SPARC M5-32- und SPARC M6-32-Server

Sicherheitshandbuch

Teilenr.: E49763-02
Juli 2014

Inhaltsverzeichnis

• • • Kapitel 1

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.

Dieses Kapitel enthält allgemeine Hardware-Sicherheitsrichtlinien für die SPARC M5-32- und M6-32-Server.

Dieses Kapitel enthält die folgenden Abschnitte:

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. Schränken Sie zu Zugang zum abgeschlossenen Schrank auf autorisiertes Personal ein.
- Überprüfen Sie regelmäßig den Zustand und die Integrität der Verriegelungen am Rack und am Schrank der Ersatzteile, um Manipulation oder unverschlossene Türen zu verhindern oder zu entdecken.
- Lagern Sie Schrankschlüssel in einem sicheren Ort mit eingeschränktem Zugriff.
- 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

- 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.

Mit drahtlosen RFID-Lesegeräten kann die Ressourcenüberwachung noch vereinfacht werden. Weitere Informationen dazu finden Sie in *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. Alternativ dazu können Sie physische Entmagnetisierungswerkzeuge verwenden, sofern angemessen und verfügbar.
- In einigen Fällen sind die Daten auf den Festplatten so sensibel, dass die Festplatte physisch zerstört werden muss, indem sie pulverisiert oder eingeäschert wird.

Es wird dringend empfohlen, dass Organisationen sich auf ihre Datenschutzrichtlinien beziehen, um die am ehesten geeignete Methode zum Bereinigen von Festplatten zu bestimmen.

Achtung

Einige Daten auf modernen Festplatten, insbesondere SSDs können möglicherweise nicht von Software zum Bereinigen von Datenträgern gelöscht werden. Dies liegt an der Art, wie sie den Datenzugriff verwalten.

• • • Kapitel 2

Softwaresicherheit

Hardwaresicherheit wird größtenteils durch Softwaremaßnahmen umgesetzt. Dieses Kapitel enthält allgemeine Software-Sicherheitsrichtlinien für die SPARC M5-32- und SPARC M6-32-Server.

Dieses Kapitel enthält die folgenden Abschnitte:

▼ 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.
  Rufen Sie das Dokument mit den Sicherheitsrichtlinien für Oracle Solaris für die verwendete BS-Version hier ab:
  http://www.oracle.com/goto/Solaris11/docs
  http://www.oracle.com/goto/Solaris10/docs

▼ Verhindern von unautorisiertem Zugriff (Oracle ILOM)

1. Verwenden Sie die 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 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 M5-32 and SPARC M6-32 Servers Administration Guide* hier ab: http://www.oracle.com/goto/M6-32/docs

▼ 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.
  Rufen Sie den *Oracle VM for SPARC Security Guide* hier ab: http://www.oracle.com/goto/VM-SPARC/docs

Einschränken des Zugriffs (OpenBoot)

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

- Implementieren des Kennwortschutzes (OpenBoot) [8]
- Prüfung auf nicht erfolgreiche Anmeldungen (OpenBoot) [8]
- Bereitstellen eines Banners zum Hochfahren (OpenBoot) [9]

Zusätzliche Informationen

- Informationen zum Festlegen der OpenBoot-Sicherheitsvariablen finden Sie im *OpenBoot 4.x-Befehlsreferenzhandbuch* unter: http://download.oracle.com/docs/cd/E19455-01/816-1177-10/cfg-var.html#pgfId-17069

▼ Implementieren des Kennwortschutzes (OpenBoot)

- Setzen Sie den Parameter "security-mode" auf **full** oder **command**.
  Bei **full** ist ein Kennwort erforderlich, um normale Vorgänge auszuführen, wie Booten. 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".

```
ok password
ok setenv security-mode command
ok password
```

▼ Prüfung auf nicht erfolgreiche Anmeldungen (OpenBoot)

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 **security-#badlogins** zurück, indem Sie den folgenden Befehl eingeben.

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

▼ Bereitstellen eines Banners zum Hochfahren (OpenBoot)

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

```
ok setenv oem-banner banner-message
ok setenv oem-banner? true
```

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 aktuellsten Aktualisierungen 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 das Oracle Solaris 10-BS finden Sie in *Oracle Solaris Installationshandbuch: Netzwerkbasierte Installation*.

  http://www.oracle.com/goto/Solaris10/docs
- Informationen für das Oracle Solaris 11-BS finden Sie in *Securing the Network in Oracle Solaris 11.1*.

  http://www.oracle.com/goto/Solaris11/docs