und PKCS #11-Bibliotheken bereit, um kryptografische Anforderungen zu verarbeiten. Die PKCS #11-Bibliotheken werden gemäß dem Standard RSA Security Inc. PKCS #11 Cryptographic Token Interface (Cryptoki) implementiert. Kryptografische Services wie Verschlüsselung und Entschlüsselung von Dateien stehen auch normalen Benutzern zur Verfügung.

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:

- Relevante Manpages umfassen `cryptoadm`(1M), `encrypt`(1), `mac`(1), `pktool`(1) und `kmfcfg`(1).
- Einen Überblick über kryptografische Services finden Sie in Kapitel 1, „Cryptographic Framework“ in „Managing Encryption and Certificates in Oracle Solaris 11.2 “ und in Kapitel 4, „Key Management Framework“ in „Managing Encryption and Certificates in Oracle Solaris 11.2 “.
- Beispiele zur Verwendung von Cryptographic Framework finden Sie in Kapitel 3, „Cryptographic Framework“ in „Managing Encryption and Certificates in Oracle Solaris 11.2 “ sowie auf den Manpages.
- Die Aktivierung des Cryptographic Framework FIPS 140-Providers wird unter „How to Create a Boot Environment with FIPS 140 Enabled“ in „Managing Encryption and Certificates in Oracle Solaris 11.2 “ beschrieben.

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 ACLs schützen Dateien, und Sie können das gesamte Dataset bei dessen Erstellung verschlüsseln. Die Oracle Solaris-Rechteverwaltung unterstützt die delegierte Verwaltung von ZFS-Datasets. Das bedeutet, dass Benutzer, denen ein bestimmter Satz Berechtigungen zugewiesen ist, ZFS-Datasets verwalten dürfen.

Weitere Informationen finden Sie hier:

- „User Rights Management“ in „Securing Users and Processes in Oracle Solaris 11.2 “
- Kapitel 1, „Oracle Solaris ZFS File System (Introduction)“ in „Managing ZFS File Systems in Oracle Solaris 11.2 “
- „Oracle Solaris ZFS and Traditional File System Differences“ in „Managing ZFS File Systems in Oracle Solaris 11.2 “
- Kapitel 5, „Managing Oracle Solaris ZFS File Systems“ in „Managing ZFS File Systems in Oracle Solaris 11.2 “
- „How to Remotely Administer ZFS With Secure Shell“ in „Managing Secure Shell Access in Oracle Solaris 11.2 “
- Relevante Manpages umfassen `zfs`(1M) und `zfs`(7FS).

Java Cryptography Extension

Java stellt JCE (Java Cryptography Extension) für Entwickler von Java-Anwendungen bereit. Weitere Informationen finden Sie unter Java SE Security (http://www.oracle.com/technetwork/java/javase/tech/index-jsp-136007.html).

Schützen und Isolieren von Anwendungen

Anwendungen können Malware und böswilligen Benutzern als Einstiegspunkte dienen. In Oracle Solaris wird diesen Bedrohungen durch die Verwendung von Benutzerrechten und die Eingrenzung von Anwendungen in Zonen begegnet. Anwendungen können mit den Berechtigungen ausgeführt werden, die allein für die jeweilige Anwendung erforderlich sind, sodass ein böswilliger Benutzer keine Root-Berechtigung zum Zugriff auf das restliche System erhält. Das Ausmaß eines Angriffs kann über Zonen eingegrenzt werden. Angriffe auf Anwendungen in einer nicht globalen Zone können sich nur auf Prozesse in der jeweiligen Zone auswirken, nicht jedoch auf Prozesse im Hostsystem der Zone.

Die Funktionen ASLR (Address Space Layout Randomization) und SMF (Service Management Facility) bieten darüber hinaus weiteren Schutz für Anwendungen. ASLR macht es Angreifern schwer, die Kontrolle über eine ausführbare Datei zu übernehmen, während Administratoren über SMF-Funktionen das Starten und Stoppen sowie die Verwendung einer Anwendung einschränken können.

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 Prozess, einem Benutzer oder einer Rolle zugewiesen werden. Viele Oracle Solaris-Befehle und -Daemons werden nur mit den Berechtigungen ausgeführt, die für die Aufgabe erforderlich sind. Berechtigungen erkennende Programme können verhindern, dass Eindringlinge mehr Berechtigungen als das Programm selbst erlangen können.

Die Verwendung von Berechtigungen wird auch als *Prozessberechtigungsverwaltung* bezeichnet. Organisationen können mithilfe von Berechtigungen bestimmen – und somit eingrenzen – welche Berechtigungen den auf ihren Systemen ausgeführten Services und Prozessen gewährt werden.

Weitere Informationen finden Sie hier:

- „Process Rights Management“ in „Securing Users and Processes in Oracle Solaris 11.2 “
- Kapitel 2, „Developing Privileged Applications“ in „Developer’s Guide to Oracle Solaris 11 Security “

- Relevante Manpages umfassen `ppriv`(1) und `privileges`(5).

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.

In Oracle Solaris 11.2 können Sie unveränderbare Root-Dateisysteme konfigurieren.

Weitere Informationen finden Sie hier:

- „Configuring Read-Only Zones“ in „Creating and Using Oracle Solaris Zones “
- „Introduction to Oracle Solaris Zones “
- Relevante Manpages umfassen `brands`(5), `zoneadm`(1M) und `zonecfg`(1M).

Zufällige Anordnung des Adressraumlayouts

Die zufällige Anordnung des Adressraumlayouts (ASLR) ordnet die Adressen, die von einem vorgegebenen Programm verwendet werden, zufällig an. ASLR kann bestimmten Angriffsarten, die auf der exakten Speicherortkenntnis bestimmter Speicherbereiche basieren, vorbeugen und bereits den Versuch erkennen, wenn das Programm gestoppt wird. Weitere Informationen finden Sie unter „Address Space Layout Randomization“ in „Securing Systems and Attached Devices in Oracle Solaris 11.2 “ und unter So prüfen Sie, ob ASLR aktiviert ist [33].

Service Management Facility

Services sorgen für eine persistente Ausführung von Anwendungen. Ein Service kann eine laufende Anwendung, den Softwarestatus eines Geräts oder ein Set anderer Services darstellen. Mithilfe der SMF-Funktion (Service Management Facility) von Oracle Solaris werden Services hinzugefügt, entfernt, konfiguriert und verwaltet. SMF nutzt eine Rechteverwaltung 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:

- „Managing System Services in Oracle Solaris 11.2 “
- „How to Assign Specific Privileges to the Apache Web Server“ in „Securing Users and Processes in Oracle Solaris 11.2 “
- Relevante Manpages umfassen `svcadm`(1M), `svcs`(1) und `smf`(5).

Schützen von Benutzern und Zuweisen zusätzlicher Rechte

Benutzer erhalten wie der erste Benutzer einen Basisberechtigungssatz, Rechteprofile und Autorisierungen aus der Datei `/etc/security/policy.conf` (siehe „Eingeschränkter und überwachter Systemzugriff“ [13]). Diese Rechte können konfiguriert werden. Sie können Benutzern Basisrechte verweigern oder weitere Rechte zuweisen.

Oracle Solaris schützt Benutzer durch Passwortanforderungen mit unterschiedlicher Komplexität, einer für unterschiedliche Standortanforderungen konfigurierbaren Authentifizierung sowie einer Benutzerrechteverwaltung, die die administrativen Rechte über Rechteprofile, Autorisierungen und Berechtigungen einschränkt und an vertrauenswürdige Benutzer verteilt. Darüber hinaus erteilen gemeinsam genutzte Konten, auch als *Rollen* bezeichnet, den Benutzern bei Übernahme der Rolle genau diese administrativen Rechte. Das Package Authorization Rules Managed On RBAC (ARMOR) stellt vordefinierte Rollen bereit.

Passwörter und Passwortbeschränkungen

Sichere Passwörter bieten Schutz vor Brute Force-Zugriffsversuchen.

Oracle Solaris bietet eine Reihe von Funktionen, mit denen Sie die Benutzerpasswörter an die Anforderungen Ihres Standorts anpassen können. Sie können Länge und Inhalt der Passwörter festlegen, bestimmen, wie häufig und auf welche Weise sie geändert werden müssen, und eine Passworthistorie führen. Außerdem ist ein Wörterbuch mit ungeeigneten Passwörtern vorhanden. Ferner sind mehrere Hash-Algorithmen für Passwörter verfügbar. Der Standardwert ist SHA256.

Weitere Informationen finden Sie hier:

- „Maintaining Login Control“ in „Securing Systems and Attached Devices in Oracle Solaris 11.2 “

- „Securing Logins and Passwords“ in „Securing Systems and Attached Devices in Oracle Solaris 11.2 “
- Relevante Manpages umfassen `passwd`(1) und `crypt.conf`(4).

Pluggable Authentication Modules

Mit dem PAM-Framework (Pluggable Authentication Module) können Administratoren Anforderungen für die Benutzerauthentifizierung für Konten, Berechtigungsnachweise, Sitzungen und Passwörter koordinieren und konfigurieren, ohne die Services zu ändern, für die eine Authentifizierung erforderlich ist.

Organisationen können mit dem PAM-Framework die Benutzerauthentifizierungserfahrung sowie Konten-, Sitzungs- und Passwortverwaltungsfunktionen anpassen. Systemeintragsservices wie `login` und `ssh` nutzen das PAM-Framework, um alle Einstiegspunkte für das neu installierte System zu sichern. PAM 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.

Oracle Solaris bietet eine breite Palette an PAM-Modulen und -Konfigurationen, mit denen die meisten Standortrichtlinien abgedeckt werden können. Weitere Informationen finden Sie hier:

- Kapitel 1, „Using Pluggable Authentication Modules“ in „Managing Kerberos and Other Authentication Services in Oracle Solaris 11.2 “
- „Writing Applications That Use PAM Services“ in „Developer’s Guide to Oracle Solaris 11 Security “
- Manpage `pam.conf`(4)

Benutzerrechteverwaltung

Benutzerrechte in Oracle Solaris werden nach dem Sicherheitsprinzip der niedrigsten Berechtigung verwaltet. Organisationen können Benutzern oder Rollen selektiv ganz nach den jeweiligen Anforderungen der Organisation administrative Rechte erteilen. Bei Bedarf können sie Benutzern auch Rechte verweigern. Rechte werden bei Prozessen als Berechtigungen und bei Benutzern oder SMF-Methoden als Autorisierungen implementiert. Mithilfe von Rechteprofilen können Berechtigungen und Autorisierungen bequem zu Gruppen zugehöriger Rechte zusammengefasst werden.

Weitere Informationen finden Sie hier:

- „Securing Users and Processes in Oracle Solaris 11.2 “
- Relevante Manpages umfassen `auths`(1), `privileges`(5). `profiles`(1), `rbac`(5), `roleadd`(1M), `roles`(1) und `user_attr`(4).

Sichern der Netzwerkkommunikation

Die Netzwerkkommunikation kann durch Funktionen wie Firewalls, TCP-Wrapper bei Netzwerkanwendungen und verschlüsselte und authentifizierte Remote-Verbindungen geschützt werden.

Paketfilterung

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

Firewall

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:

- Eine IP Filter-Übersicht finden Sie in Kapitel 4, „About IP Filter in Oracle Solaris“ in „Securing the Network in Oracle Solaris 11.2 “.
- Anwendungsbeispiele zu IP Filter finden Sie in Kapitel 5, „Configuring IP Filter“ in „Securing the Network in Oracle Solaris 11.2 “ sowie auf den Manpages.
- Informationen zu und Syntaxbeispiele für die IP Filter-Richtliniensprache erhalten Sie auf der Manpage `ipnat`(4).
- Relevante Manpages umfassen `ipfilter`(5), `ipf`(1M), `ipnat`(1M), `svc.ipfd`(1M) und `ipf`(4).

TCP-Wrapper

TCP-Wrapper stellen eine Zugriffskontrolle für Internetservices bereit. Wenn verschiedene Internetservices (`inetd`) aktiviert sind, gleicht der `tcpd`-Daemon die Adresse eines Hosts, der einen bestimmten Netzwerkservice anfordert, mit einer Zugriffskontrollliste ab. Anforderungen werden dann entsprechend genehmigt oder verweigert. TCP-Wrapper bieten zudem eine hilfreiche Überwachungsfunktion, denn sie protokollieren Hostanforderungen für Netzwerkservices in `syslog`.

Die Funktionen Secure Shell (`ssh`) und `sendmail` von Oracle Solaris sind für die Verwendung von TCP-Wrappern konfiguriert. TCP-Wrapper eignen sich für Netzwerkservices, die eine Eins-zu-Eins-Zuordnung zu ausführbaren Dateien wie `proftpd` und `rpcbind` besitzen.

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.

Informationen zu TCP-Wrappern finden Sie unter:

- So verwenden Sie TCP-Wrapper [49]
- Informationen und Syntaxbeispiele für die Zugriffskontrollsprache für TCP-Wrapper finden Sie auf der Manpage `hosts_access`(4).
- Relevante Manpages umfassen `tcpd`(1M) und `inetd`(1M).

Remote-Zugriff

Bei Angriffen über Remote-Zugriff können System und Netzwerk beschädigt werden. Oracle Solaris bietet umfangreiche Verteidigungsfunktionen für Netzwerkübertragungen. Diese Verteidigungsfunktionen umfassen Verschlüsselung und Authentifizierungsprüfungen für Datenübertragung, Anmeldeauthentifizierung und die Deaktivierung nicht benötigter Remote-Services.

IPsec und IKE

Mit IP Security (IPsec) werden Netzwerkübertragungen durch die Authentifizierung von IP-Paketen und/oder durch deren Verschlüsselung geschützt. Da IPsec unterhalb der Anwendungsschicht implementiert ist, können Internetanwendungen IPsec ohne Änderungen an deren Code nutzen.

IPsec und sein automatisches Key Exchange-Protokoll IKE verwenden Cryptographic Framework-Algorithmen. Darüber hinaus bietet Cryptographic Framework einen zentralen Keystore. Wenn IKE so konfiguriert ist, dass es den Metaslot verwendet, können Organisationen die Schlüssel auf einem Datenträger, einem angeschlossenen Hardware-Keystore oder in einem als *Softtoken*-Keystore bezeichneten Software-Keystore speichern.

IPsec und IKE erfordern eine Konfigurierung und werden daher standardmäßig zwar installiert, aber nicht aktiviert. Wenn es richtig vewaltet wird, ist IPsec ein wirksames Tool bei der Sicherung des Netzwerkverkehrs.

Weitere Informationen finden Sie hier:

- Kapitel 6, „About IP Security Architecture“ in „Securing the Network in Oracle Solaris 11.2 “

- Kapitel 7, „Configuring IPsec“ in „Securing the Network in Oracle Solaris 11.2 “
- „IPsec and FIPS 140“ in „Securing the Network in Oracle Solaris 11.2 “
- Kapitel 8, „About Internet Key Exchange“ in „Securing the Network in Oracle Solaris 11.2 “
- Kapitel 9, „Configuring IKEv2“ in „Securing the Network in Oracle Solaris 11.2 “
- Relevante Manpages umfassen `ipsecconf`(1M) und `in.iked`(1M).

Secure Shell

Auf neu installierten Systemen kann nur die Secure Shell-Funktion von Oracle Solaris für den Remote-Zugriff verwendet werden. Alle anderen Netzwerkservices sind entweder deaktiviert oder befinden sich im Horchmodus.

Secure Shell baut einen verschlüsselten Kommunikationskanal zwischen den Systemen auf. Secure Shell kann zudem als bedarfsorientiertes 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.

Weitere Informationen finden Sie hier:

- Kapitel 1, „Using Secure Shell (Tasks)“ in „Managing Secure Shell Access in Oracle Solaris 11.2 “
- „Secure Shell and FIPS 140“ in „Managing Secure Shell Access in Oracle Solaris 11.2 “
- Relevante Manpages umfassen `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, auf denen Systeme verschiedene Betriebssysteme sowie den Kerberos-Service ausführen.

Kerberos basiert auf dem Kerberos V5-Netzwerkauthentifizierungsprotokoll, das am MIT (Massachusetts Institute of Technology) entwickelt wurde. Der Kerberos-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:

- „Managing Kerberos and Other Authentication Services in Oracle Solaris 11.2 “
- „FIPS 140 Algorithms and Kerberos Encryption Types“ in „Managing Kerberos and Other Authentication Services in Oracle Solaris 11.2 “
- Relevante Manpages umfassen `kadmin`(1M), `kdcmgr`(1M), `kerberos`(5), `kinit`(1) und `krb5.conf`(4).

Verwalten der Systemsicherheit

Oracle Solaris stellt folgende Funktionen zum Verwalten der Systemsicherheit bereit:

- Geprüfter Startvorgang (Verified Boot) – Sichert den Startvorgang. Die Funktion des geprüften Startvorgangs ist standardmäßig deaktiviert.
- Packageverifizierung – Überprüft, ob die installierten Packages mit den Packages im Quell-Repository übereinstimmen.
- Prüfservice – Prüft den Zugriff auf und die Nutzung des Systems. Die Prüfung ist standardmäßig aktiviert.
- Dateiintegritätsprüfung – BART-Manifestdateien können jede Datei im System auflisten, und über Vergleiche der Manifestdateien kann geprüft werden, ob die Dateiintegrität aufrechterhalten wird.
- Logdateien – SMF stellt für jeden Service Logdateien bereit. Das Dienstprogramm `syslog` bietet eine zentrale Datei zum Benennen und Konfigurieren von Logs für Systemservices. Optional können damit Administrationen über kritische Ereignisse benachrichtigt werden. Andere Funktionen wie die Prüfung können auch ihre eigenen Logs erstellen.
- Complianceberichte – Oracle Solaris stellt mehrere Sicherheitsbenchmarks bereit, anhand derer Sie Ihr System bewerten können. Bei diesen Bewertungen werden Berichte erzeugt, die Ihnen helfen, die Sicherheitslage des Systems einzuschätzen.

Geprüfter Startvorgang (Verified Boot)

Der geprüfte Startvorgang ist eine Oracle Solaris-Funktion, bei der der Startvorgang eines Systems gesichert wird. Diese Funktion schützt das System vor Bedrohungen wie beispielsweise der Installation nicht autorisierter Kernel-Module und Trojaner. Die Funktion des geprüften Startvorgangs ist standardmäßig deaktiviert.

Weitere Informationen finden Sie in Kapitel 2, „Protecting Oracle Solaris Systems Integrity“ in „Securing Systems and Attached Devices in Oracle Solaris 11.2 “.

Überprüfung der Packageintegrität

Nach der Installation oder dem Update von Packages können Sie über den Befehl `pkg verify` sicherstellen, dass die Packages auf Ihrem System mit den Packages aus dem Quell-Repository übereinstimmen.

Weitere Informationen finden Sie auf der Manpage pkg(1) sowie unter Pakete überprüfen [33].

Prüfservice

Oracle Solaris stellt einen Prüfservice bereit, mit dem Daten über den Systemzugriff und die Systemnutzung erfasst werden. Die Prüfdaten bieten ein zuverlässiges, mit Zeitstempel versehenes, Log der sicherheitsbezogenen Systemereignisse. Anhand dieser Daten können Sie anschließend die Verantwortlichkeit für die auf einem System ausgeführten Aktionen zuweisen.

Prüfungen sind eine Grundanforderung bei Sicherheitsevaluierungen, Validierungen, Compliance 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 7, „Auditing Reference“ in „Managing Auditing in Oracle Solaris 11.2 “.
- Richtlinien finden Sie unter Wichtige Ereignisse außer Anmelden/Abmelden prüfen [45] und auf den Manpages.
- Einen Überblick über Prüfungen finden Sie in Kapitel 1, „About Auditing in Oracle Solaris“ in „Managing Auditing in Oracle Solaris 11.2 “.
- Informationen zu Prüfungsaufgaben finden Sie in Kapitel 3, „Managing the Audit Service“ in „Managing Auditing in Oracle Solaris 11.2 “.

Überprüfung der Dateiintegrität

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. Nach der Installation können Sie über den Befehl `pkg verify` bestätigen, dass der Inhalt Ihrer Quell- und Zielpackages übereinstimmt. Nach der Packageüberprüfung können mithilfe von BART-Manifestdateien leicht und zuverlässig Informationen über die Dateien auf einem System erfasst werden.

BART ist ein nützliches Tool für das Integritätsmanagement in einem System oder Systemnetzwerk. Die Dateien eines Systems können mit den ursprünglichen Dateien des

Systems sowie mit den Dateien anderer Systeme verglichen werden. Die Berichte zeigen möglicherweise an, dass ein System nicht gepatcht wurde, ein Eindringling nicht genehmigte Dateien installiert hat oder dass ein Eindringling die Berechtigungen oder den Inhalt sensibler Dateien, wie solche mit dem Eigentümer `root`, geändert hat.

Weitere Informationen finden Sie hier:

- Entsprechende Richtlinien finden Sie unter „Die Dateiintegrität mittels BART überprüfen.“ [58], „Die Dateiintegrität mittels BART überprüfen.“ [58] und auf den Manpages.
- Einen Überblick über BART finden Sie in Kapitel 2, „Verifying File Integrity by Using BART“ in „Securing Files and Verifying File Integrity in Oracle Solaris 11.2 “.
- Beispiele für die Verwendung von BART finden Sie im Abschnitt „About Using BART“ in „Securing Files and Verifying File Integrity in Oracle Solaris 11.2 “ sowie auf den Manpages.
- Relevante Manpages umfassen `bart`(1M), `bart_rules`(4) und `bart_manifest`(4).

Logdateien

In der SMF-Funktion (Service Management Facility) von Oracle Solaris wird der Status jedes Service einzeln protokolliert. Für zahlreiche Services (Beispiel: Prüfung und Secure Shell) werden eigene Logs geführt. Der `syslog`- oder `rsyslog`-Daemon schreibt ein zentrales Log, mit dem Administratoren Informationen und Warnungen zu kritischen Zuständen in zahlreichen Services erhalten. Beispiel: Die Prüfung kann so konfiguriert werden, dass eine Zusammenfassung der Prüfdatensätze in `syslog` geschrieben wird. Weitere Informationen finden Sie auf den Manpages `syslogd`(1M) und `syslog.conf`(4).

Compliance mit Sicherheitsstandards

Über den Befehl `compliance assess` erhalten Sie einen Snapshot zur Sicherheitslage Ihres Systems. In den aus der Bewertung hervorgehenden Berichten werden bestimmte Änderungen an Ihrem System zur Erfüllung der Sicherheitsbenchmarks der Branche vorgeschlagen. Weitere Informationen hierzu finden Sie im „Oracle Solaris 11.2 Handbuch zur Sicherheitscompliance “ sowie auf der Manpage `compliance`(1M).

Sicherheitskennzeichnung

Eine Sicherheitskennzeichnung wird in Oracle Solaris über die Funktion Trusted Extensions bereitgestellt.

Die Funktion Trusted Extensions in Oracle Solaris

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.

Die Implementierung von Trusted Extensions bietet die einzigartige Möglichkeit, einen hohen Grad an Sicherheit bei gleichzeitiger Maximierung der Kompatibilität und Minimierung des Overheads bereitzustellen. Trusted Extensions ist Teil der „Oracle Solaris 11 Common Criteria EAL4+-Zertifizierung“ [29].

Die Funktion Trusted Extensions erfüllt die Anforderungen des LSPs (Common Criteria Labeled Security Package). Siehe „Oracle Solaris 11 Common Criteria EAL4+-Zertifizierung“ [29]

Weitere Informationen finden Sie hier:

- Informationen zur Konfiguration und Verwaltung von Trusted Extensions erhalten Sie in „Trusted Extensions Configuration and Administration “.
- Relevante Manpages umfassen `trusted_extensions`(5), `labeladm`(1M) und `labeld`(1M).

Dateisystemkennzeichnung

Standardmäßig wird Dateisystemen eine einzelne Kennzeichnung in einer Zone mit derselben Kennzeichnung zugewiesen. Sie können ein mehrstufiges ZFS-Dataset erstellen, es in einem Trusted Extensions-System mounten und die Dateien in diesem Dataset – sofern Sie die entsprechenden Berechtigungen besitzen – upgraden und downgraden. Weitere Informationen finden Sie im Abschnitt „Multilevel Datasets for Relabeling Files“ in „Trusted Extensions Configuration and Administration “.

Gekennzeichnete Netzwerkkommunikation

Die Funktion Trusted Extensions kennzeichnet die Netzwerkkommunikation. Anhand eines Vergleichs der mit Ausgangs- und Empfangsendpunkten des Netzwerks verknüpften Kennzeichnungen werden die Datenflüsse eingeschränkt. Gateways und Zwischenhops müssen ebenfalls gekennzeichnet werden, damit die Daten auf der gekennzeichneten

Kommunikationsebene übertragen werden können. NFS und mehrstufige ZFS-Datasets stellen zusätzliche Funktionen in einem Netzwerk bereit.

Weitere Informationen finden Sie hier:

- „Configuring the Network Interfaces in Trusted Extensions“ in „Trusted Extensions Configuration and Administration “
- Kapitel 15, „Trusted Networking“ in „Trusted Extensions Configuration and Administration “
- Kapitel 16, „Managing Networks in Trusted Extensions“ in „Trusted Extensions Configuration and Administration “

Trusted Extensions – Mehrstufiger Desktop

Im Gegensatz zu den meisten anderen mehrstufigen Betriebssystemen verfügt Trusted Extensions über einen mehrstufigen Desktop. Benutzer können so konfiguriert werden, dass sie nur die für sie zulässigen Kennzeichnungen sehen. Jede Kennzeichnung kann so konfiguriert werden, dass jeweils ein eigenes Passwort erforderlich ist.

Weitere Informationen finden Sie im „Trusted Extensions User’s Guide “. Informationen zur Konfiguration von Benutzern finden Sie in Kapitel 11, „Managing Users, Rights, and Roles in Trusted Extensions“ in „Trusted Extensions Configuration and Administration “.

Oracle Solaris 11 Common Criteria EAL4+-Zertifizierung

Oracle Solaris 11 ist unter dem kanadischen Common Criteria Scheme unter der EAL4-Stufe (Evaluation Assurance Level 4) zertifiziert und wird über automatische Fehlerbehebung (Flaw Remediation, EAL4+) noch verbessert. EAL4 ist die höchste Bewertungsstufe, die unter dem CCRA-Standard (Common Criteria Recognition Arrangement) von 26 Ländern anerkannt wird.

Die Zertifizierung gilt für das OSPP-Schutzprofil (Operating System Protection Profile) und umfasst folgende erweiterte Packages:

- Erweitertes Management
- Erweiterte Identifizierung und Authentifizierung
- Sicherheitskennzeichnung
- Virtualisierung

Weitere Informationen zu der Zertifizierung finden Sie unter:

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

- 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:

- Importance of Software Security Assurance (http://www.oracle.com/us/support/assurance/overview/index.html)
- 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-BS

Die Installation von Oracle Solaris-BS erfolgt durch Auswahl einer Reihe von als *Gruppe* bezeichneten Packages aus einem Package-Repository. Verschiedene Gruppen stellen Packages für unterschiedliche Verwendungszwecke bereit. Beispiel: Mehrzweckserver, Systeme mit Minimalinstallation und Desktopsysteme. Packages sind signiert, und ihre sichere Übertragung kann überprüft werden.

Wählen Sie bei der Installation des Oracle Solaris-BS das Medium mit dem geeigneten *Gruppen*package 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 Small Server –** Über die AI-Installation (Automated Installer) und den Text Installer wird optional die Gruppe `group/system/solaris-small-server` installiert, die eine Befehlszeilenumgebung bereitstellt, zu der Sie Packages hinzufügen können.

- **Oracle Solaris Minimal Server –** Über die AI-Installation (Automated Installer) und den Text Installer wird optional die Gruppe `group/system/solaris-small-server` installiert, die eine Befehlszeilenumgebung bereitstellt, der Sie einfach die gewünschten Packages hinzufügen können.
- **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 11.2 Systems “.

Zur Anleitung bei der Mediaauswahl lesen Sie die folgenden Installationshandbücher und Handbücher zum Packageinhalt:

- „Installing Oracle Solaris 11.2 Systems “
- „Creating a Custom Oracle Solaris 11.2 Installation Image “
- „Adding and Updating Software in Oracle Solaris 11.2 “
- „Oracle Solaris 11.2 Package Group Lists “

Erstmaliges Sichern des Systems

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

TABELLE 2-1 Systemsicherung - Übersicht der Schritte

Aufgabe	Beschreibung	Anweisungen siehe
1. Überprüfen der Pakete im System	Dadurch wird überprüft, ob die Packages auf der Installationsquelle den installierten Packages entsprechen.	Pakete überprüfen [33]
2. Sicherstellen, dass die ausführbaren Dateien geschützt sind	Dadurch wird geprüft, ob ASLR aktiviert ist.	So prüfen Sie, ob ASLR aktiviert ist [33]
3. Schutz der Hardwareeinstellungen des Systems	Die Hardware wird geschützt, indem ein Passwort für Änderungen der Hardwareeinstellungen verlangt wird. Auf einem x86-Rechner wird der Zugriff auf das GRUB-Menü gesteuert. Auf einem SPARC-Rechner wird die Hardware über den Befehl `eeprom` geschützt.	„Controlling Access to System Hardware“ in „Securing Systems and Attached Devices in Oracle Solaris 11.2 “

Aufgabe	Beschreibung	Anweisungen siehe
3. Deaktivieren nicht erforderlicher Services	Prozesse, die für den Systemablauf nicht erforderlich sind, werden nicht ausgeführt.	Nicht erforderliche Services deaktivieren [34]
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 [35]
6. Erstellen Sie eine Anmeldewarnmeldung gemäß Ihrer Standortsicherheitsrichtlinie.	Benutzer werden vor und nach der Authentifizierung benachrichtigt, dass das System überwacht wird.	Sicherheitsmeldung zu allen Bannerdateien hinzufügen [36] Sicherheitsmeldung in den Desktop-Anmeldebildschirm einfügen [37]

▼ 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 „Using Your Assigned Administrative Rights“ in „Securing Users and Processes in Oracle Solaris 11.2 “.

1. **Prüfen Sie das Installationslog.**
2. **Führen Sie den Befehl `pkg verify` aus.**
   Leiten Sie die Befehlsausgabe zur Dokumentation in eine Datei um.

   ```
   # pkg verify > /var/pkgverifylog
   ```
3. **Sehen Sie in der Protokolldatei nach, ob Fehler aufgetreten sind.**
4. **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`.

▼ So prüfen Sie, ob ASLR aktiviert ist

Standardmäßig werden getaggte ausführbare Anweisungen in nicht verknüpfte Adressbereiche geschrieben, um zu verhindern, dass Angreifer Anweisungen per Injection in den ausführbaren Stack einfügen.

Bevor Sie beginnen Sie müssen die `root`-Rolle übernehmen. Weitere Informationen finden Sie unter „Using Your Assigned Administrative Rights“ in „Securing Users and Processes in Oracle Solaris 11.2 “.

1. **Stellen Sie sicher, dass ASLR aktiviert ist.**

```
# sxadm info
EXTENSION       STATUS                  CONFIGURATION
aslr            enabled (all)           enabled (all)
```

Der Wert `all` ist stärker als der Standardwert und könnte bei Anwendungen, die in ihrem Arbeitsspeicher einen aufeinander folgenden Stack benötigen, zu Fehlern führen. Beispiel: Manche Datenbanken benötigen einen aufeinander folgenden Stack in ihrem Arbeitsspeicher.

2. **Wenn ASLR deaktiviert ist, aktivieren Sie den Standardwert, und prüfen Sie, ob er aktiviert ist.**

```
# sxadm delcust aslr
# sxadm info
EXTENSION       STATUS                  CONFIGURATION
aslr            enabled (tagged-files)  system default (default)
```

Siehe auch Zum Debugging können Sie ASLR deaktivieren, indem Sie den Befehl `sxadm` auf einer bestimmten Binärdatei aufrufen. Beispiele hierzu finden Sie auf der Manpage `sxadm`(1M).

▼ Nicht erforderliche Services deaktivieren

Führen Sie diese Schritte durch, um die auf Ihrem System nicht erforderlichen Services zu deaktivieren.

Bevor Sie beginnen Sie müssen die `root`-Rolle übernehmen. Weitere Informationen finden Sie unter „Using Your Assigned Administrative Rights“ in „Securing Users and Processes in Oracle Solaris 11.2 “.

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

```
# svcs | grep network
online         Sep_07   svc:/network/loopback:default
online         Sep_07   svc:/network/http:apache22
online         Sep_07   svc:/network/nfs/server:default
...
online         Sep_07   svc:/network/ssh:default
```

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

Beispiel: Wenn es sich beim System nicht um einen NFS-Server oder Webserver handelt und deren 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, „Introduction to the Service Management Facility“ in „Managing System Services in Oracle Solaris 11.2 “ und auf der Manpage `svcs`(1).

▼ Energieverwaltungsfunktion für Benutzer entfernen

Führen Sie diese Schritte durch, damit Benutzer auf der Konsole eines Systems dieses weder anhalten noch abschalten können. Diese Softwarelösung funktioniert nicht, wenn die Systemhardware vom Konsolenbenutzer ausgeschaltet werden kann.

Bevor Sie beginnen Sie müssen die `root`-Rolle übernehmen. Weitere Informationen finden Sie unter „Using Your Assigned Administrative Rights“ in „Securing Users and Processes in Oracle Solaris 11.2 “.

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

```
% profiles -p "Console User" info
 name=Console User
 desc=Manage System as the Console User
 auths=solaris.system.shutdown,solaris.device.cdrw,
             solaris.smf.manage.vbiosd,solaris.smf.value.vbiosd
 profiles=Suspend To RAM,Suspend To Disk,Brightness,CPU Power Management,
                Network Autoconf User
 help=RtConsUser.html
```

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

   Anweisungen finden Sie unter „How to Create a Rights Profile“ in „Securing Users and Processes in Oracle Solaris 11.2 “.

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.**

   - Wenn zahlreiche Benutzer ein Rechteprofil gemeinsam verwenden, kann das Einrichten dieses Wertes in einem Rechteprofil eine akzeptable Lösung sein.

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

   - Sie können das Profil auch in der Datei `policy.conf` für jedes System einzeln zuweisen.

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

Siehe auch Weitere Informationen finden Sie im Abschnitt „policy.conf File“ in „Securing Users and Processes in Oracle Solaris 11.2 “ sowie in 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. Die Datei `/etc/issue` wird vor der Authentifizierung angezeigt, die Datei `/etc/motd` hingegen erst danach.

Anmerkung - Die hier als Beispiele angeführten Meldungen entsprechen nicht den Anforderungen der US-Behörden und wahrscheinlich auch nicht Ihrer Sicherheitsrichtlinie. Besprechen Sie den Inhalt der Sicherheitsmeldung mit dem Rechtsberater in Ihrem Unternehmen.

Bevor Sie beginnen Sie müssen Administrator mit dem zugewiesenen Rechteprofil "Administrator Message Edit" sein. Weitere Informationen finden Sie unter „Using Your Assigned Administrative Rights“ in „Securing Users and Processes in Oracle Solaris 11.2 “.

1. **Erstellen Sie die Datei `/etc/issue`, und fügen Sie 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 `ssh`-, `telnet`- und FTP-Services tun. Informationen zur Anzeige des Inhalts von `/etc/issue` bei der Desktopanmeldung finden Sie unter Sicherheitsmeldung in den Desktop-Anmeldebildschirm einfügen [37].

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 Authentifizierung, nach der Authentifizierung oder bei beidem angezeigt wird. Die Datei `/etc/issue` wird vor der Authentifizierung angezeigt, die Datei `/etc/motd` hingegen erst danach.

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.

Anmerkung - Die hier als Beispiel angeführte Meldung entspricht nicht den Anforderungen der US-Behörden und wahrscheinlich auch nicht Ihrer Sicherheitsrichtlinie. Besprechen Sie den Inhalt der Sicherheitsmeldung mit dem Rechtsberater in Ihrem Unternehmen.

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.

1. **Fügen Sie eine Sicherheitsmeldung vor der Authentifizierung in den Desktopanmeldebildschirm ein, indem Sie eine der nachfolgenden Optionen verwenden.**

   Die Optionen, mit denen ein Dialogfeld vor der Authentifizierung erstellt wird, verwenden die Sicherheitsmeldung der Datei `/etc/issue` aus Schritt 1 von Sicherheitsmeldung zu allen Bannerdateien hinzufügen [36].

   - **Option 1: 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 und nach der Authentifizierung anzeigen.

     ```
     # 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).

   - **Option 2: 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.

Anmerkung - 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 finden 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
```

2. Fügen Sie eine Sicherheitsmeldung nach der Authentifizierung in den Desktopanmeldebildschirm ein, indem Sie eine der nachfolgenden Optionen verwenden.

Die Datei, mit der ein Dialogfeld nach der Authentifizierung erstellt wird, verwendet die Sicherheitsmeldung in der Datei `/etc/motd` aus Schritt 2 von Sicherheitsmeldung zu allen Bannerdateien hinzufügen [36].

- **OPTION 1: Fügen Sie nach der Authentifizierung eine Sicherheitsmeldung in den Desktop ein.**

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

Anmerkung - Das Dialogfeld kann durch Fenster im Arbeitsbereich des Benutzers verdeckt werden.

- **OPTION 2: Erstellen Sie eine Desktopdatei, mit der die Sicherheitsmeldung nach der Authentifizierung in einem zusätzlichen Fenster 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/motd
OnlyShowIn=GNOME;
X-GNOME-Autostart-Phase=Application
```

Um nach der Authentifizierung im Anmeldefenster zum Arbeitsbereich zu gelangen, muss der Benutzer das Fenster mit der Sicherheitsmeldung schließen. Optionen des Befehls `zenity` finden Sie auf der Manpage `zenity`(1).

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.

TABELLE 2-2 Schutz für Benutzer - Übersicht der Schritte

Aufgabe	Beschreibung	Anweisungen siehe
Sichere Passwörter und regelmäßige Passwortänderungen	Dadurch werden die standardmäßig auf jedem System vorhandenen Passwortbeschränkungen verstärkt.	Striktere Passwortbeschränkungen festlegen [40]
Konfigurieren Sie restriktive Dateiberechtigungen für normale Benutzer.	Hierdurch wird ein restriktiverer Wert als `022` für Dateiberechtigungen der normalen Benutzer festgelegt.	So legen Sie einen restriktiveren `umask`-Wert für normale Benutzer fest [44].
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 [42]
Wählen Sie die Prüfklasse `cusa` für alle Benutzer im Voraus.	Auf diese Weise können Sie potenzielle Bedrohungen des Systems überwachen und aufzeichnen.	Wichtige Ereignisse außer Anmelden/ Abmelden prüfen [45]
Erstellen Sie Rollen.	Dadurch werden einzelne administrative Aufgaben an mehrere vertrauenswürdige Benutzer verteilt, sodass das System nicht beschädigt werden kann. Sie können vordefinierte ARMOR-Rollen verwenden, Ihre eigenen Rollen erstellen oder ARMOR mit Ihren eigenen Rollen erweitern.	„Managing User Accounts by Using the CLI“ in „Managing User Accounts and User Environments in Oracle Solaris 11. 2 “ „Assigning Rights to Users“ in „Securing Users and Processes in Oracle Solaris 11. 2 “
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 11.2 Desktop Administrator’s Guide “.
Schränken Sie Benutzerrechte ein.	Dadurch werden die Basisberechtigungen entfernt, die Benutzer nicht benötigen.	Nicht benötigter Basisberechtigungen von Benutzern entfernen [46]

▼ Striktere Passwortbeschränkungen festlegen

Führen Sie diese Schritte durch, wenn die Standardwerte nicht den Sicherheitsbestimmungen Ihres Standorts entsprechen. Die Schritte orientieren sich an der Reihenfolge der Variableneinträge in der Datei `/etc/default/passwd`.

Bevor Sie beginnen Sie müssen Administrator mit der Berechtigung `solaris.admin.edit/etc/default/passwd` sein. Weitere Informationen finden Sie unter „Using Your Assigned Administrative Rights“ in „Securing Users and Processes in Oracle Solaris 11.2 “.

- **Nehmen Sie über den Befehl `pfedit` folgende Änderungen in der Datei `/etc/default/passwd` vor:**

  a. **Passwortänderung durch den Benutzer frühestens alle drei Wochen, spätestens alle vier Monate**

  ```
  ## /etc/default/passwd
  ##
  #MAXWEEKS=
  #MINWEEKS=
  MAXWEEKS=13
  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 der Variablen, die die Passworterstellung einschränken, finden Sie auf der Manpage `passwd`(1).
- Informationen zu den nach der Installation wirksamen Passwortbeschränkungen finden Sie in „Eingeschränkter und überwachter Systemzugriff“ [13].

▼ Kontosperre für normale Benutzer festlegen

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

Anmerkung - Rollen sind gemeinsam verwendete Konten. Legen Sie keine Kontosperre für Benutzer fest, die Rollen übernehmen können, oder für Rollen, da ein gesperrter Benutzer die Rolle sperren kann.

Bevor Sie beginnen Legen Sie keinen systemweiten Schutz fest auf einem System, das Sie für administrative Aufgaben nutzen. Überwachen Sie stattdessen das Administrationssystem auf ungewöhnliche Nutzung, und halten Sie es für Administratoren zugänglich.

Sie müssen die `root`-Rolle übernehmen. Weitere Informationen finden Sie unter „Using Your Assigned Administrative Rights“ in „Securing Users and Processes in Oracle Solaris 11.2 “.

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

   Wählen Sie den Geltungsbereich des Attributwerts.

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

     Dieser Schutz gilt für alle Benutzer, die versuchen, das System zu verwenden.

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

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

     Dieser Schutz gilt nur für den Benutzer, für den Sie diesen Befehl ausführen. Wenn Sie zahlreiche Benutzer haben, ist dies keine akzeptable Lösung.

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

   - **Erstellen Sie ein Rechteprofil, und weisen Sie es zu.**

     Dieser Schutz gilt für alle Benutzer oder Systeme, für die Sie dieses Rechteprofil zuweisen.

     a. **Erstellen Sie das Rechteprofil.**

        ```
        # profiles -p shared-profile -S ldap
        shared-profile: set lock_after_retries=yes
        ...
        ```

Weitere Informationen zur Erstellung von Rechteprofilen finden Sie unter „Creating Rights Profiles and Authorizations“ in „Securing Users and Processes in Oracle Solaris 11.2 “.

b. Weisen Sie das Rechteprofil einzelnen Benutzern oder systemweit zu.

Wenn zahlreiche Benutzer ein Rechteprofil gemeinsam verwenden, kann das Einrichten dieses Wertes in einem Rechteprofil eine akzeptable Lösung sein.

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

Sie können das Profil auch in der Datei `policy.conf` für jedes System einzeln zuweisen.

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

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

Wählen Sie den Geltungsbereich des Attributwerts.

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

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

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

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

- **Erstellen Sie ein Rechteprofil, und weisen Sie es zu.**

  Befolgen Sie die Schritte unter Schritt 1.3, um ein Rechteprofil zu erstellen, das `lock_after_retries=3` umfasst.

Siehe auch

- Eine Erläuterung der Attribute zur Benutzer- und Rollensicherheit finden Sie in Kapitel 8, „Reference for Oracle Solaris Rights“ in „Securing Users and Processes in Oracle Solaris 11.2 “.
- Relevante Manpages umfassen `policy.conf`(4), `profiles`(1), `user_attr`(4) und `usermod`(1M).

So legen Sie einen restriktiveren umask-Wert für normale Benutzer fest

Das Dienstprogramm umask legt die Dateiberechtigungsbits von benutzerdefinierten Dateien fest. Wenn der umask-Standardwert 022 nicht ausreichend ist, gehen Sie folgendermaßen vor, um einen restriktiveren Wert festzulegen.

Bevor Sie beginnen Sie müssen Administrator werden, der zum Bearbeiten der Skeleton-Dateien autorisiert ist. Diesen Autorisierungen wird die root-Rolle zugewiesen. Weitere Informationen finden Sie unter „Using Your Assigned Administrative Rights“ in „Securing Users and Processes in Oracle Solaris 11.2 “.

1. **Sehen Sie sich die Beispieldateien an, die Oracle Solaris für Standardwerte von Benutzershells bereitstellt.**

```
# ls -1a /etc/skel
.bashrc
.profile
local.cshrc
local.login
local.profile
```

2. **Legen Sie den Wert umask in den /etc/skel-Dateien fest, die Sie den Benutzern zuweisen werden.**

   Wählen Sie einen der folgenden Werte:

   - umask 026 – bietet maßvollen Dateischutz

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

     (750) – 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:

- „Managing User Accounts by Using the CLI“ in „Managing User Accounts and User Environments in Oracle Solaris 11.2 “
- „Default umask Value“ in „Securing Files and Verifying File Integrity in Oracle Solaris 11.2 “
- Relevante Manpages umfassen useradd(1M) und umask(1).

▼ Wichtige Ereignisse außer Anmelden/Abmelden prüfen

Führen Sie diese Schritte durch, um administrative Befehle, Systemzugriffe und andere in Ihrer Standortsicherheitsrichtlinie angegebene wichtige Ereignisse zu prüfen.

Anmerkung - 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 „Using Your Assigned Administrative Rights“ in „Securing Users and Processes in Oracle Solaris 11.2 “.

1. **Prüfen Sie jede Verwendung privilegierter Befehle durch Benutzer, denen administrative Rechteprofile und Rollen zugewiesen sind.**

   Fügen Sie die Prüfklasse `cusa` zu deren Vorauswahlmaske hinzu.

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

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

   Die in der Metaklasse `cusa` aufgeführten Prüfklassen sind in der Datei `/etc/security/audit_class` aufgeführt.

2. **Zeichnen Sie die Argumente für Prüfbefehle auf.**

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

3. **(Optional) Zeichnen Sie die Umgebung auf, in der Prüfbefehle ausgeführt werden.**

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

Anmerkung - Diese Policy-Option kann bei der Problembehandlung nützlich sein.

Siehe auch

- Informationen zur Prüf-Policy finden Sie unter „Audit Policy“ in „Managing Auditing in Oracle Solaris 11.2 “.
- Beispiele zum Einrichten von Prüf-Flags finden Sie unter „Configuring the Audit Service“ in „Managing Auditing in Oracle Solaris 11.2 “ sowie unter „Troubleshooting the Audit Service“ in „Managing Auditing in Oracle Solaris 11.2 “.
- Manpage `auditconfig`(1M)

▼ Nicht benötigter Basisberechtigungen von Benutzern entfernen

Unter bestimmten Umständen können einige Basisberechtigungen aus einem Basissatz für normale Benutzer oder Gastbenutzer entfernt werden. Beispiel: Sun Ray-Benutzer werden möglicherweise daran gehindert, den Status von Vorgängen zu prüfen, deren Eigentümer sie nicht sind.

Bevor Sie beginnen Sie müssen die `root`-Rolle übernehmen. Weitere Informationen finden Sie unter „Using Your Assigned Administrative Rights“ in „Securing Users and Processes in Oracle Solaris 11.2 “.

1. **Listen Sie eine vollständige Definition des Basisberechtigungssatzes auf.**

   Die nachstehenden drei Basisberechtigungen müssen möglicherweise entfernt werden.

   ```
   % ppriv -lv basic
   file_link_any
    Allows a process to create hardlinks to files owned by a uid
    different from the process' effective uid.
   ...
   proc_info
    Allows a process to examine the status of processes other
    than those it can send signals to.  Processes which cannot
    be examined cannot be seen in /proc and appear not to exist.
   proc_session
    Allows a process to send signals or trace processes outside its
    session.
   ...
   ```

2. **Wählen Sie, für welchen Bereich die Entfernung der Berechtigung gelten soll.**

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

     Benutzern, die versuchen, auf das System zuzugreifen, werden diese Berechtigungen nicht erteilt. Diese Art der Entfernung von Berechtigungen kann für einen öffentlich zugänglichen Rechner angemessen sein.

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

   - **Entziehen Sie einzelnen Benutzern Berechtigungen.**

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

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

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

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

- **Benutzer sollen keine zweite Sitzung neben der aktuellen starten können. Beispiel: eine `ssh`-Sitzung.**

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

- **Entfernen aller drei Basisberechtigungen aus einem Basissatz für normale Benutzer**

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

- **Erstellen Sie ein Rechteprofil, und weisen Sie es zu.**
  Dieser Schutz gilt für alle Benutzer oder Systeme, für die Sie dieses Rechteprofil zuweisen.

  a. **Erstellen Sie das Rechteprofil.**

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

  Weitere Informationen zur Erstellung von Rechteprofilen finden Sie unter „Creating Rights Profiles and Authorizations“ in „Securing Users and Processes in Oracle Solaris 11.2 “.

  b. **Weisen Sie das Rechteprofil einzelnen Benutzern oder systemweit zu.**
  Wenn zahlreiche Benutzer ein Rechteprofil gemeinsam verwenden (Beispiel: Sun Ray- oder Remote-Benutzer), kann das Einrichten dieses Wertes in einem Rechteprofil eine akzeptable Lösung sein.

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

  Sie können das Profil auch in der Datei `policy.conf` für jedes System einzeln zuweisen.

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

Siehe auch Weitere Informationen finden Sie in Kapitel 1, „About Using Rights to Control Users and Processes“ in „Securing Users and Processes in Oracle Solaris 11.2 “ sowie auf der Manpage `privileges`(5).

Schutz des Netzwerks

Zu diesem Zeitpunkt haben Sie wahrscheinlich Benutzer, die Rollen übernehmen können, und Rollen erstellt.

Führen Sie von den folgenden Schritten diejenigen durch, die zusätzliche Sicherheit gemäß den Anforderungen Ihres Standorts geben. Diese Netzwerkaufgaben bieten zusätzliche Sicherheit für die Protokolle IP, ARP und TCP.

TABELLE 2-3 Konfigurieren des Netzwerks - Übersicht der Schritte

Aufgabe	Beschreibung	Anweisungen siehe
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 11.2 “
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 11.2 “
	Es wird nicht auf Broadcast- und Multicast-Echoanforderungen reagiert.	„How to Disable Responses to Echo Requests“ in „Securing the Network in Oracle Solaris 11.2 “
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 11.2 “
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 11.2 “
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 11.2 “
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 11.2 “
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
Konfigurieren Sie eine Firewall.	Dadurch wird mit der IP Filter-Funktion eine Firewall bereitgestellt.	Kapitel 4, „About IP Filter in Oracle Solaris“ in „Securing the Network in Oracle Solaris 11.2 “ Kapitel 5, „Configuring IP Filter“ in „Securing the Network in Oracle Solaris 11.2 “
Konfigurieren Sie verschlüsselte und authentifizierte Netzwerkverbindungen.	Durch IPsec und IKE werden Netzwerkübertragungen zwischen Knoten und Netzwerken geschützt, die gemeinsam mit IPsec und IKE konfiguriert werden.	Kapitel 7, „Configuring IPsec“ in „Securing the Network in Oracle Solaris 11.2 “ Kapitel 9, „Configuring IKEv2“ in „Securing the Network in Oracle Solaris 11.2 “

▼ 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 11.2 “ 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 „Administering TCP/IP Networks, IPMP, and IP Tunnels in Oracle Solaris 11.2 “.**

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 `proftpd.conf` hinzufügen:**

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

   c. **Starten Sie den FTP-Service neu.**

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

Schutz von Dateisystemen

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

Das `tmpfs`-Dateisystem kann ohne Grenzen anwachsen. Um DoS-Attacken (Denial of Service) abzuwenden, führen Sie die Schritte unter Die Größe des `tmpfs`-Dateisystems beschränken [50] aus.

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 „Managing ZFS File Systems in Oracle Solaris 11.2 “ sowie auf der Manpage zfs(1M).

TABELLE 2-4 Schutz von Dateisystemen - Übersicht der Schritte

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 „Managing ZFS File Systems in Oracle Solaris 11.2 “
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 „Managing ZFS File Systems in Oracle Solaris 11.2 “
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 „Managing ZFS File Systems in Oracle Solaris 11.2 “ „Examples of Encrypting ZFS File Systems“ in „Managing ZFS File Systems in Oracle Solaris 11.2 “
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 [50]

▼ 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 Um die Datei vfstab bearbeiten zu können, müssen Sie ein Administrator mit zugewiesener solaris.admin.edit/etc/vfstab-Autorisierung sein. Um das System neu starten zu können, muss Ihnen das Rechteprofil "Maintenance and Repair" (Wartung und Reparatur) zugewiesen sein. Die root-Rolle verfügt über alle diese Rechte. Weitere Informationen finden Sie unter „Using Your Assigned Administrative Rights“ in „Securing Users and Processes in Oracle Solaris 11.2 “.

1. **Bestimmen Sie den Speicherplatz auf Ihrem System.**

Anmerkung - Das im folgenden Beispiel eingesetzte SPARC-System der Serie T3 besitzt ein SSD-Laufwerk (Solid State Disk) für eine I/O-Beschleunigung und umfasst acht 279,40-MB-Datenträger. 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
   #
   ...
   #swap       -            /tmp        tmpfs   -       yes     -
   swap        -            /tmp        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 Tues Feb 4 14:07:27 2014
   swap on /tmp type tmpfs
   read/write/setuid/devices/rstchown/xattr/size=10400m/dev=89c0006 on Tues ...
   ```

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

Standardmäßig dürfen Änderungen an den Systemdateiberechtigungen nur über die `root`-Rolle vorgenommen werden. Rollen und Benutzer, denen die Autorisierung `solaris.admin.edit/`*path-to-system-file* zugewiesen ist, können *system-file* ändern. Eine Suche nach allen Dateien kann nur über die `root`-Rolle vorgenommen werden.

TABELLE 2-5 Dateischutz und -änderungen - Übersicht der Schritte

Aufgabe	Beschreibung	Anweisungen siehe
Konfigurieren Sie restriktive Dateiberechtigungen für normale Benutzer.	Hierdurch wird ein restriktiverer Wert als `022` für Dateiberechtigungen der normalen Benutzer festgelegt.	So legen Sie einen restriktiveren `umask`-Wert für normale Benutzer fest [44]
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)
Bewahren Sie die Integrität der Systemdateien.	Sucht nach Rogue-Dateien über ein Skript oder BART.	„How to Find Files With Special File Permissions“ in „Securing Files and Verifying File Integrity in Oracle Solaris 11.2 “

Sichern von Systemzugriff und -verwendung

Sie können die Sicherheitsfunktionen von Oracle Solaris so konfigurieren, dass Ihre Systemnutzung geschützt wird, einschließlich Anwendungen und Services im System und im Netzwerk.

TABELLE 2-6 Sichern von Systemzugriff und -verwendung - Übersicht der Schritte

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 „Securing Files and Verifying File Integrity in Oracle Solaris 11.2 “
Stellen Sie sicher, dass Binärdateien, die für ASLR (Address Space Layout Randomization) getaggt sind, ASLR auch verwenden können.	Dadurch wird ASLR für getaggte Binärdateien aktiviert.	So prüfen Sie, ob ASLR aktiviert ist [33]
Konfigurieren Sie die Prüfung.	Hiermit wird die Prüfkonfiguration für Abdeckung und Dateiintegrität angepasst.	„Verwenden des Prüfservice“ [58]
Schützen Sie Core-Dateien, die möglicherweise vertrauliche Informationen enthalten.	Es wird ein Verzeichnis mit eingeschränktem Zugriff erstellt, das für Core-Dateien verwendet wird.	„Enabling File Paths“ in „Troubleshooting System Administration Issues in Oracle Solaris 11.2 “ „Administering Your Core File Specifications“ in „Troubleshooting System Administration Issues in Oracle Solaris 11.2 “
Schützen Sie einen Webserver mit SSL-Kernel-Proxy.	Mit dem SSL-Protokoll (Secure Sockets Layer) können Sie die Webserverkommunikation verschlüsseln und beschleunigen.	Kapitel 3, „Web Servers and the Secure Sockets Layer Protocol“ in „Securing the Network in Oracle Solaris 11.2 “
Erstellen Sie Zonen für die Eingrenzung von Anwendungen.	Bei Zonen handelt es sich um Container, die Prozesse isolieren. Sie können Anwendungen ganz oder teilweise isolieren. Beispiel: Zonen können eingesetzt werden, um die Datenbank einer Website vom Webserver der Site zu trennen.	„Introduction to Oracle Solaris Zones “
Verwalten Sie Ressourcen in Zonen.	Zonen bieten eine Reihe von Tools zur Verwaltung von Zonenressourcen.	„Administering Resource Management in Oracle Solaris 11.2 “

Schutz eines Legacy-Service mit SMF

Sie können die Anwendungskonfiguration auf vertrauenswürdige Benutzer oder Rollen einschränken, indem Sie die Anwendung der SMF-Funktion (Service Management Facility) von Oracle Solaris hinzufügen und dann Rechte zum Starten, Aktualisieren und Stoppen des Service erforderlich machen.

Informationen und Anweisungen:

- „Locking Down Resources by Using Extended Privileges“ in „Securing Users and Processes in Oracle Solaris 11.2 “
- Securing MySQL using SMF - the Ultimate Manifest (http://blogs.oracle.com/bobn/entry/securing_mysql_using_smf_the).
- Relevante Manpages umfassen `smf`(5), `smf_security`(5), `svcadm`(1M), `svcbundle`(1M) und `svccfg`(1M).

Konfigurieren eines Kerberos-Netzwerks

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 3, „Planning for the Kerberos Service“ in „Managing Kerberos and Other Authentication Services in Oracle Solaris 11.2 “
- Kapitel 4, „Configuring the Kerberos Service“ in „Managing Kerberos and Other Authentication Services in Oracle Solaris 11.2 “
- Relevante Manpages umfassen `kadmin`(1M), `pam_krb5`(5) und `kclient`(1M).

Hinzufügen einer mehrstufigen Sicherheitskennzeichnung

Trusted Extensions erweitert die Oracle Solaris-Sicherheit, indem eine obligatorische kennzeichnungsbasierte 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 Kennzeichnungen erkennenden Geräten

Die Packages `system/trusted` und `system/trusted/trusted-global-zone` sind ausreichend bei einem "Headless"-System oder bei einem Server, bei dem kein mehrstufiger Desktop erforderlich ist. Das Package `system/trusted/trusted-extensions` bietet die vertrauenswürdige Desktopumgebung mit mehreren Ebenen von Oracle Solaris.

Konfiguration von Trusted Extensions

Sie müssen zuerst die Trusted Extensions-Pakete installieren und anschließend das System konfigurieren. Bei der Installation des Package `trusted-extensions` kann das System einen Desktop mit einem direkt angeschlossenen 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, „About IP Security Architecture“ in „Securing the Network in Oracle Solaris 11.2 “
- „Administration of Labeled IPsec“ in „Trusted Extensions Configuration and Administration “
- „Configuring Labeled IPsec“ in „Trusted Extensions Configuration and Administration “

♦ ♦ ♦ KAPITEL 3

Verwalten und Überwachen der Oracle Solaris-Sicherheitsfunktionen

Nach der erstmaligen Installation und Konfiguration können Sie die Sicherheitslage Ihres Systems durch folgende Maßnahmen verwalten und überwachen:

- Regelmäßige Überprüfung der Prüfdatensätze
- Ausführen von Package- und Dateiintegritätsprüfungen
- Überwachung der Netzwerkaktivität
- Ausführen von Compliancеprüfungen

Verwalten und Überwachen der Systemsicherheit

Mithilfe der folgenden Aufgaben können Sie den Zugriff auf und die Verwendung Ihres Systems und Ihrer Daten sowie die Einhaltung der Sicherheitsanforderungen Ihres Standorts verwalten und überwachen.

TABELLE 3-1 Verwalten und Überwachen der Systemsicherheit - Übersicht der Schritte

Aufgabe	Beschreibung	Anweisungen siehe
Überprüfen Sie die Packages im System.	Dadurch wird überprüft, ob die Packages nach einem Update mit den Quellpackages identisch sind.	Pakete überprüfen [33]
Überprüfen Sie die Dateiintegrität.	Nach der Konfiguration werden BART-Manifestdateien in regelmäßigen Abständen verglichen, um sicherzugehen, dass nur Dateien geändert werden, die auch geändert werden sollen.	„Die Dateiintegrität mittels BART überprüfen.“ [58]
Spüren Sie Rogue-Dateien auf.	Dadurch wird die möglicherweise unberechtigte Verwendung der Berechtigungen `setuid` und `setgid` für Programme lokalisiert.	„How to Find Files With Special File Permissions“ in „Securing Files and Verifying File Integrity in Oracle Solaris 11.2 “
Überprüfen Sie Prüflogs in regelmäßigen Abständen.	Dadurch werden ungewöhnliche Zugriffe und Nutzungen des Systems lokalisiert.	„Verwenden des Prüfservice“ [58]
Überprüfen Sie die Prüflogs auf An- und Abmeldeereignisse in Echtzeit.	Dadurch werden versuchte Sicherheitsverletzungen zeitnah erkannt.	„Überwachen von Prüfdatensätzen in Echtzeit“ [59]

Aufgabe	Beschreibung	Anweisungen siehe
Führen Sie Compliancetests durch.	Dadurch wird die Compliance des Systems mit Sicherheitsbenchmarks bewertet.	„Oracle Solaris 11.2 Handbuch zur Sicherheitscompliance “ und die Manpage `compliance`(1M)

Die Dateiintegrität mittels BART überprüfen.

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

Informationen und Anweisungen:

- „About BART“ in „Securing Files and Verifying File Integrity in Oracle Solaris 11.2 “
- „About Using BART“ in „Securing Files and Verifying File Integrity in Oracle Solaris 11.2 “
- „BART Manifests, Rules Files, and Reports“ in „Securing Files and Verifying File Integrity in Oracle Solaris 11.2 “

Anweisungen zum Nachverfolgen von Änderungen an installierten Systemen finden Sie unter „How to Compare Manifests for the Same System Over Time“ in „Securing Files and Verifying File Integrity in Oracle Solaris 11.2 “.

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.

Der Prüfservice wird in „Managing Auditing in Oracle Solaris 11.2 “ erläutert. Eine Liste der Manpages mit den entsprechenden Links finden Sie unter „Audit Service Man Pages“ in „Managing Auditing in Oracle Solaris 11.2 “.

Die folgenden Prüfserviceverfahren erweisen sich in zahlreichen sicheren Umgebungen als nützlich:

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

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

  Informationen zur Erstellung von Rollen oder zur Verwendung der vordefinierten ARMOR-Rollen finden Sie unter „Assigning Rights to Users“ in „Securing Users and Processes in Oracle Solaris 11.2 “.

- Prüfen Sie alle Administratoren mit der `cusa`-Prüfklasse.

  Ereignisse in der `cusa`-Prüfklasse umfassen administrative Aktionen, die sich auf die Sicherheitslage des Systems auswirken. Eine Beschreibung finden Sie in der Datei `/etc/security/audit_class`. Die genaue Vorgehensweise finden Sie unter Wichtige Ereignisse außer Anmelden/Abmelden prüfen [45].
- Senden Sie Prüfdatensätze an einen zentralen Server.
  - Konfigurieren Sie die Prüfung so, dass diese den Audit Remote Server (ARS) verwendet.

    Siehe „How to Send Audit Files to a Remote Repository“ in „Managing Auditing in Oracle Solaris 11.2 “.
  - Bereiten Sie die sichere Übertragung kompletter Prüfdateien in ein Dateisystem für die Dateieinsicht auf einem separaten ZFS-Pool vor.
- Überwachen Sie Textzusammenfassungen ausgewählter überprüfter Ereignisse im `syslog`-Dienstprogramm.

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

  Siehe „How to Configure syslog Audit Logs“ in „Managing Auditing in Oracle Solaris 11.2 “.
- 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 „Managing Auditing in Oracle Solaris 11.2 “.
- 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 Prüfdatensätzen in Echtzeit

Mit dem Plug-in `audit_syslog` können Sie Zusammenfassungen zuvor ausgewählter Prüfereignisse aufzeichnen. Um Prüfzusammenfassungen bei ihrer Generierung in einem Terminalfenster anzuzeigen, führen Sie einen Befehl aus, der in etwa dem Folgenden gleichkommt:

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

Informationen zur Konfiguration des Prüflogs finden Sie unter „How to Configure syslog Audit Logs“ in „Managing Auditing in Oracle Solaris 11.2 “.

Einsehen und Archivieren der Prüfprotokolle

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

Informationen und Anweisungen:

- „Audit Logs“ in „Managing Auditing in Oracle Solaris 11.2 “
- „Preventing Audit Trail Overflow“ in „Managing Auditing in Oracle Solaris 11.2 “
- „Displaying Audit Trail Data“ in „Managing Auditing in Oracle Solaris 11.2 “

♦ ♦ ♦ ANHANG A

Literaturverzeichnis zur Oracle Solaris-Sicherheit

Folgende Referenzen enthalten hilfreiche Informationen zum Thema Sicherheit auf Oracle Solaris-Systemen. Sicherheitsinformationen zu früheren Releases von Oracle Solaris enthalten teils nützliche, teils veraltete Informationen.

Sicherheitsreferenzen im Oracle Technology Network

Die folgenden Bücher und Artikel auf der Oracle Technology Network-Website enthalten Beschreibungen zur Sicherheit in Oracle Solaris 11-Systemen:

- „Securing Systems and Attached Devices in Oracle Solaris 11.2 “
- „Securing Files and Verifying File Integrity in Oracle Solaris 11.2 “
- „Securing the Network in Oracle Solaris 11.2 “
- „Securing Users and Processes in Oracle Solaris 11.2 “
- „Managing Encryption and Certificates in Oracle Solaris 11.2 “
- „Managing Auditing in Oracle Solaris 11.2 “
- „Managing Kerberos and Other Authentication Services in Oracle Solaris 11.2 “
- „Managing Secure Shell Access in Oracle Solaris 11.2 “
- „Oracle Solaris 11.2 Handbuch zur Sicherheitscompliance “
- „Using a FIPS 140 Enabled System in Oracle Solaris 11.2 “

Oracle Solaris-Sicherheitsreferenzen in Veröffentlichungen Dritter

Die folgenden Bücher enthalten eine Beschreibung der Sicherheit in Oracle Solaris 11-Systemen:

- *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. In diesem Dokument werden Sicherheitseinstellungen für das Betriebssystem Oracle Solaris empfohlen. 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.

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

  Dieses Fachbuch behandelt Fragen zur Oracle Solaris-Sicherheit.
- *Oracle Solaris 11: First Look*. Philip P. Brown. 2013. Packt Publishing. ISBN 9781849688307.

  Dieses Fachbuch bietet eine Einführung in Oracle Solaris und darin enthaltene Sicherheitsfunktionen für Administratoren.
- *Oracle Solaris 11 System Administration*, Bill Calkins. 2013. Prentice Hall. ISBN 9780133007114.

  In diesem Fachbuch werden die neuen Funktionen von Oracle Solaris behandelt, einschließlich Sicherheitsfunktionen.