SPARC M8- und SPARC M7-Server - Sicherheitshandbuch

Teilenr.: E63781-02
September 2017

Teilenr.: E63781-02

Copyright © 2015, 2017, Oracle und/oder verbundene Unternehmen. All rights reserved. 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, dann gilt Folgendes:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

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 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 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 von The Open Group.

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

Zugriff auf Oracle-Support

Oracle-Kunden mit einem gültigen Oracle-Supportvertrag haben Zugriff auf elektronischen Support über My Oracle Support. Weitere Informationen erhalten Sie unter `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` oder unter `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs`, falls Sie eine Hörbehinderung haben.

Inhalt

Hardwaresicherheit

Physische Isolierung und Zugriffskontrolle stellen die Grundlage dar, auf der die Sicherheitsarchitektur basieren muss. Indem Sie sicherstellen, dass der physische Server in einer sicheren Umgebung aufgestellt wird, können Sie ihn vor unautorisiertem Zugriff schützen. Ebenso wird die Aufzeichnung aller Seriennummern empfohlen, um die Verwendung von nicht autorisierten Hardwarekomponenten zu verhindern.

Die folgenden Abschnitte enthalten allgemeine Hardwaresicherheitsrichtlinien für Server.

Zugriffsbeschränkungen

- Installieren Sie Server und zugehörige Komponenten in einem Raum, der abgeschlossen werden kann und zu dem nicht jeder Zutritt hat.
- Wenn sich Geräte in einem Rack mit Türverriegelung befinden, halten Sie die Tür geschlossen, wenn Sie keine Wartungsarbeiten an Komponenten im Rack vornehmen müssen. Durch Verriegeln der Türen wird auch der Zugang zu Hot-Swapping- oder Hot-Plugging-Geräten eingeschränkt.
- Bewahren Sie alle Ersatzteile in einem verschlossenen Schrank auf. Nur autorisiertes Personal darf Zugang zu diesem Schrank haben.
- Überprüfen Sie regelmäßig den Zustand und die Integrität der Verriegelungen am Rack und am Schrank der Ersatzteile, um Manipulation oder versehentlich unverschlossene Türen zu verhindern oder zu entdecken.
- Lagern Sie Schrankschlüssel in einem sicheren Ort mit eingeschränktem Zugang.
- Schränken Sie den Zugriff auf USB-Konsolen ein. Geräte wie Systemcontroller, Stromverteilereinheiten (Power Distribution Units, PDUs) und Netzwerk-Switches können USB-Anschlüsse aufweisen. Der physische Zugriff ist eine sicherere Methode, auf eine Komponente zuzugreifen, da sie dabei keinen netzwerkbasierten Angriffen ausgesetzt ist.
- Schließen Sie die Konsole an ein externes KVM an, um Remote-Konsolenzugriff zu ermöglichen. KVM-Geräte unterstützen häufig Zwei-Faktor-Authentifizierung,

zentralisierte Zugriffskontrolle und Auditing. Weitere Informationen zu den Sicherheitsrichtlinien und Best Practices für KVMs finden Sie in der Dokumentation für das KVM-Gerät.

Seriennummern

Verhindern Sie die Verwendung von nicht autorisierten Hardwarekomponenten, indem Sie alle Seriennummern beim Erhalt der Komponenten genau aufzeichnen und ablegen. Bevor die Komponente installiert oder verwendet wird, müssen Sie ihre Authentizität prüfen, indem Sie ihre Seriennummer mit der Aufzeichnung beim Erhalt der Komponente vergleichen. Befolgen Sie diese Vorgehensweisen zur Sicherung von Hardware:

- Bewahren Sie alle Hardwareseriennummern auf.
- Versehen Sie alle wichtigen Komponenten der Computerhardware, wie z.B. Ersatzteile, mit einer Sicherheitskennzeichnung. Verwenden Sie spezielle UV-Stifte oder geprägte Beschriftungen.
- Bewahren Sie Hardwareaktivierungsschlüssel und Lizenzen an einem sicheren Ort auf, der im Systemnotfall für den Systemverwalter einfach zugänglich ist. Die ausgedruckten Dokumente sind möglicherweise Ihr einziger Eigentumsnachweis.

Durch drahtlose RFID-Lesegeräte (Radio Frequency Identification) gestaltet sich die Ressourcenüberwachung noch einfacher. Weitere Informationen dazu finden Sie im Oracle-Whitepaper *How to Track Your Oracle Sun System Assets by Using RFID* unter:

`http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-001-rfid-oracle-214567.pdf`

Festplatten

Festplattenlaufwerke und Solid-State-Laufwerke werden häufig zur Speicherung vertraulicher Daten verwendet. Um diese Informationen vor nicht autorisierter Offenlegung zu schützen, bereinigen Sie die Festplattenlaufwerke, bevor Sie sie wiederverwenden, außer Betrieb setzen oder entsorgen.

- Verwenden Sie Tools zum Bereinigen von Datenträgern, wie den Oracle Solaris-Befehl `format` (1M), um alle Daten vollständig von der Festplatte zu löschen.
- Unternehmen sollten anhand ihrer Datenschutzrichtlinien die am ehesten geeignete Methode zum Bereinigen von Festplatten bestimmen.
- Falls erforderlich nutzen Sie den Oracle Customer Data and Device Retention Service.

http://www.oracle.com/us/support/library/data-retention-ds-405152.pdf

Softwaresicherheit

Hardwaresicherheit wird größtenteils durch Softwaremaßnahmen umgesetzt. Die folgenden Abschnitte enthalten allgemeine Softwaresicherheitsrichtlinien für Server.

▼ Verhindern von unautorisiertem Zugriff (Oracle Solaris-BS)

- **Verwenden Sie Oracle Solaris-BS-Befehle, um den Zugriff auf die Oracle Solaris-Software einzuschränken, das BS zu schützen, Sicherheitsfunktionen zu verwenden und Anwendungen zu schützen.**

  Sie erhalten das *Oracle Solaris Security Guidelines*-Dokument für die von Ihnen verwendete Version unter:

  - `http://www.oracle.com/goto/solaris11/docs`
  - `http://www.oracle.com/goto/solaris10/docs`

▼ Verhindern von unautorisiertem Zugriff (Oracle ILOM)

1. **Verwenden Sie Oracle ILOM-Befehle, um den Benutzerzugriff auf die Oracle ILOM-Software einzuschränken, das werksseitig eingestellte Kennwort zu ändern, die Verwendung des Root Superuser-Accounts einzuschränken und das private Netzwerk für den Serviceprozessor zu sichern.**

   Rufen Sie das *Oracle ILOM - Sicherheitshandbuch* hier ab:

   `http://www.oracle.com/goto/ilom/docs`

2. **Verwenden Sie wenn möglich die plattformspezifischen Oracle ILOM-Befehle, um individuelle Domänen durch Erstellung von Benutzeraccounts mit Rollen zu sichern, die für eine spezielle physische Domäne gelten.**

   Wenn Sie einer physischen Domäne Benutzerrollen zuweisen, spiegeln die Fähigkeiten für diese Domäne diejenigen der für die Plattform zugewiesenen Benutzerrollen wider. Sie sind aber auf die für die angegebene Komponente ausgeführten Befehle eingeschränkt.

   Anmerkung - Lediglich die Benutzerrollen "administrator" (a), "console" (c) und "reset" (r) können für individuelle physische Domänen zugewiesen werden.

   Rufen Sie den *SPARC M8 and SPARC M7 Servers Administration Guide* hier ab:

   `http://docs.oracle.com/cd/E55211_01/`

Verhindern von unautorisiertem Zugriff (Oracle VM Server for SPARC)

- **Verwenden Sie Oracle VM for SPARC-Befehle, um den Zugriff auf die Oracle VM for SPARC-Software einzuschränken.**

  Den *Oracle VM for SPARC Security Guide* erhalten Sie unter: `http://www.oracle.com/goto/vm-sparc/docs`.

Zugriff einschränken (OBP)

In diesen Themen wird erläutert, wie Sie den Zugriff an dem OBP-Prompt einschränken.

Informationen zum Festlegen der OpenBoot-Sicherheitsvariablen finden Sie in der OpenBoot-Dokumentation unter:

`http://www.oracle.com/goto/openboot/docs`

▼ Implementieren des Kennwortschutzes

- **Wenn Sie noch kein Kennwort festgelegt haben, führen Sie diesen Schritt jetzt aus.**

```
{0} ok password
New password (8 characters max):
Retype new password: password
```

Das Kennwort muss ein bis acht Zeichen enthalten. Wenn Sie mehr als acht Zeichen eingeben, werden nur die ersten acht Zeichen verwendet. Alle druckbaren Zeichen sind zulässig. Steuerzeichen sind nicht zulässig.

Anmerkung - Wenn Sie das Kennwort auf null Zeichen festlegen, wird die Sicherheit deaktiviert und der Parameter `security-mode` wird behandelt, als wäre er auf `none` festgelegt. Die Einstellung wird dadurch nicht geändert.

▼ Aktivieren des Sicherheitsmodus

1. **Setzen Sie den Parameter `security-mode` auf `full` oder `command`.**

   Bei `full` ist ein Kennwort erforderlich, um normale Vorgänge auszuführen, wie `boot`. Bei `command` ist kein Kennwort für die Befehle `boot` und `go` erforderlich. Für alle anderen Befehle ist aber ein Kennwort erforderlich. Setzen Sie den Parameter`security-mode` aus Gründen der Geschäftskontinuität wie im folgenden Beispiel auf `command`.

```
{0} ok setenv security-mode command
{0} ok
```

2. **Rufen Sie den Prompt für den Sicherheitsmodus auf.**

   Nachdem Sie den Sicherheitsmodus wie oben beschrieben festgelegt haben, gibt es zwei Möglichkeiten, den Prompt für den Sicherheitsmodus aufzurufen.

   - **Verwenden Sie die Befehle `logout` und `login`.**

```
{0} ok logout
Type boot , go (continue), or login (command mode)
>
> login
Firmware Password: password
Type help for more information
{0} ok
```

     Um den Sicherheitsmodus zu beenden, verwenden Sie die Befehle `logout` und `login`.

   - **Verwenden Sie den Befehl `reset-all`.**

```
{0} ok reset-all
```

Dieser Befehl setzt das System zurück. Wenn das System wieder hochgefahren wird, geht OpenBoot zu dem Prompt für den Sicherheitsmodus. Um sich wieder bei dem Befehlsprompt anzumelden (oder sich von dem Sicherheitsmodus abzumelden), verwenden Sie die Befehle `logout` und `login` und geben dann das Kennwort wie oben beschrieben ein.

Deaktivieren des Sicherheitsmodus

1. **Setzen Sie den Parameter `security-mode` auf `none`.**

   ```
   {0} ok setenv security-mode none
   ```

2. **Setzen Sie das Kennwort auf eine Nulllänge, indem Sie nach beiden Kennwortprompts die Eingabetaste drücken.**

Prüfung auf nicht erfolgreiche Anmeldungen (OBP)

1. **Bestimmen Sie, ob jemand nicht erfolgreich versucht hat, auf die OpenBoot-Umgebung zuzugreifen, indem Sie den Parameter `security-#badlogins` wie im folgenden Beispiel verwenden.**

   ```
   ok printenv security-#badlogins
   ```

   Wenn dieser Befehl einen höheren Wert als Null zurückgibt, wurde ein nicht erfolgreicher Zugriffsversuch auf die OpenBoot-Umgebung aufgezeichnet.

2. **Setzen Sie den Parameter zurück, indem Sie Folgendes eingeben:**

   ```
   ok setenv security-#badlogins 0
   ```

Bereitstellen eines Banners zum Hochfahren

Auch wenn es keine direkte Vorsichts- oder Erkennungsmaßnahme ist, kann ein Banner doch verwendet werden, um:

- die Eigentümerschaft zu vermitteln.
- Benutzer vor der Verwendung des Servers zu warnen.

- anzugeben, dass OpenBoot-Parameter nur von autorisiertem Personal verwendet oder geändert werden dürfen.

- **Mit den folgenden Befehlen können Sie eine benutzerdefinierte Warnmeldung aktivieren.**

```
{0} ok setenv oem-banner banner-message
{0} ok setenv oem-banner? true
```

Die Bannermeldung kann maximal 68 Zeichen umfassen. Alle druckbaren Zeichen sind zulässig.

Oracle-Systemfirmware

Die Oracle-Systemfirmware verwendet einen kontrollierten Aktualisierungsprozess, um nicht autorisierte Modifizierungen zu verhindern. Ausschließlich der Superuser oder ein authentifizierter Benutzer mit der entsprechenden Autorisierung kann den Aktualisierungsprozess verwenden.

Informationen zum Abrufen der neuesten Updates oder Patches finden Sie in den Produkthinweisen unter:

http://docs.oracle.com/cd/E55211_01/

Sicherer WAN-Boot

WAN-Boot unterstützt verschiedene Sicherheitsstufen. Sie können die von WAN-Boot unterstützten Sicherheitsfunktionen im Hinblick auf die Anforderungen in Ihrem Netzwerk kombinieren. Eine Konfiguration mit einer höheren Sicherheit erfordert zwar mehr Administrationsaufwand, bedeutet aber auch einen besseren Schutz für Ihre Systemdaten.

- Informationen zur Konfiguration der sicheren WAN-Boot-Installation für Oracle Solaris 10 BS finden Sie in dem Buch *Oracle Solaris Installation Guide: Network-Based Installations*.

  Siehe http://www.oracle.com/goto/solaris10/docs
- Informationen für das Oracle Solaris 11-BS finden Sie in *Securing the Network in Oracle Solaris*.

  Siehe http://www.oracle.com/goto/solaris11/docs