

Oracle® Solaris 10-Sicherheitsrichtlinien

Copyright © 2011, Oracle und/oder verbundene Unternehmen. Alle Rechte vorbehalten.

Diese Software und zugehörige Dokumentation werden im Rahmen eines Lizenzvertrages zur Verfügung gestellt, der Einschränkungen hinsichtlich Nutzung und Offenlegung enthält und durch Gesetze zum Schutz geistigen Eigentums geschützt ist. Sofern nicht ausdrücklich in Ihrem Lizenzvertrag vereinbart oder gesetzlich geregelt, darf diese Software weder ganz noch teilweise in irgendeiner Form oder durch irgendein Mittel zu irgendeinem Zweck kopiert, reproduziert, übersetzt, gesendet, verändert, lizenziert, übertragen, verteilt, ausgestellt, ausgeführt, veröffentlicht oder angezeigt werden. Reverse Engineering, Disassemblierung oder Dekompilierung der Software ist verboten, es sei denn, dies ist erforderlich, um die gesetzlich vorgesehene Interoperabilität mit anderer Software zu ermöglichen.

Die hier angegebenen Informationen können jederzeit und ohne vorherige Ankündigung geändert werden. Wir übernehmen keine Gewähr für deren Richtigkeit. Sollten Sie Fehler oder Unstimmigkeiten finden, bitten wir Sie, uns diese schriftlich mitzuteilen.

Wird diese Software oder zugehörige Dokumentation an die Regierung der Vereinigten Staaten von Amerika bzw. einen Lizenznehmer im Auftrag der Regierung der Vereinigten Staaten von Amerika geliefert, gilt Folgendes:

U.S. GOVERNMENT RIGHTS

Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065, USA.

Diese Software oder Hardware ist für die allgemeine Anwendung in verschiedenen Informationsmanagementanwendungen konzipiert. Sie ist nicht für den Einsatz in potenziell gefährlichen Anwendungen bzw. Anwendungen mit einem potenziellen Risiko von Personenschäden geeignet. Falls die Software oder Hardware für solche Zwecke verwendet wird, verpflichtet sich der Lizenznehmer, sämtliche erforderlichen Maßnahmen wie Fail Safe, Backups und Redundancy zu ergreifen, um den sicheren Einsatz dieser Software oder Hardware zu gewährleisten. Oracle Corporation und ihre verbundenen Unternehmen übernehmen keinerlei Haftung für Schäden, die beim Einsatz dieser Software oder Hardware in gefährlichen Anwendungen entstehen.

Oracle und Java sind eingetragene Marken von Oracle und/oder ihren verbundenen Unternehmen. Andere Namen und Bezeichnungen können Marken ihrer jeweiligen Inhaber sein.

Intel und Intel Xeon sind Marken oder eingetragene Marken der Intel Corporation. Alle SPARC-Marken werden in Lizenz verwendet und sind Marken oder eingetragene Marken der SPARC International, Inc. AMD, Opteron, das AMD-Logo und das AMD Opteron-Logo sind Marken oder eingetragene Marken der Advanced Micro Devices. UNIX ist eine eingetragene Marke der The Open Group.

Diese Software oder Hardware und die zugehörige Dokumentation können Zugriffsmöglichkeiten auf Inhalte, Produkte und Serviceleistungen von Dritten enthalten. Oracle Corporation und ihre verbundenen Unternehmen übernehmen keine Verantwortung für Inhalte, Produkte und Serviceleistungen von Dritten und lehnen ausdrücklich jegliche Art von Gewährleistung diesbezüglich ab. Oracle Corporation und ihre verbundenen Unternehmen übernehmen keine Verantwortung für Verluste, Kosten oder Schäden, die aufgrund des Zugriffs oder der Verwendung von Inhalten, Produkten und Serviceleistungen von Dritten entstehen.

Inhalt

Vorwort5

1 Oracle Solaris 10 Sicherheitsrichtlinien 9

Oracle Solaris 10-Systemabsicherungsreferenzen9

Zusätzliche Sicherheitsreferenzen für Oracle Solaris 10 10

Vorwort

Dieses Handbuch enthält Verweise und Beschreibungen zu Sicherheitsrichtlinien für Betriebssystem Oracle Solaris (Oracle Solaris). In den Systemabsicherungsreferenzen werden die Absicherung von Oracle Solaris 10-Systemen und die Verwendung der Oracle Solaris-Sicherheitsfunktionen zum Schutz von Daten und Anwendungen beschrieben. Die Angaben sind als Empfehlungen zu verstehen, die an die Sicherheitsrichtlinien des jeweiligen Standorts angepasst werden können.

Zusätzlich enthält dieses Handbuch Verweise auf Hintergrundinformationen über Oracle Solaris-Sicherheit und White Papers zur Unterstützung bei gängigen Implementierungen.

Zielgruppe

Die *Oracle Solaris 10-Sicherheitsrichtlinien* richten sich an Sicherheitsadministratoren und andere Administratoren, die folgende Aufgaben ausführen:

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

Um dieses Dokument verwenden zu können, benötigen Sie allgemeine Kenntnisse zur UNIX-Administration, ein gutes Grundlagenwissen zur Softwaresicherheit und müssen Ihre Standort-Sicherheitsrichtlinien kennen.

Themenverwandte Websites von Drittanbietern

In der vorliegenden Dokumentation wird auf URLs von Drittanbietern verwiesen, über die zusätzliche relevante Informationen zur Verfügung gestellt werden.

Oracle ist nicht für die Verfügbarkeit der in diesem Dokument genannten Drittanbieter-Websites verantwortlich. Oracle ist in keinerlei Weise verantwortlich oder haftbar für Inhalte, Werbung, Produkte oder Materialien, die mittels solcher Websites oder Ressourcen bereitgestellt werden. Oracle übernimmt keine Verantwortung oder Haftung für tatsächliche oder angebliche Schäden oder Verluste, die im Zusammenhang mit den auf diesen Websites angebotenen Informationen, Waren oder Dienstleistungen entstanden sind.

Zugriff auf Oracle-Support

Oracle-Kunden haben über My Oracle Support Zugriff auf elektronischen Support. Weitere Informationen finden Sie unter <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> oder für Hörgeschädigte unter <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs>.

Typografische Konventionen

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

TABELLE P-1 Typografische Konventionen

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

Shell-Eingabeaufforderungen in Befehlsbeispielen

Die folgende Tabelle zeigt die UNIX-Standardeingabeaufforderung und die Superuser-Eingabeaufforderung für Shells, die zum Betriebssystem Oracle Solaris gehören. Die in den Befehlsbeispielen angezeigte Standard-Systemeingabeaufforderung variiert, abhängig von der Oracle Solaris-Version.

TABELLE P-2 Shell-Eingabeaufforderungen

Shell	Eingabeaufforderung
Bash-Shell, Korn-Shell und Bourne-Shell	\$
Bash-Shell, Korn-Shell und Bourne-Shell für Superuser	#
C-Shell	system%
C-Shell für Superuser	system#

Oracle Solaris 10 Sicherheitsrichtlinien

Oracle Solaris 10 ist ein robustes Unternehmensbetriebssystem mit bewährten Sicherheitsfunktionen. Mit einem ausgeklügelten netzwerkweiten Sicherheitssystem, das den Zugriff auf Dateien steuert, Systemdatenbanken schützt und die Verwendung von Systemressourcen überwacht, erfüllt Oracle Solaris 10 Sicherheitsanforderungen auf jeder Ebene. Während traditionelle Betriebssysteme mit systemeigenen Sicherheitsschwächen behaftet sein können, ist Oracle Solaris 10 dank seiner Flexibilität an die verschiedensten Sicherheitsanforderungen von Unternehmensservern bis zu Desktop-Clients anpassbar.

Oracle Solaris 10-Systemabsicherungsreferenzen

Die folgenden beiden Dokumente beschreiben die Absicherung von Oracle Solaris, die Verwendung der Sicherheitsfunktionen zur Konfiguration von Systemen, in denen Anwendungen und Benutzer sicher hinzugefügt werden können, und die Benutzung bestimmter Funktionen zum Schutz netzwerkbasierter Anwendungen. Zu jedem Dokumenttitel ist eine kurze Beschreibung vorhanden.

- *CIS Solaris 10 Benchmark v5.0.0* (<http://benchmarks.cisecurity.org/en-us/?route=downloads.show.single.solaris10.500>), 9. Juli 2010.
Dieses Dokument hat auch den Titel *Security Configuration Benchmark for Solaris 10 11/06 through 10/09*. Das Dokument ist das Resultat einer siebenjährigen Zusammenarbeit zahlreicher Mitwirkender, einschließlich Sun Microsystems, der Defense Information Systems Agency (DISA), dem Center for Internet Security (CIS), dem National Institute of Standards and Technology (NIST), der National Security Agency (NSA) und vieler einzelner Unternehmen, akademischer Einrichtungen und Einzelpersonen. Das Dokument enthält grundlegende Richtlinien zur Absicherung, die von Sun, CIS, NSA und DISA vereinbart wurden.
- *An Overview of Solaris 10 Operating System Security Controls* (http://www.nsa.gov/ia/_files/os/sunsol_10/s10-cis-appendix-v1.1.pdf), Glenn Brunette, September 2007, v1.0

Dieser Anhang zu *Security Configuration Benchmark for Solaris 10 11/06 through 10/09* konzentriert sich auf sicherheitsrelevante Aspekte von Oracle Solaris 10, die außerhalb der Bereiche Systemabsicherung und Sicherheitskonfiguration liegen. Der Anhang bietet eine komplette Übersicht der Sicherheitsfunktionen und -fähigkeiten von Oracle Solaris 10 und enthält, wenn möglich, spezifische Empfehlungen.

Zusätzliche Sicherheitsreferenzen für Oracle Solaris 10

Die folgenden Handbücher und Artikel ergänzen die Systemabsicherungsrichtlinien im vorhergehenden Abschnitt:

- *Systemverwaltungshandbuch: Sicherheitsservices*

Dieses Sicherheitshandbuch wurde von Oracle für Oracle Solaris 10-Administratoren veröffentlicht. In diesem Handbuch werden die Sicherheitsfunktionen des Betriebssystems Oracle Solaris 10 und ihre Verwendung beschrieben. Anders als *Security Configuration Benchmark for Solaris 10 11/06 through 10/09* geht es in diesem Handbuch nicht speziell um die Systemabsicherung oder um Best Practices.

- *Solaris 10 Security Essentials*, Sun engineers, 2009. ISBN 978-0137012336

Solaris-Ingenieure und technische Redakteure beschreiben in diesem im Buchhandel erhältlichen Werk 12 Solaris-Sicherheitstechnologien mit Beispielen. Anders als *Security Configuration Benchmark for Solaris 10 11/06 through 10/09* geht es in diesem Handbuch nicht speziell um die Systemabsicherung oder um Best Practices.

- *Using Oracle® Solaris 10 to Overcome Security Challenges* (<http://www.oracle.com/technetwork/server-storage/solaris/solaris-10-security-167783.pdf>), August 2010.

Dieses von Oracle herausgegebene White Paper richtet sich an Organisationen mit umfangreichen Anforderungen in Bezug auf Sicherheitsfunktionen. IT-Abteilungen, die eine effektive und effiziente Lösung für die Computersicherheit benötigen, können die einzigartigen und leistungsfähigen Funktionen von Oracle Solaris 10 nutzen, um das Unternehmen vor potenziellen Bedrohungen zu schützen, Anforderungen von Unternehmen und Behörden zu erfüllen und sicherheitsspezifischen Herausforderungen gewachsen zu sein. Dieses White Paper bietet eine allgemeine Beschreibung der Oracle Solaris-Sicherheitsfunktionen. Es ist nicht als Systemabsicherungs- oder Best Practices-Dokument ausgelegt.

- *Hardening Oracle Database with Oracle Solaris Security Technologies* (<http://www.oracle.com/technetwork/server-storage/solaris/solaris-security-hardening-db-167784.pdf>), Glenn Faden und Christoph Schuba, August 2010.

Dieses von Oracle herausgegebene White Paper beschreibt und veranschaulicht, wie die Sicherheitsfunktionen von Oracle Solaris zum Sperren der auf das Netzwerk ausgerichteten Services verwendet werden können, um sie vor internen und externen Bedrohungen zu

schützen. Technologiekonzepte und ihre Implementierung werden praxisnah an einem unter Solaris 10 10/09 ausgeführten Beispiel (Oracle Database Server 11g Release 2) veranschaulicht.

