Sicherheitshandbuch für Server der Serien SPARC und Netra SPARC S7-2

Teilenr.: E77185-01
Juni 2016

Teilenr.: E77185-01

Barrierefreie Dokumentation

Informationen zu Oracles Verpflichtung zur Barrierefreiheit erhalten Sie über die Website zum Oracle Accessibility Program http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

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. Gleichermaßen empfiehlt es sich, alle Seriennummern aufzuzeichnen, um Diebstahl, Wiederverkauf oder Lieferkettenrisiken (also die Einführung gefälschter oder kompromittierter Komponenten in die Lieferkette Ihrer Organisation) zu vermeiden.

Diese Abschnitte enthalten allgemeine Hardwaresicherheitsrichtlinien für die SPARC- und Netra SPARC S7-2-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.
- Lagern Sie nicht verwendete FRUs (Field Replaceable Units) oder CRUs (Customer Replaceable Units) in einem abschließbaren Schrank. Nur autorisiertes Personal sollte 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.
- Bewahren Sie Schrankschlüssel an einem sicheren Ort mit eingeschränktem Zugriff auf.
- Schränken Sie den Zugriff auf USB-Konsolen ein. Geräte wie System-Controller, Steckdosenleisten (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 den 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

- 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

Festplatten werden häufig zum Speichern sensibler Informationen verwendet. Um die unautorisierte Offenlegung dieser Informationen zu verhindern, müssen Festplatten komplett bereinigt werden, bevor sie wiederverwendet, außer Betrieb genommen oder entsorgt werden.

- 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.
- Nutzen Sie bei Bedarf 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. Diese Abschnitte enthalten allgemeine Softwaresicherheitsrichtlinien für die SPARC- und Netra SPARC S7-2-Server.

▼ Unautorisierten Zugriff verhindern (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`

▼ Unautorisierten Zugriff verhindern (Oracle ILOM)

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

  Rufen Sie das *Oracle ILOM Security Guide* hier ab:

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

▼ Unautorisierten Zugriff verhindern (Oracle VM Server for SPARC)

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

  Rufen Sie den *Oracle VM for SPARC - Sicherheitshandbuch* hier ab:

  `http://www.oracle.com/goto/vm-sparc/docs`

Zugriff einschränken (OpenBoot)

In diesen Themen wird beschrieben, wie Sie den Zugriff an der OpenBoot-Eingabeaufforderung einschränken.

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

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

▼ Passwortschutz implementieren

- **Falls Sie noch kein Passwort festgelegt haben, führen Sie diesen Schritt aus.**

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

Das Passwort kann ein bis acht Zeichen umfassen. Wenn Sie mehr als acht Zeichen eingeben, werden nur die ersten acht Zeichen verwendet. Alle druckbaren Zeichen werden akzeptiert. Steuerzeichen werden nicht akzeptiert.

Anmerkung - Ein Passwort mit null Zeichen schaltet die Sicherheit aus und behandelt den Parameter `security-mode` als wäre er auf `none` gesetzt. Dies ändert aber die Einstellung nicht.

▼ Sicherheitsmodus aktivieren

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

   Bei `full` ist ein Passwort erforderlich, um beliebige Aktionen, einschließlich normaler Vorgänge wie `boot`, auszuführen. Bei `command` ist kein Passwort für die Befehle `boot` und `go` erforderlich. Für alle anderen Befehle ist aber ein Passwort 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 die Sicherheitsmodus-Eingabeaufforderung auf.**

   Nachdem Sie den Sicherheitsmodus wie oben beschrieben eingerichtet haben, können Sie die Sicherheitsmodus-Eingabeaufforderung auf zwei Arten abrufen.

   - **Mit den Wörtern `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
     ```

     Zum Verlassen des Sicherheitsmodus verwenden Sie die Namen `logout` und `login` (siehe Beispiel).

   - **Verwenden Sie das Wort `reset-all`.**

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

     Mit diesem Wort setzen Sie das System zurück. Wenn das System wieder hochfährt, wird "OpenBoot" an die Sicherheitsmodus-Eingabeaufforderung übergeben. Um sich wieder bei der Eingabeaufforderung anzumelden (oder sich vom Sicherheitsmodus abzumelden), verwenden Sie die Namen `logout` und `login` und geben dann wie oben beschrieben das Passwort ein.

▼ Sicherheitsmodus deaktivieren

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

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

2. **Setzen Sie das Passwort auf die Länge null, indem Sie nach beiden Passwort-Eingabeaufforderungen auf "Zurück" drücken.**

▼ Auf nicht erfolgreiche Anmeldungen prüfen

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.**

```
{0} ok printenv security-#badlogins
```

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

2. **Setzen Sie den Parameter zurück, indem Sie diesen Befehl eingeben.**

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

▼ Banner zum Hochfahren bereitstellen

Auch wenn es keine direkte Schutzfunktion oder Erkennungsüberwachung darstellt, kann ein Banner aus den folgenden Gründen verwendet werden:

- Eigentumsrechte ausdrücken.
- Benutzer vor akzeptierbarer Servernutzung warnen.
- Informieren, dass Zugriffe oder Änderungen auf bzw. am OpenBoot-Parameter nur auf autorisierte Personen beschränkt sind.

- **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 bis zu 68 Zeichen umfassen. Alle druckbaren Zeichen werden akzeptiert.

Oracle-Systemfirmware

Die Oracle-Systemfirmware verwendet einen kontrollierten Aktualisierungsprozess, um nicht autorisierte Modifizierungen zu verhindern. Ausschließlich der Superuser oder ein

authentifizierter Benutzer mit ordnungsgemäßer Autorisierung kann den Aktualisierungsprozess verwenden.

Informationen zum Abrufen der neuesten Updates oder Patches finden Sie in den Produkthinweisen für Ihren Server.

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 zusätzlichen 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 im Handbuch *Oracle Solaris Installation Guide: Network-Based Installations*.
- Informationen für das Oracle Solaris 11-BS finden Sie in *Securing the Network in Oracle Solaris 11.3*.

Geprüfter Startvorgang (Verified Boot)

Mit Verified Boot können Sie Systemboot-Blöcke und Oracle Solaris-Kernel-Module überprüfen, bevor Sie im System geladen werden. Aktivieren Sie Verified Boot über Oracle ILOM, und geben Sie an, wie die Systemreaktion bei einer nicht erfolgreichen Überprüfung aussehen soll. Durch die Aktivierung von Verified Boot können Sie verhindern, dass schädliche Änderungen an den Systemboot-Blöcken oder Oracle Solaris-Kernel-Modulen in Kraft treten.

Informationen zur Konfiguration der SPARC Verified Boot-Eigenschaften finden Sie im *Oracle ILOM Administrator's Guide for Configuration and Maintenance*.